The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0956-5698.htm

Received 2 January 2014
Revised 20 January 2014
Accepted 21 January 2014

Clear skies or cloudy forecast?

Legal challenges in the management and acquisition of audiovisual materials in the cloud

Elaine Goh
School of Library, Archival and Information Studies, The University of British Columbia, Vancouver, Canada

Abstract

Purpose – Using the example of audiovisual materials, this paper aims to illustrate how records-related and archival legislation lags behind advances in technology. As more audiovisual materials are created on the cloud, questions arise about the applicability of national laws over the control, ownership, and custody of data and records.

Design/methodology/approach – This paper analyses court cases relating to audiovisual materials in the cloud and archival legislation from three Commonwealth countries: Canada, Australia, and Singapore – representing North America, the Pacific, and Asia respectively.

Findings – Current records-related and archival legislation does not effectively address the creation, processing, and preservation of records and data in a cloud environment. The paper identifies several records-related risks linked to the cloud – risks related to the ownership and custody of data, legal risks due to transborder data flow, and risks due to differing interpretations on the act of copying and ownership of audiovisual materials.

Research limitations/implications – The paper identifies the need for records professionals to pay greater attention to the implications of the emerging cloud environment. There is a need for further research on how the concept of extraterritoriality and transborder laws can be applied to develop model laws for the management and preservation of records in the cloud.

Originality/value – The paper identifies record-related risks linked to the cloud by analyzing court cases and archival legislation. The paper examines maritime law to find useful principles that the archival field could draw on to mitigate some of these risks.

Keywords Cloud computing, Records management, Risk management, Laws

Paper type Case study

Introduction – the convergence of media and cloud technology

The riot that broke out in December 2013 in Little India, Singapore was an unprecedented event, as it was the first riot in Singapore after four decades. Members of the public who were in the vicinity took videos and photographs of the incident and

Part of the research for this paper was conducted as part of the author's responsibilities as a research assistant for the Records in the Cloud Project (www.recordsinthecloud.org). An earlier version of this paper was presented at the 17th Southeast Asia-Pacific Audio-Visual Archives Association (SEAPAVVA) Conference: Redefining the Audio-Visual Archives in the Digital Age, 27-31 May 2013 Bangkok, Thailand. The author wishes to thank Ms Irene Lim, Vice-President of SEAPAVVA and Principal Archivist, Audio-visual Archives from the National Archives of Singapore for her encouragement and Dr Luciana Duranti and Dr Donald Force for their comments on the earlier draft of the paper.

Records Management Journal
Vol. 24 No. 1, 2014
pp. 56-73

0956-5698
DOI 10.1108/RMJ-01-2014-0001

made them available in the cloud. Some citizen journalists claimed that audiovisual recordings produced by the public on the scene were circulated in the cloud much earlier than the multimedia content from mainstream media (Barimen, 2013; *The Independent*, 2013). The spontaneous citizen journalism, characterized by very timely audio visual recordings that are stored, disseminated, and consumed via cloud-based services, occurred alongside and independent of mainstream coverage. The affordance of cloud technology has changed the way in which individuals produce audiovisual materials. Broadcasting and production companies are also turning to the cloud to keep abreast with emerging technological trends and demands from consumers, who are keen to access audiovisual materials online through the use of smart phones and tablet devices.

In a general sense, the creation, transmission, and access of multimedia content in the cloud have become a pervasive global phenomenon, as revealed by a survey of media usage conducted in 56 countries in 2011. About 74 percent of the survey's respondents watched video online and 56 percent of respondents watched video on their mobile phone at least once a month (The Neilson Company, 2012, p. 4). Multimedia specialists and market observers thus spoke of the death of television, particularly since video can be accessed from various platforms, including mobile devices and tablets (Breitman *et al.*, 2010). Market observers also noted that consumers have "increasingly [turned a] cold shoulder to TV" and that the "battle for consumer's eyeballs" is now being fought on multiple platforms, since people have a choice of selecting a wide range of devices to view multimedia content (Broadcast Engineering, 2012). The increased market penetration of online multimedia content has resulted in media convergence, which is defined as the "digitization of media content, widespread availability of high-speed broadband connections, and proliferation of Internet enabled devices" (Media Convergence Review Panel, 2012, p. 2). In other words, media convergence involves an integration of multimedia data and the telecommunication, computing, and broadcasting industries (Hudson, 1997; Lee, 2001).

The phenomenon of creating, managing, distributing, and accessing audiovisual materials in the cloud raises questions regarding the ability of records-related legislation, which is defined as the legislation that "deals with records or information generally," to address issues concerning the ownership and control over data and records (Suderman *et al.*, 2005, p. 4). This paper aims to highlight some of the legal challenges in managing records in a cloud environment and to illustrate how records-related legislation, such as the copyright legislation, lags behind advances in technology. The paper also discusses issues of acquisition in relation to the cloud environment through an analysis of archival legislation. Audiovisual materials are used as an example, because of the complex interplay of potential benefits and risks that the cloud represents to the audiovisual industry. The potential scalability and cost-saving benefits of the cloud would be very prominent in the process of creating, transmitting, and storing large audiovisual materials. However, the cloud also introduces a number of legal risks with regards to intellectual rights, privacy, and jurisdiction; which can affect archival concerns such as chain of custody, authenticity, and trustworthiness.

The paper will draw on three cases from Canada, Australia, and Singapore to illustrate how the copyright legislation governs the ownership of audiovisual materials

within specific national boundaries. These three countries were selected as examples because, based on the Commonwealth framework, Canada represents North America, Australia represents the Pacific, and Singapore represents Asia. As more digital records are created in the cloud, questions arise about the applicability of a national law over the control, ownership and custody of data and records by content providers, cloud providers, and cloud users. The Singapore's Broadcasting (Class Licence) Notification (2013) also raises the issue of how the domestic law can regulate content within the geographical boundaries of Singapore, when news content and audiovisual materials can be hosted anywhere in the cloud. Finally, the paper will discuss aspects of archival legislation in Canada, Australia, and Singapore that are related to the acquisition of audiovisual materials in a networked, digital environment.

Moving multimedia content to the cloud – benefits and risks

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 provisioned rapidly and released with minimal management effort or service provider interaction" (Mell and Grance, 2011, p. 2). Essentially, cloud computing can be thought of not as a new technology *per se* but rather a new service and "business model" (Convery, 2010, p. 7). Cloud computing also involves "multiple stakeholders providing a "metered service at multiple granularities for a specified level of quality (of service)" (European Commission Information Society and Media, 2010, p. 8). There are various types of cloud computing services and business models offered to users, namely, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (National Institute of Standards and Technology, 2011, pp. 2-3).

