Stormy Weather: Jurisdiction over Privacy and Data Protection in the Cloud

Patrick D. Flaherty and **Giancarlo Ruscio**[1]

Session: 90 — ***Cloud computing: its impact on privacy, jurisdiction, security, lawful access, ownership and permanence of data*** — Committee on Copyright and Other Legal Matters (CLM)

Abstract:

I*n recent months, the "Cloud" has worked its way firmly into the lexicon of the popular media.*[2] *Often, the Cloud is presented as a choice between convenience and efficiency versus privacy. On the one hand, Cloud Providers, tech gurus and private enterprise expound the benefits of a mass migration to Cloud based computing, including better customer service, enhanced consumer experience, and lower overhead costs. On the other hand, privacy advocates and civil libertarians have sounded the alarm about the increased risks to individuals when their personal information is transferred, stored, accessed and processed across multiple jurisdictions by multiple parties in a Cloud environment. Caught in the middle of the debate are organizations contemplating migrating some or all of their IT infrastructure to the Cloud. While the benefits to the Cloud seem tangible, so do the legal, reputational and enterprise risks. To compound the complexity of the choice faced by an organization contemplating a move to the Cloud, the jurisdictional questions of what law applies, and when, in the transnational Cloud environment can seem insurmountably complex and uncertain, such that some organizations are reluctant to move to the Cloud for fear of violating their obligations.*

[1] Mr. Flaherty is a Partner in the Litigation Department of Torys LLP in Toronto, Canada. Mr. Ruscio is a Summer Law Student at Torys.

[2] "*There is a battle in the Cloud for your business*", Wall Street Journal, August 3, 2012; "*Getting your head into the Cloud*" The Globe and Mail, July 31, 2012; "*Keep your head in the Cloud*", The Times, May 1, 2012.

In this paper, we will address the jurisdictional issues associated with privacy and data protection in the Cloud, particularly as they relate to the obligations of libraries and archival institutions, and offer some guidance on how organizations might consider compliance. While the jurisdictional questions can be confounding, there exists already a substantial body of law and resources in many major jurisdictions that offer guidance on how best to meet privacy and data protection obligations while not missing out on the benefits that can be delivered by the evolving and expanding Cloud environment.

Background

(a) What is Cloud computing and what are the benefits?

Cloud computing[3] generally refers to the delivery of computing services over the Internet, which allow individuals and businesses to use software and hardware managed by third parties at remote locations. As described by the U.S. National Institute of Standards and Technology, Cloud computing enables convenient, on-demand access to a shared pool of resources such as networks, servers, storage, applications and services with minimal management effort[4]. Important from the perspective of legal obligations, the computer power of the Cloud is frequently located in multiple different locations and countries across the network, often with different entities involved in its delivery to the users of the service.

Many businesses are moving their IT infrastructure to the Cloud. This allows organizations to focus on their primary business activities as opposed to building and maintaining an internal IT infrastructure. The benefits for any organization considering moving to the Cloud are numerous: "low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations"[5]. Importantly for smaller organizations, Cloud Providers have specialized expertise and can bring advanced services that would be difficult and costly to develop and maintain in-house. Both private and public institutions are attracted by the benefits offered by the Cloud, and library and archival services are no exception. This is particularly so as budgets shrink and IT demands grow with the expanding data rich environment in which libraries and archives operate.

(b) Privacy and Data Protection Concerns with the Cloud

Although the benefits to moving an organization's IT infrastructure to the Cloud are numerous, there are potential privacy and data protection risks that must be addressed. A movement to the Cloud can, and typically will, entail a broad outsourcing of IT functions, and thus will frequently require the transfer to the Cloud Provider the personal information collected,

---

[3] As has been observed by the Privacy Commissioner of Canada, "Cloud computing" has become a "nebulous term" that covers all forms of IT solutions and infrastructure and is thus often misunderstood or confused by consumers and business alike [see "*Reaching for the Cloud(s): Privacy Issues Concerning Cloud Computing*", March 29, 2010 http://www.priv.gc.ca/information/pub/cc_201003_e.asp (*Reaching for the Cloud*)].