One of the benefits of cloud computing is that the pricing model in the cloud environment offers broadcasting and entertainment companies the option of paying for services based on their usage level. The scalability of services offered by this model makes it possible for broadcasters to better respond to the changing needs of their customers (Accenture, 2009; Harshbarger, 2011). Broadcasters also have the option of using a cloud based workflow to better integrate their work processes, such as "delivering video from the field to studios or production centers for news, sports and other events using cellular networks" instead of via physical media (Broadcasting & Cable, 2011). Similarly, dissemination to consumers via the cloud, using a SaaS service such as Youtube, Netflix, or Vimeo, is less time-consuming and costly than producing and distributing physical media. In other words, a cloud based workflow allows broadcasters and producers to create, manage, and disseminate multimedia content on multiple platforms faster and more economically. From the perspective of the customers, the provision of cloud based television programmes provides them with the flexibility to view multimedia content without being tied to a physical television and a scheduled date and time. However, there are certain risks linked to the cloud-computing environment.

Ownership and custody of data risks

The ownership and custody of data are "principally unknown" in the cloud environment, due to the multi-tenancy model (European Commission Information

Society and Media, 2010). A cloud user may store materials in several data centers that may be in different locations and each managed by a different service provider. Conversely, an organization may own the hardware and software infrastructure, without offering cloud computing services to users (Hon *et al.*, 2012, p. 130). Unless expressly prohibited in the service level agreement, cloud service providers may subcontract part of their services or the content they are entrusted with to other providers, who may reside in multiple countries and jurisdictions. As noted by Mason and George (2011), "copies of data might not only be stored in an unknown number of computers across the globe, but there might be an unknown number of copies of the same digital document in different iterations across different jurisdictions" (p. 526). Furthermore, it is in the interest of cloud providers to create their own service level lock-in for their users, either via terms in the service level agreement or via proprietary technology. Therefore, cloud users may encounter challenges should they wish to export their data (Blair, 2010, p. HT4). While most users may not be concerned about the physical location of digital bits and bytes, this issue is of interest to records professionals and archivists, who are responsible for identifying and exporting "all the digital components of each record and apply(ing) the appropriate software to each component to reproduce the record" (Duranti and Thibodeau, 2006, p. 19)[1]. The physical location of a digital record can also be of interest in the event that an authentic copy of a record must be presented in court. The outsourcing of data raises questions about the trustworthiness of the records in terms of accuracy, reliability, and authenticity over time. Furthermore, archivists are faced with the challenge of acquiring the metadata associated with the audiovisual materials by the service provider(s).

Transborder data flow risks

Transborder data flow is defined as the "movement across national boundaries of computerized, machine-readable data for processing, storage, or retrieval" (United Nations Center on Transnational Corporations, 1982, p. 8). Although this definition was used by the United Nations in 1982, well before the advent of cloud computing, it is still relevant in a cloud environment, as it conveys the continuous movement of data across national boundaries. In fact, Industry Canada's Report on the Trilateral Committee on Transborder Data Flows (2010) highlighted that while the concept has not changed since the 1980s, "technological advances and ever-increasing efficiencies applied to existing technologies have expanded the scope of transborder data flows." There are multiple juridical systems to be taken into consideration in a cloud computing environment: the legal system of the cloud service provider, the legal system of the cloud customer, the legal system of the place where the data centers storing the data/records are located, and the legal system of the individuals to which the data/records are related (McCullagh, 2012). This involvement of multiple juridical systems means that in case of litigation, it may be very difficult to establish the relevant jurisdiction because "nationality is not a quality attributable to data" but it is "an attribute to an individual person" (Poullet *et al.*, 2010, p. 9)[2]. Claims of breaches in privacy, data protection, and copyright could be extremely difficult to resolve (Weber, 2013).

It may also be difficult to establish how national laws apply to specific bytes of data, which may flow across a number of jurisdictions in a very short time span. A 2011

study that reviewed the contractual clauses offered by cloud service providers found that most of the clauses contravened European intellectual property and privacy laws. This is to be expected, because a large number of cloud computing contracts are based on American law (Union des consommateurs, 2011, pp. 18-19). Although the USA signed a safe harbor agreement with the European Union (EU) to regulate the manner in which US companies comply with the EU Directive on Data Protection, there are "serious doubts as to the adequacy of the Safe Harbor Principles with the privacy protection standards of EU law" (Weber, 2013, p. 10)[3]. American companies can self-certify that they abide by the Safe Harbor privacy principles, but the onus is still on the European Union companies that are exporting data to "obtain evidence that the Safe Harbor self-certification exists and request evidence demonstrating that their principles are complied with" (European Union Data Protection Working Party, 2012, p. 17).

Although the cloud computing environment facilitates transborder data flow across countries, records-related legislation is still largely based on the principle of territoriality. The territoriality principle is one of the basic jurisdictional principles, and states that any act committed in the physical territory of a jurisdiction will be tried under the laws of that jurisdiction (Ryngaert, 2008). The recent changes to the licensing rules stipulated in the Broadcasting (Class Licence) Notification (c. 28. 2013) in Singapore is an example of how countries still subscribe to the principle of territoriality, which conflicts with the borderless nature of the cloud. The licensing rules require all online news sites to be individually licensed if they publish at least one article per week on Singapore's current affairs over a duration of two months and if the site is visited by at least 50,000 unique IP addresses from Singapore per month on average over a two-month period. With the increasing adoption of cloud services by the online news and broadcasting industries, such a regulatory approach to content management raises questions about the regulation of content that has relevance to Singapore but exists beyond Singapore's national border. The Asia Internet Coalition has argued against such a regulatory framework, as intermediaries, such as cloud service providers, are placed in the "untenable position of proactively policing (user-generated) content" (Asia Internet Coalition, 14 June 2013)[4].