[4] "*Fact Sheet: Introduction to Cloud Computing"*, October 2011 http://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf.

[5] *Ibid*.

used and maintained by an organization. This can include data about employees, customers, patrons, and suppliers. The Cloud, like any outsourcing arrangement, therefore, raises concerns about the security, retention, and use of personal information once transferred to third parties.

Unlike many outsourcing arrangements, however, realization of the full cost-saving benefits of the Cloud often involves outsourcing to multiple parties (and sub-parties) who operate in multiple jurisdictions, frequently without full transparency to the user of the Cloud service. In addition, because the Cloud primarily, if not exclusively, involves collection, use and storage of information (including personal information) in digital format, information in the Cloud can be copied, transferred and disclosed across borders and between parties with an ease not available with data stored in physical format.

With this background, the main privacy concerns raised about the Cloud, therefore, are:

(a) increased risk of improper use and disclosure of personal information that is stored and accessible in multiple locations, by multiple parties, across multiple jurisdictions;

(b) risk of disclosure to foreign law enforcement or regulatory authorities created by storage and processing of data outside of the home country of individuals from whom the information was collected;

(c) compliance with an organization's data retention and destruction obligations; and,

(d) meeting an organization's transparency obligations with regard to its privacy and data protection practices, when often the full knowledge of how and where data is stored, processed and shared can be obscured in the Cloud environment.

(c) The Cloud and Privacy/Data Protection Regulation: The Jurisdictional Conundrum

Since the Cloud is distributed in nature, data is collected, used, stored, processed and duplicated (for fault tolerance), in multiple places, often at the same time[6]. It is not unusual, therefore, to have a transnational cast of characters behind a Cloud Provider. For example, a Cloud Provider operating in the United States can be dealing with personal information of users in Canada and Australia, while utilizing data processors in India, who access the data on servers located in Uruguay, all of which is backed up on servers located in Ireland.

As has been observed, there can be a false sense of so called "jurisdictional neutrality" created among users of the Cloud, who confuse the seamless nature of the technology with its implications on parties' legal rights and obligations.[7] In the scenario described above, there are potentially seven different bodies of national privacy and data protection laws that touch this particular Cloud and those who use and provide it. As to be expected, not all of these laws are consistent in terms of parties' rights and obligations with regard to personal information. The jurisdictional permutations of "whose law applies" are challenging for lawyers and courts, let

[6] See Mutkoski, Stephen "Jurisdiction in the Cloud: Clear Rules to Build Confidence in Cloud Computing" http://Cloudlaw.ca/presentations/Jurisdiction%20in%20the%20Cloud-%20Stephen%20Mutkoski-%20Microsoft%20Corporation.pdf describing how Microsoft's Cloud service, Azure.

[7] *Reaching for the Cloud, supra* note 3.

alone the IT person charged with determining how to outsource to the Cloud in a cost-effective and complaint manner.

As we describe below, however, we believe that the jurisdictional conundrum posed by the Cloud can be managed to some degree if one grasps a few fundamentals:

- first, there is no one set of national laws that will exclusively apply to most Clouds. Rather, such as in our scenario, the laws of each of the jurisdictions in which the users and providers of our Cloud will most likely apply to a party that has a presence in that jurisdiction, irrespective of the contractual choices parties make about what law will govern their rights and obligations as against each other;

- second, a party should focus first and foremost on complying with its local law, which typically will be the law of the jurisdiction in which a party is physically present, and which will thus impact it most directly. If the collection, use, storage and/or disclosure of personal information required by the Cloud arrangement offends its local law, an organization will not want to proceed; and,

- third, even if the local laws of other parties in the Cloud arrangement do not apply to it directly, the Cloud user should understand to where and to whom personal information will be transferred in the Cloud, and understand how information can be used and disclosed (lawful or otherwise) in those jurisdictions so as not offend its own legal obligations by permitting an outsourcing to those places.