Legal cases related to the copyright of audiovisual materials in the cloud

The Supreme Court of Canada case involving the *Society of Composers, Authors and Music Publishers of Canada (SOCAN)* vs *Canadian Assn. of Internet Providers (CAIP)* illustrates the difficulties in deciding which legislation apply in a cloud computing environment. This is because the prevalent law is always the domestic law, which is based on territorial boundaries of a nation, whereas the cloud computing environment is not confined to a specific geographical boundary (Leong and Saw, 2007, p. 40). The central issues of this case are whether musical composers and artists in Canada, represented by SOCAN, should be compensated for the download of their artistic content in a country outside Canada via the Internet, and, if so, who should compensate them. SOCAN wanted to "impose liability for royalties on the various Internet Service Providers located in Canada irrespective of where the transmission originates" (*SOCAN* vs *CAIP*, 2004, para 3). However, the Canadian Internet Service Providers (ISPs) argued that they are only the conduit of content and "do not control the message" (*SOCAN* vs *CAIP,* 2004, para 4). The Federal Court of Appeal determined

that the ISPs are absolved of liability for information (music) that merely "pass(es) through" their system (*SOCAN* vs *CAIP,* 2004, para 23). Moreover, the Court stated that the "knowledge that someone might be using content-neutral technology to violate copyright" is not sufficient to constitute an authorization or approval of such copyright violation (*SOCAN* vs *CAIP,* 2004, p. 4). Even if the music were stored in a cache, the act of storage would not be considered more than the simple relaying of information if the cache was generated for purely technical purposes, such as reducing transmission delays. However, the Court also noted that an ISP that refuses to remove copyrighted material from its server after being given reasonable opportunity to do so, such as being served a notice of infringing content, can be held liable.

The *SOCAN* vs *CAIP* case is based on the old copyright law in Canada, before the amendment in 2012[5]. However, this case is still relevant, because it illustrates the challenges involved in the application of a law that is based on a territoriality principle to the cloud, which operates in a borderless environment. As one of the judges argued, the "copyright law respects the territoriality principle, reflecting the implementation of a web of interlinking international treaties," such as the World Intellectual Property Organization Copyright Treaty (1996), and "Parliament does not intend the Act to operate beyond Canada's borders" (*SOCAN* vs *CAIP,* 2004, paras 56 and 148). The majority of the judges present in the case ruled that the definition for transmissions occurring in Canada, and the liability for such transmissions, should not be limited to "transmission (originating) from a server located in Canada" alone (*SOCAN* vs *CAIP,* 2004, para 105). Conversely, a content provider does not become immune from copyright liability in Canada simply by employing a host server outside of the country. In order for the Copyright Act in Canada to apply to the transmission and communication of content via the Internet, the Court decided that there must be "real and substantial connection to Canada" (*SOCAN* vs *CAIP,* 2004, para 60). If such connections are determined to exist, Canada could exercise "copyright jurisdiction" for transmissions that originate from Canada as well as transmissions that come from other countries and are received in Canada (*SOCAN* vs *CAIP,* 2004, p. 3). Such a ruling means that the court has to decide on a combination of factors, such as the sites of the content provider, the host server, the user, and any other intermediaries and to determine on a case by case basis whether there is a "real and substantial connection to Canada" (*SOCAN* vs *CAIP,* 2004, p. 3). The court also ruled that as long as service providers confine their roles to being intermediaries and do not actively participate in the "content of the communication," such as providing links that include copyrighted artistic content, they are not liable for copyright infringement (*SOCAN* vs *CAIP,* 2004, p. 4 and para 32).

While it may be debatable when an Internet Service Provider (ISP) simply serves as a "conduit (of) communications" for the general public, the broadcasting and telecommunication industries tend to have a specific target audience in mind (*SOCAN* vs *CAIP,* 2004, para 32). In order to increase viewership, these industries have utilised cloud storage facilities to allow users to record and to access free-to-air TV. However, current legislative provisions are not robust enough to deal with the "potential for new and emerging cloud computing to infringe copyright, or enable their customers to infringe copyright" (Australian Law Reform Commission, 2012, pp. 26-27). This is illustrated by comparing two similar cases, one in Australia and one in Singapore, that involved cloud-based digital recording, storage, and streaming of free-to-air TV

signals: the *National League Investments Pty Limited* vs *Singtel Optus Pty Ltd* case in Australia (2012, FCAFC 59) and the *RecordTV Pte Ltd* vs *MediaCorp TV Singapore Pte Ltd* case in Singapore (2011, SLR 830).

The *National League Investments Pty Limited* vs *Singtel Optus Pty Ltd* case involved the use of a subscription service offered by Singtel Optus Pty Ltd to schedule, record, and play back free-to-air television broadcasts on the subscribers' mobile devices, tablets, and personal computers, within a limited timeframe. The system developed by Singtel Optus Pty Ltd involved sending streams of data from five main cities in Australia to a data center in Sydney. In the process of copying the selected broadcast, the system would make four copies in its cloud storage system, so that the subscribers could select their desired device to watch the programme. The case's main issue is whether the act of recording and storing the television broadcast of the football games in the cloud is considered an infringement of the Copyright Act in Australia. The case resulted in an initial ruling in late 2011 and an appeal ruling in April 2012. In the appeal ruling, the Federal Court of Australia asserted that Singtel Optus Pty Ltd and the subscriber made a copy of the recording and were "jointly and severally responsible for the act of copying" (*National League Investments Pty Limited* vs *Singtel Pty Ltd*, 2012, para 4). The court also ruled that Singtel Optus' act of providing such a subscription service did not constitute an exemption under the Australian Copyright Act. This judgement overturned the initial 2011 ruling, where it was decided that the subscriber was the one wholly responsible for copying the programme.

The *RecordTV Pte Ltd* vs *MediaCorp TV Singapore Pte Ltd* case in Singapore also involved a cloud-based subscription service offered by RecordTV Pte Ltd, which provided nearly identical functionalities to the one offered by Singtel Optus Pty Ltd in the Australian case: the ability to schedule, record, and playback free-to-air television broadcasts on multiple devices. Similarly, the issue in contention was whether the act of recording and storing MediaCorp's television broadcasts in the cloud is considered an infringement under Singapore's copyright law. This case resulted in an initial ruling in 2009 and an appeal ruling in late 2010. However, this case progressed and concluded very differently from the Optus case. In the initial ruling, the judge determined that RecordTV did the copying, and thus violated MediaCorp's copyright. The Singapore Court of Appeal overturned the initial ruling and determined that the responsibility for copying the TV shows, storing them in the cloud, and streaming them later on lay with the subscribers of RecordTV, thus absolving the cloud service provider of copyright infringement. The differing interpretations of similar points between the two cases in Australia and Singapore, and the disagreement even among the judges within each of these two cases, raise several important issues for archivists and records professionals.