Libraries and The Cloud: Some Special Considerations

Before reviewing generally the law on privacy and outsourcing of some jurisdictions, it is worth noting that libraries and archives pose some special compliance considerations when dealing with the Cloud.

Many libraries and archives are public bodies and thus subject to public sector regulation of their collection, use, maintenance and disclosure of personal information[8]. Frequently, public sector regulation imposes more stringent privacy obligations than private sector equivalents. For example, in Ontario, public libraries' privacy obligations are regulated in the same manner as government organizations, which are more limited in the kinds of personal information that can be collected, used and disclosed than private sector organizations.[9] Further, as public institutions, some libraries are precluded from outsourcing data processing outside of their own jurisdiction at all or unless they comply with additional obligations to those applicable to the private sector[10] (for example in the Provinces of British Columbia and Nova Scotia in Canada). In addition,

[8] For example, in Ontario the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, C-M.56 ("MFIPPA") applies to public libraries.

[9] See MFIPPA, s. 2(1) for definition of "personal information".

[10] See for example, *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, C-165, s. 30.1.

many public libraries are limited by statute in how long they can maintain personal information[11] (such as records of books borrowed). Further, many librarians and archivists are subject (either voluntarily or by law) to the rules of self-governing regulatory bodies that impose obligations with respect to privacy and data protection as ethical obligations.[12] The difference in privacy regulation applied to public libraries and archives as compared to the private sector has implications for compliance with local law when assessing the suitability of a Cloud arrangement.

In addition, libraries and archives often collect highly sensitive personal information from patrons. Typically, libraries collect from their patrons name, address, telephone number, and email address, which mirrors what other organizations collect about their clientele. In addition, though, libraries and archives also collect reading preferences, records of materials borrowed, program attendance, financial information, opinions, and information Internet use from library terminals.[13] This is all potentially highly sensitive information about an individual's interests, beliefs and practices, including information which is sometimes of interest to law enforcement and other governmental authorities.[14] Because of the sensitive nature of some of the information libraries maintain, and the interest of law enforcement and others in it, the outsourcing of data processing in the Cloud in the library context, therefore, raises unique implications and questions.

Compliance with Substantive Law

Not all countries have comprehensive privacy legislation. The U.S., for example, has yet to regulate across all industries the collection, use, processing and disclosure of personal information. Most jurisdictions that have adopted privacy laws have done so on models based on the Organization for Economic Co-operation and Development's (OECD) privacy guidelines. The core obligations under the guidelines are as follows: only the personal information needed for a stated purpose should be collected, the collection should be openly communicated, the user must give informed consent to the collection and use, and the personal information must be properly safeguarded.[15]

---

[11] Public libraries in Ontario must retain and dispose of personal information in accordance with the regulations attached to MFIPPA. Personal information that has been used by a library should be retained for one year after use, or a shorter period set out in a bylaw or resolution made by a library board, unless consent is given for earlier disposal. Libraries must ensure that records are disposed of in accordance with the relevant regulations when they are no longer required. This includes ensuring that the information is destroyed in a manner that it cannot be reconstructed or retrieved and that reasonable steps are taken to protect the security and confidentiality of records during the destruction process.

[12] For example "Ethics and Information Ethical principles of the library and information professionals" IFLA**,** at http://www.ifla.org/en/node/6496**.**

[13] "*What are the privacy responsibilities of public libraries*?", Information and Privacy Commissioner/Ontario, December 2002, at http://www.ipc.on.ca/images/Resources/library-e.pdf.

[14] See for example "*F.B.I., Using Patriot Act, Demands Library's Records"*, The New York Times, April 26, 2005, which reported on US law enforcement seeking to access under the Patriot Act borrowing records from a Connecticut library

[15] See MacIsaac, Barbara, Shields, Rick and Klein, Kris, *The Law of Privacy in Canada* (Toronto: Carswell, 2000) at 5.1.1.