Relevant issues for archivists and record professionals

First, cloud technology brings the need for clarifications of legislation, such as copyright laws, which can affect records management and the archives. Most legislators stress the need for the law to be technological neutral and not partial to "any particular communications technology, business model or delivery method for content services". However, in reality, the language of the legislation, as well as the way that this language can be applied in real world situations may sometimes be too vague and subjected to a number of interpretations by the relevant parties (Commonwealth of Australia, 2012, p. xvi). An example of this is the disagreement between the judges in

the Optus case with regard to the act of "making a copy" using a cloud storage facility (*National League Investments Pty Limited* vs *Singtel Pty Ltd*, 2012, para 47). The judge in the initial ruling viewed this act as being no different from the act of copying from a video cassette recorder in the analogue environment, which would place the liability on the subscribers. However, this interpretation was overturned completely in the appeal ruling. The liability was shifted to the cloud service provider Optus, with the reasoning that, at all times in the Optus-subscribers relationship, Optus retained the "possession, ownership, and control of the physical copies" which were created and stored on Optus's cloud-based system (*National League Investments Pty Limited* vs *Singtel Pty Ltd*, 2012, para 52). In emphasis, the judge in the appeal ruling asserted that "no principle of technological neutrality can overcome what is the clear and limited legislative purpose" with regard to Fair Use and other copyright exceptions (*National League Investments Pty Limited* vs *Singtel Pty Ltd*, 2012, para 96).[6]

Second, the affordance of the cloud environment has made it easy to produce and disseminate multiple copies of a given material. Increasingly, the courts will have to deliberate on the activities that consumers and service providers conducted within a technological context, and not only those activities of the original creators and distributors of audiovisual materials, so as to decide on the party responsible in making available the copies that constitute an infringement of the Copyright Act. The difficulties in applying legal principles and interpreting legal concepts highlighted in the three court cases serve to reaffirm that the law is often unable to keep up with the changes in technology. In fact, the Singapore Court of Appeal in the *RecordTV Pte Ltd* vs *MediaCorp TV Singapore Pte Ltd* case claimed that the services provided by RecordTV was "simply a technological advance that is not addressed by the Copyright Act (in Singapore)" (*RecordTV Pte Ltd* vs *MediaCorp TV Singapore Pte Ltd*, 2010, para 71). Archivists and records professionals can benefit from being cognizant of the legal risks surrounding emerging technological trends, such as the cloud, when developing record management programmes and policies or when acquiring and preserving records, so that they may take into account the potential for inadequate legislative provisions or differing interpretations of similar issues across jurisdictions and over time.

Potential impact of keeping audiovisual materials in the cloud on archival legislation

Audiovisual archivists working in their respective national archives derive the mandate to acquire audiovisual materials from the archival legislation. The archival legislation or archives-enabling legislation is one that "enables (brings into existence and assigns responsibilities) an archival institution or repository" (Suderman *et al.*, 2005, p. 4). This section discusses the potential impact of the models for audiovisual materials production, distribution, and access facilitated by cloud technology on archival legislation, using Canada, Australia, and Singapore as examples.

Both *Library and Archives Canada (LAC) Act* (S.C. 2004) and the *National Library Board (NLB) Act* (c. 197. 2012) in Singapore have a consolidated mandate for the acquisition of published and unpublished materials[7]. Under the *LAC Act* (S.C. 2004), the legal deposit clause enables the institution to acquire publications, which includes audiovisual recordings. Section 10 of the *LAC Act* (S.C. 2004) states that "subject to the regulations, the publisher who makes a publication available in Canada shall, at the

publisher's own expense, provide two copies of the publication to the Librarian and Archivist." This illustrates that as long as an audiovisual recording is "made available in Canada" for access, copies of the materials should be deposited in LAC. The clause does not state the manner in which the audiovisual recording is "made available in Canada", and this may be interpreted to include not only recordings disseminated through broadcasting stations and production companies within Canada but also recordings hosted on servers outside Canada and disseminated to the public via cloud services. In contrast, the legal deposit component of the *NLB Act* (c. 197. 2012) in Singapore confines the acquisition to materials published within the geographic boundaries of the country. Section 10(1) of the *NLB Act* (c. 197. 2012) states that the "publisher of every library material published in Singapore shall, at the publisher's own expense and within four weeks after the date of publication, deposit two copies (except as otherwise provided by regulations) of that library material with the Board at such place as the Board may determine." The phrase "published in (a country)" reflects the mindset of an analogue environment, where the publication and distribution of library materials can be confined to a specific geographical space. Such a condition no longer holds true in a cloud-computing environment as broadcasters and producers may create, store, and distribute Singapore-related materials outside the physical geography of the country.

Fortunately, the provisions for "obtaining archival quality recordings for preservation purposes" in the *LAC Act* (S.C. 2004) and the "deposit of certain recordings" provisions in the *NLB Act* (c. 197. 2012) enable the respective archival institutions to acquire audiovisual recordings that are broadcast to the public in Canada or Singapore, but are not necessarily published within Canada or Singapore. For example, Section 11 of the *LAC Act* (S.C. 2004) states that the Librarian and the Archivist can request that a person give a copy of a recording, should the record be "made available to the public in Canada" and have "historical or archival value" and in the "form and quality that the Librarian and Archivist determines is suitable for archival purposes." Similarly, Section 14I of the *NLB Act* (c. 197. 2012) states that "the producer or distributor of a recording shall, within six months after a request in writing is made by the Board, provide without charge the Board with a copy of the recording in such form as may be specified in the request." Even before the legislative transfer of the National Archives of Singapore (NAS) to the NLB, the archives had signed agreements with various broadcasting stations and non-governmental organizations like the Asia Film Archives to preserve audiovisual records[8]. Such administrative agreements often work in tandem with the archival legislation to complement the mandate of the archives to acquire and preserve recordings. Nevertheless, the integrated archives and library legislation in Singapore needs to be harmonised and updated to reflect the changing nature of the cloud environment, where film producers and artists may disseminate multimedia content in a distributed environment outside of Singapore.

Unlike LAC and the NAS, the National Archives of Australia (NAA) does not acquire private records and non-Commonwealth audiovisual materials[9]. Compared to the archival legislation of Canada and Singapore, Australian archival legislation does not have a specific clause addressing the acquisition of audiovisual recordings. Section 5 of the *Archives Act* (Act No. 79.1993) in Australia states the mandate and functions of the institution. The functions include to "determine the material that constitutes the

archival resources of the Commonwealth" and "to have the care and management of Commonwealth records" and "to seek, to obtain and to have the care and management of, material (including Commonwealth records) not in the custody of Commonwealth institution, that forms part of the archival resources of the Commonwealth and, in the opinion of the Director-General, ought to be in the care of the Archives" (Act No. 79. 1993, Section 5). In other words, Commonwealth records, which include audiovisual recordings, come under the acquisition mandate of NAA. These audiovisual records include records transferred from government agencies and the government broadcasting agencies, such as the Australian Broadcasting Corporation (Somes, 2012). The Archives Act (Act No. 79. 1983) in Australia defines Commonwealth record in terms of property. A Commonwealth record means "a record that is the property of the Commonwealth or of a Commonwealth institution" (Act No. 79.1993, Section 3). A property based definition, which is closely aligned with the concept of possession and ownership, can potentially be an issue in a cloud environment. The ease of use of cloud services makes it possible for individuals from various government agencies to store audiovisual records relating to the activities of their agency directly onto a public cloud, thereby bypassing the traditional chain of custody of records from government agencies to an archival institution. Moreover, SaaS services hosting audiovisual content, such as Youtube and Vimeo, state that they are granted a "a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the Content in connection with the Service and YouTube's (and its successors' and affiliates') business . . . in any media formats and through any media channels"[10]. Content providers that upload audiovisual materials to these cloud services also "hereby grant each user of the Service a non-exclusive license to access your Content through the Service, and to use, reproduce, distribute, display and perform such Content as permitted through the functionality of the Service"[10]. The terms of service of Youtube (Vimeo's also contains similar clauses)[11] means that audiovisual records can potentially be created, copied, and reproduced in the cloud and without the archives acquiring and preserving these records under their custody. However, the *Archives Act* of Australia (Act No. 79.1983) has provisions that reduce the risk of potential loss of records and facilitate their acquisition and preservation by the NAA. Section 24 of the Australian *Archives Act* (Act No. 79.1983) expressly states that "a person must not engage in conduct that results in the transfer of the custody or ownership of a Commonwealth record." The NAA's policy also stipulates that an agency is required to use a cloud service that provides adequate protection to Commonwealth records (National Archives of Australia, 2011). Archivists, however, still need to be mindful on how the existing definitions and clauses in their archival legislation might be challenged, due to changes in the recordkeeping environment and the individual behavior of record creators.

Applicability of maritime law to records in the cloud

The legal cases and some of the archival legislation discussed in this paper are based on the territoriality concept, which, by definition, implies that any action that is committed can be neatly associated with one physical location in one jurisdiction through the actor who carries it out. This does not adequately address the management and preservation of records in a global cloud environment. Such an environment is not

one of "nations, states, and provinces" but involves the movement of data/records across national boundaries (Burnstein, 1996, p. 81). In effect, the management and preservation of records in the cloud environment not only involves the jurisdiction of data and records within a state's territory and has effects within a state's jurisdiction (territoriality) but also has extraterritorial implications. Extraterritoriality is the "application of one country's laws to persons, conduct or relationships outside of that country" (Clopton, 2013, p. 217). One possible way of reconciling both the territorial and extraterritorial implications of managing records and data is to examine existing supra-national legislation, such as international maritime laws, in order to develop a model law for the cloud environment. A model law is defined by the United Nations Commission for International Trade Law as a "suggested pattern for law-makers in national governments to consider adopting as part of their domestic legislation" (United Nations Commission on International Trade Law, n.d.). The development of a model law based on the principles of maritime law is timely, because cloud service providers, such as Google, have obtained a patent to build data centers on ships, which can be stationed in international waters (*Daily Mail*, 2013; Miller, 2008).

One of the principles of maritime law is that it is "not the law of a particular country but is part of the law of nations" (Burnstein, 1996, p. 104). The United Nations Convention on the Law of the Sea makes a clear distinction between a state's territorial waters and those of the high seas, and it is the latter concept that can be further explored and applied to the cloud-computing environment. The global cloud environment, just like the high seas, may require a "balance between a state's ability to regulate the cloud and an overseeing international authority" (Narayanan, 2012, p. 808). Historically, under maritime international law, the legal status of a ship was dependent on its flag state (Anderson, 1998). This means that ships could choose to register under a particular flag state but could not indiscriminately change its flag state. The main responsibility of a port is to check the registration status of the ship and to inform the flag state of any problems or issues. Over time, this led to a situation of "flag of convenience" as ships chose to register in countries that did not have the resources to effectively monitor the safety of the ships (Anderson, 1998, p. 561). Consequently, there was a gradual shift towards greater control by port states (where the ships come into port) to ensure that ships complied with international maritime agreements. Similarly, the sovereignty of coastal states (where the ships pass by) is limited to an area of 12 nautical miles over sea and air space, and foreign ships have to abide by coastal state laws, such as those relating to sea-lanes and traffic navigation, while travelling in this area. The UK was one the first countries to publish a list of "ships of shame" with the names of vessels that did not pass port state inspections (Anderson, 1998, p. 563). The international maritime community has also produced a whitelist of ships, and ships that are not identified in the list are subjected to greater port state inspections (Anderson, 1998, p. 563). Finally, because "the ownership and management chain surrounding any ship can embrace many countries [. . .] often far from the country of registry," the International Maritime Organization, a United Nations specialized agency, was formed in order to develop "international standards to regulate shipping – which can be adopted and accepted by all" (International Maritime Organization, n.d.).

An analogy to the cloud environment would have cloud service providers as the ships, the jurisdictions where service providers incorporate their business as the flag states, and the jurisdictions where the service providers have servers as the port states.

The concept of coastal state would apply to the jurisdictions through which a packet of data may pass but where it would not be stored. The nation states where service providers may host the data (the port states of the cloud) can potentially issue policies, standards, and best practices for these service providers to abide by. There could be a whitelist of cloud service providers who meet internationally agreed standards on various aspects of data/records control, such as data security, ownership of data, and business continuity. At the same time, one could also envision a parallel list of "ships of shame" which would show the events related to and the cloud service providers responsible for specific breaches of data privacy and data loss.

There are, however, certain limits to how much the reasoning process of maritime law may be applied to the cloud environment. The concept of coastal state is very difficult to translate directly into the cloud environment. A packet of data may be transmitted through multiple jurisdictions before reaching its destination, analogous to a ship passing through multiple physical coastal states without going into port. However, a data transmission can also involve temporary copies, which can be created in the cyber "coastal states" in the usual operation of a cloud service provider, such as for temporary storage (caching) to reduce transmission delay. These temporary copies of transmitted data can be intercepted or even tampered with. As noted by Hildebrandt (2013), "territorialization of cyberspaces easily generates cross-border communication, commerce and crime, situating the same action seamlessly in different territories, both online and offline" (p. 203). Because a packet of data in a cloud service may both be transmitted across multiple jurisdictions and temporarily stored in multiple jurisdictions, the cloud service provider "ship" would appear to exist in multiple coastal states at the same time. However, this problem may be resolved by applying another concept in maritime law. The "ship" can also be said to be on the high seas at any given time. In this interpretation, the cloud service provider "ship" would not necessarily be subjected to the local laws of any particular jurisdiction, but there would be a need for an international, non-profit regulatory body for cloud services, which would be the equivalent of the International Maritime Organization. This hypothetical organization would be responsible for developing model laws to mitigate the legal risks affecting records (including audiovisual) in the cloud environment. For example, the model law could suggest that cloud service providers need to state in their service-level agreement the locations of servers that data may pass through and in which data may be stored, as well as whether a part of the service is sub-contracted to another cloud service provider. This example is similar to the inspection record of a ship as it passes through multiple port states, and would allow the users of cloud services to make an informed decision regarding the transborder data flow risks that they are willing to take.

The creation of model laws for records in the cloud will also facilitate a "harmonization of provisions related to the proper control of our digital heritage from the moment of creation throughout its life-cycle" which can be "adapted to each national and cultural context" (Duranti, 2012, p. 9). The model laws can also include the roles and responsibilities of the cloud service providers and users regarding the creation and management of digital assets. The legal and policy issues governing the management of records in the cloud are part of a four-year multidisciplinary project led by the School of Library, Archival, and Information Studies at the University of British Columbia. One of the objectives of the project is to "determine what policies and

procedures a (service) provider should have in place for fully implementing the records/archives management regime of the organization outsourcing the records, for responding promptly to its needs, and for detecting, identifying, analyzing and responding to incidents"[12].

Conclusion and future works

The law is often unable to keep up with the advances made in technology, and a law that was "previously unobjectionable (can) become subject to criticisms" (Moses, 2003, p. 396). Audiovisual archivists and information professionals cannot assume that the current legislative provisions on copyright and archival acquisition and preservation, which were developed in an analogue world, would be adequate to address issues relating to the trustworthiness of records in an environment that is increasingly connected and distributed across jurisdictions. Cloud-based technology and workflows promise cost saving and scalability for the creation, distribution, and storage of audiovisual content, but this promise also comes with new legal challenges and risks. Some of these records-related legal risks are discussed in this paper: risks related to the ownership and custody of data, risks due to transborder data flow, and risks due to the vague and differing interpretations of legal concepts related to audiovisual materials in the cloud. It is time for archivists and information professionals to become engaged with the larger internet community, comprising cloud providers, cloud users, legal practitioners, information security experts, and policy makers, to develop international model laws or standards and codes of practices governing the creation, use, and dissemination of records and digital materials in the cloud.

There is also a need to further investigate the concepts of extraterritoriality in the digital environment to examine how these can be applied to the management and preservation of records in the cloud. Directions of future research on extraterritoriality may be inspired by the reasoning process and specific best practices within various types of transborder laws – such as maritime laws, aero-spatial laws, international trade laws, and international treaties on cybercrime.

Notes

1. A digital component is a "digital object that is part of one or more digital documents, and the metadata necessary to order, structure or manifest its content and form, requiring a given preservation action", See InterPARES 3 Terminology Database, available at: www.interpares.org/ip3/ip3_terminology_db.cfm?term = 213 (last accessed 15 December 2013). An audiovisual record may contain a number of digital components including audio, image, and text. A manifested record is the "visualization or materialization of the record in a form suitable for presentation to a person or another system" (Duranti and Thibodeau, 2006, p. 51).
2. One of the precepts of international law is the principle of nationality, which is that "states may assert jurisdiction over the acts of their nationals, wherever the act might take place" (Currie and Scassa, 2011, p. 5).
3. In 2012, the European Union proposed a draft data protection regulation to replace the current directive in order to better meet the challenges in an online environment and to strengthen citizens' data protection rights. See www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform (last accessed 15 December 2013).

4. Letter from Dr John Ure, Executive Director, Asia Internet Coalition to Singapore's Minister for Communications and Information, 14 June 2013, available at: www.asiainternetcoalition.org/wp-content/uploads/2013/11/AIC-Open-Letter-to-Singapores-MIC-on-Government%E2%80%99s-new-licensing-framework-for-online-news-sites.pdf (last accessed 15 December 2013).
5. The Copyright Modernization Act was enacted in 2012. One of the key components of the Act is that Parliament should revisit the Act every five years. This is not only a recognition of the "important role that modern and updated copyright laws play in our economy" but is also a recognition that laws can become obsolete over time with technological advances and thus need to be reviewed. See http://news.gc.ca/web/article-eng.do?nid = 683909 (last accessed 15 December 2013).
6. Australia is currently reviewing their Copyright Act. As part of the consultation process, the Australian Law Reform Commission has issued a Copyright and Digital Economy Issues Paper (August 2012) and Copyright and Digital Economy Discussion Paper (May 2013) in order to invite comments from the public. See www.copyright.com.au/get-information/alrc-inquiry/alrc-issues-paper (last accessed 15 December 2013).
7. Although the Acts provide a consolidated mandate, there are differences in the reporting structure of the archival institutions. In Canada, the former National Library and the National Archives merged in 2004 to form an entity known as the Library and Archives Canada (LAC). In Singapore, the National Archives of Singapore, which was previously a department under the National Heritage Board, was legislatively transferred to the National Library Board in 2012. The current National Library Board Act (2012) includes the archives component that was previously under the National Heritage Board Act (1993). It is notable that that the archival legislation in Canada has the word archives in the title of legislation, but this is absent in Singapore. The title of the archival legislation by itself indirectly reflects the current administrative structure of the archival institutions in these two countries.
8. The NAS and the Asian Film Archives signed a Memorandum of Understanding in 2005 to acquire and preserve Asian film heritage. See www.asianfilmarchive.org/About/Press/MouNas.aspx (last accessed 22 October 2013). Subsequently, in 2007, the National Library Board signed a separate Memorandum of Understanding with the Asia Film Archives to establish a "reference library collection of films made by Singaporean and Asian film makers." See http://newsletter.nlb.gov.sg/back_feb_mar07/features/active/index02.asp (last accessed 15 December 2013). Currently, the NLB in Singapore is examining issues relating to synergies and alignment of processes and services between the archives and the library, which would have an impact on the acquisition and preservation of audiovisual recordings, in published and unpublished form.
9. The NAA does collect the personal records of politicians and senior public servants. Their collecting policy states that "The National Archives collects official Commonwealth government records, and the personal records of governors-general, prime ministers, ministers, federal and High Court judges and some senior Commonwealth public servants, whose records complement the official record." See www.naa.gov.au/collection/fact-sheets/fs218.aspx (last accessed 15 December 2013).
10. Youtube's terms of service, section 6c. See www.youtube.com/static?template = terms (last accessed 29 December 2013).
11. Vimeo's terms of service, section 9. See http://vimeo.com/terms#license (last accessed 29 December 2013).
12. See research objectives from the Records in the Cloud web site: www.recordsinthecloud.org/ritc/home (last accessed 15 December 2013).

References

Accenture Media and Entertainment (2009), "Not just blue sky thinking: Cloud computing and the digital supply chain", available at: www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Cloud_computing_and_the_digital_supply_chain.pdf (accessed 15 December, 2013).

Anderson, D. (1998), "Roles of flag states, port states, coastal states and international organisations in the enforcement of international rules and standards governing the safety of navigation and the prevention of pollution from ships under the UN convention on the law of the sea and other international agreements, the MINDEF-SILS conference papers", *Singapore Journal of International & Comparative Law*, Vol. 2, pp. 557-578.

Australian Law Reform Commission (2012), "Copyright and the digital economy: issues paper", available at: www.alrc.gov.au.ezproxy.library.ubc.ca/publications/copyright-ip42 (accessed 15 December, 2013).

Barimen, A. (2013), "Media failure: the Little India riot", *All About Digital and Social Media*, December 10, available at: www.skribeproductions.com/2013/12/10/media-failure-the-little-india-riot/ (accessed December, 15, 2013).

Blair, B.T. (2010), "Governance for protecting information in the cloud. ARMA's international hot topic – making the jump to the cloud? How to manage information governance challenges", ARMA International, Overland Park, KS, pp. HT1-HT4, available at: www.arma.org/docs/hot-topic/hottopic910.pdf (accessed December 15, 2013).

Breitman, K., Endler, M., Pereira, R. and Azambuja, M. (2010), "When TV dies, will it go to the cloud?", *Computer*, Vol. 43 No. 4, pp. 81-83.

Broadcasting & Cable (2011), "Beyond the TV: multiplatform and cloud-based tech", *Broadcasting and Cable*, September 5, available at: http://connection.ebscohost.com/c/articles/66211228/beyond-tv-multiplatform-cloud-based-tech (accessed December 15, 2013).

Broadcast Engineering (2012), "Consumers increasingly turn cold shoulder to TV as love affair with tablets, smartphone intensifies, says survey", *Broadcast Engineering*, January 11, available at: http://broadcastengineering.com/ott/consumers-increasingly-turn-cold-shoulder-tv-love-affair-tablets-smartphones-intensifies-says-su (accessed December 15, 2013).

Broadcasting (Class License) Notification Act, Statutes of Singapore (2013), *Broadcasting (Class License) Notification Act, Statutes of Singapore*, Singapore web site: tatutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A"a5408556-62b8-49ca-b697-0f292996f7d5"%20Status%3Ainforce%20Depth%3A0;rec=0;whole=yes#xv- (retrieved from Attorney-General's Chambers).

Burnstein, M.R. (1996), "Conflicts on the net: choice of law in transnational cyberspace notes", *Vanderbilt Journal of Transnational Law*, Vol. 29 No. 1, pp. 75-116.

Clopton, Z. (2013), "Extraterritoriality and extranationality: a comparative study", *Duke Journal of Comparative and International Law*, Vol. 23, pp. 217-265.

Commonwealth of Australia (2012), "Convergence review final report", Commonwealth of Australia, Canberra, available at: www.dbcde.gov.au/__data/assets/ pdf_file/0007/147733/Convergence_Review_Final_Report.pdf (accessed December 15, 2013).

Convery, N. (2010), "Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud", Department of Information Studies, Aberystwyth University, Ceredigion and The Archives and Records Association UK and Ireland.

Currie, R.J. and Scassa, T. (2011), "New first principles? Assessing the internet's challenges to jurisdiction", *Georgetown Journal of International Law*, Vol. 42 No. 4, pp. 1017-1082.

Daily Mail (2013), "Is Google building a Navy? Internet giant launches second 'floating data centre'", *Daily Mail*, October 30, available at: www.dailymail.co.uk/news/article-2479299/Second-floating-Google-data-center-spotted-Maine.html (accessed December 15, 2013).

Duranti, L. (2012), "Keynote: Trust and conflicting rights in the digital environment", *Proceedings of the Memory of the World in the Digital Age: Digitization and Preservation. An International Conference on Permanent Access to Digital Documentary Heritage, 26-28 September 2012, Vancouver, BC*, available at: www.unesco.org/new/en/communication-and-information/events/calendar-of-events/events-websites/the-memory-of-the-world-in-the-digital-age-digitization-and-preservation/ (accessed March 25, 2012).

Duranti, L. and Thibodeau, K. (2006), "The concept of record in interactive, experiential and dynamic environments: the view of InterPARES", *Archival Science*, Vol. 6 No. 1, pp. 13-68.

European Commission Information Society and Media (2010), "The future of cloud computing – opportunities for European cloud computing beyond 2010", available at: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf (accessed December 15, 2013).

European Union Data Protection Working Party (2012), "Opinion 05/20 on cloud computing", available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0846:FIN:EN:PDF (accessed December 15, 2013).

Harshbarger, J.A. (2011), "Cloud computing providers and data security law: building trust with United States companies", *Journal of Technology Law & Policy*, Vol. 16, pp. 229-256.

Hildebrandt, M. (2013), "Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace", *University of Toronto Law Journal*, Vol. 63 No. 2, pp. 196-224.

Hon, W.K., Hörnle, J. and 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", *International Review of Law, Computers & Technology*, Vol. 26 Nos 2-3, pp. 129-164.

Hudson, H. (1997), *Global Connections: International Telecommunications Infrastructure and Policy*, Van Nostrand Reinhold, New York, NY.

Independent (The) (2013), "Little India riot: where were ST, Today, MyPaper and BT?", December 10, available at: http://theindependent.sg/little-india-riot-where-were-st-today-mypaper-and-bt/ (accessed 15 December, 2013).

Industry Canada (2010), *Report on the Trilateral Committee on Transborder Data Flows – North American Leaders Summit*, 4 May, available at: www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00546.html#s2 (accessed 15 December, 2013).

International Maritime Organization (n.d.), "Introduction", available at: www.imo.org/About/Pages/Default.aspx (accessed 15 December 2013.

Lee, A. (2001), "Convergence in telecom, broadcasting and IT: a comparative analysis of regulatory approaches in Malaysia, Hong Kong and Singapore", *Singapore Journal of International & Comparative Law*, Vol. 5, pp. 674-695.

Leong, S.H.S. and Saw, C.L. (2007), "Copyright infringement in a borderless world – does territoriality matter – *Society of Composers, Authors and Music Publishers of Canada vs Canadian Association of Internet Providers* [2004] 2 SCR 427", *International Journal of Law and Information Technology*, Vol. 15, pp. 38-53.

McCullagh, K. (2012), "Response to EU commission public consultation on cloud computing", *European Journal of Law and Technology*, Vol. 3 No. 1, pp. 1-5.

Mason, S. and George, E. (2011), "Digital evidence and 'cloud' computing", *Computer Law & Security Review*, Vol. 27 No. 5, pp. 524-528.

Media Convergence Review Panel (2012), "Media convergence review final report", Media Convergence Review Panel, Singapore, available at: www.mda.gov.sg/Reports/Documents/Media%20Convergence%20Review%20Final%20Report.pdf (accessed December 15, 2013).

Mell, P. and Grance, T. (2011), "The NIST definition of cloud computing – recommendations of the National Institute of Standards and Technology", National Institute of Standards and Technology, Gaithersburg, available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (accessed December 15, 2013).

Miller, R. (2008), "Google planning off-shore data barges", *Data Center Knowledge*, September 6, available at: www.datacenterknowledge.com/archives/2008/09/06/google-planning-offshore-data-barges/ (accessed December 15, 2013).

Moses, L.B. (2003), "Adapting the law to technological change: a comparison of common law and legislation", *University of New South Wales Law Journal*, Vol. 26 No. 2, pp. 394-417.

Narayanan, V. (2012), "Harnessing the cloud: international law implications of cloud-computing", *Chicago Journal of International Law*, Vol. 12 No. 2, pp. 783-809, available at: http://search.proquest.com.ezproxy.library.ubc.ca/docview/933282234?accountid=14656 (accessed December, 15, 2013).

National Archives of Australia (2011), "A checklist for records management and the cloud", available at: www.naa.gov.au/records-management/publications/cloud-checklist.aspx (accessed December 15, 2013).

National Library Board Act, Statutes of Singapore (2012), c. 197, Singapore web site: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A%22fbf7d269-e298-4085-bcce-d25e024fdd6d%22%20Status%3Ainforce%20Depth%3A0;rec=0. See also www.nlb.gov.sg/Corporate.portal?_nfpb=true& _pageLabel=Corporate_portal_page_aboutnlb&node=corporate%2FAbout+NLB%2FNLB+ Act&corpCareerNLBParam=NLB+Act (retrieved from Attorney-General's Chambers).

Neilsen Company (The) (2012), "A Neilsen Report – Global online consumers and multi-screen media: today and tomorrow", May, available at: www.nielsen.com/us/en/reports/2012/global-online-consumers-and-multi-screen-media-today-and-tomorr.html (accessed December 15, 2013).

Poullet, Y., Van Gyseghem, J., Gérard, J., Gayrel, C. and Moiny, J. (2010), "Cloud computing and its implications on data protection", discussion paper, Council of Europe Project on Cybercrime, 5 March, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/ Reports-Presentations/2079_reps_ IF10_yvespoullet1b.pdf (accessed 15 December, 2013).

RecordTV Pte Ltd vs MediaCorp TV Singapore Pte Ltd (2010), "SGCA 43", December 1.

Ryngaert, C. (2008), "The territoriality principle", in Ryngaert, C. (Ed.), *Jurisdiction in International Law,* Ch 3, Oxford University Press, New York, NY.

Somes, B. (2012), "Audiovisual preservation at the National Archives of Australia", available at: www.naa.gov.au/about-us/partnerships/conferences/brendan-somes-audiovisual-preservation.aspx (accessed 15 December, 2013).

Suderman, J., Foscarini, F. and Coulter, E. (2005), "International Research on Permanent Authentic Records in Electronic Systems (InterPARES 2 Project) Policy Cross-domain: Archives legislation study report", 2 September, available at: www.interpares.org/display_file.cfm?doc=ip2%28policy%29archives_legislation_study_report.pdf (accessed 15 December, 2013).

Union des consommateurs (2011), "*Canadian Perspectives on Cloud Computing and Consumers: Final Report of the Research Project Presented to Industry Canada's Office of Consumer*

Affairs, Union des consommateurs, Montreal,, available at: http://uniondesconsommateurs.ca/docu/vieprivee/CloudComputingE.pdf (accessed December 15, 2013).

United Nations Centre on Transnational Corporations (1982), "Transnational corporations and transborder data flows: a technical paper", United Nations, New York, NY, available at: http://unctc.unctad.org/data/e82iia4a.pdf (accessed December 15, 2013).

United Nations Commission on International Trade Law (UNCITRAL) (n.d.), "FAQ – UNCITRAL", available at: www.uncitral.org/uncitral/en/uncitral_texts_faq.html#model (accessed December 15, 2013).

Weber, R.H. (2013), "Transborder data transfers: concepts, regulatory approaches and new legislative initiatives", *International Data Privacy Law*, Vol. 3 No. 2, pp. 117-130.

Further reading

Archives Act, Statutes of Australia (1983), Act No. 79, available at: www.comlaw.gov.au/Details/C2012C00025 (accessed from Australian Government Commonwealth Law).

Business Software Alliance (2013), "2013 BSA global cloud computing scorecard – a blueprint for economic activity", available at: http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf (accessed December 15, 2013).

Kobrin, S.J. and Kobrin, S. (2004), "Safe harbours are hard to find: the Trans-Atlantic data privacy dispute, territorial jurisdiction and global governance", *Review of International Studies*, Vol. 30 No. 1, pp. 111-131.

Library and Archives Act, Statutes of Canada (2004), c.11, available at: http://laws-lois.justice.gc.ca/PDF/L-7.7.pdf (retrieved from Department of Justice Canada).

National Rugby League Investments Pty Limited vs Singtel Optus Pty Ltd (2012), FCAFC 59, April 27.

Society of Composers, Authors and Music Publishers of Canada vs Canadian Assn. of Internet Providers (2004), "SCC 45", June 30.

About the authors

Elaine Goh is a Doctoral Candidate at the School of Library, Archival and Information Studies at The University of British Columbia in Vancouver, Canada. Her research interests are archival legislation, organizational culture and behavior, records management, and digital preservation. She is a graduate research assistant in the Records in the Cloud project and the International Research on Permanent Authentic Records in Electronic Systems (InterPARES) Trust project. Elaine Goh can be contacted at: nicolette_elaine@yahoo.com