An understanding of the jurisdictional issues the Cloud poses requires some appreciation of the substantive privacy laws as they relate to the outsourcing of personal information. The following is a brief review of some of the main legal requirements of some major jurisdictions.[16]

(a) Collection and Use of Information

Under Canadian law, public libraries generally are not free to collect personal information of their patrons for any purpose; they can only do so where the collection is authorized by statute, is to be used for law enforcement purposes, or is necessary for the administration of a lawfully authorized activity. An institution is not permitted to use personal information in its custody or in its control without consent except for the purpose for which it was collected or compiled or for another consistent purpose.[17] If a library wishes to use the personal information of its patrons for a purpose (or a consistent use) for which consent has not already been obtained, written consent of the individual is necessary.[18]

In the U.S. as noted above, there is no comprehensive legislation dealing with the protection of personal information. For businesses, disclosing the personal information of customers "is often unrestricted by law because no privacy law or other law applies"[19]. Compliance, therefore, is largely dependent on the nature of the information in issue, from whom it is collected, and state or industry specific laws.[20] Adding to this complex maze of legislation are enforcement actions by the FTC, which it has been observed, "demonstrate that regulators have the consumer protection authority – even outside an overarching federal privacy law – to take action against companies that don't live up to their privacy terms of service."[21] In exercising this jurisdiction, the FTC typically considers whether the Cloud user has adequate notice of how the service was collecting, using, transferring and storing their personal information to determine compliance.

In the EU the *Directive on the Protection of Personal Data With Regard to the Processing of Personal Data and the Free Movement of Such Data* (EC Directive) enumerates a list of principles for the protection of personal information to which Member States must adhere. For example, personal information must be collected for specified, explicit and legitimate

---

[16] This is not meant to be an exhaustive review of the law, particularly for jurisdictions outside of Canada. Parties should consult legal counsel in their own jurisdiction for informed views of compliance.

[17] See for example Ontario's MFIPPA, *supra* note 8 at s. 32.

[18] Note that written consent should include the patron's name, the personal information to be used, the use for which consent is given, the date of the consent and the institution to which consent is given.

[19] Gellman, Robert, "Privacy in the Clouds: *Risks to Privacy and Confidentiality from Cloud Computing*", February 23, 2009 from http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf. at 5.

[20] Although federal agencies are subject to the *Privacy Act* of 1974, which regulates the collection, maintenance, use and disclosure of personal information, not all states have enacted similar legislation to regulate public agencies. Examples of specific legislation regulating certain kinds of information include the *Video Privacy Protection Act*, the *Gremm-Leach-Bliley Act* (financial information) and the *Children's Online Privacy Protection Act*.

[21] Maier, Fran, "Can There Ever Really Be Privacy in the Cloud?", October 19, 2011 from http://mashable.com/2011/10/19/Cloud-privacy/

purposes and not further processed in a way incompatible with those purposes.[22] Unambiguous consent obtained from the data subject serves to ensure that the information collected is legitimate. Important to compliance with EU law in the Cloud context, an individual whose data has been collected are required to be informed of parties who control that data. Because of the inherent distributed nature of Cloud computing, it may be difficult at any given time to establish who has "control" of the data in a manner sufficient to comply with EU law.[23]

In Australia, the Federal *Privacy Act* applies to both public bodies and private sector organizations and regulates the collection, use and disclosure of personal information. Public libraries, however, are subject to state laws such as Victoria's *Information Privacy Act 2000* (IPA). Most obligations regarding the collection and use of personal information under the IPA are similar in substance to those of Canadian law. Collection must be necessary to carry out the functions and activities of an organization, information must be collected lawfully and fairly, and notice must be given to individuals at the time of collection.[24] Furthermore, a library can only use information for the same purpose it was collected or for a consistent purpose, unless there has been additional consent.[25]

(b) Limitations on Disclosure

In Canada, libraries are prohibited from disclosing personal information except in accordance with applicable legislation. Examples where disclosure of personal information is permitted include public access according to law, where there is informed consent, for the purpose for which it was obtained, or to assist in an investigation by a law enforcement agency. Libraries cannot, for example, disclose to a reporter a list of books or videos that an individual has borrowed without their consent.

Under U.S. law, the limitations on disclosure are once again a function of the particular legislation covering a given organization, so generalizations are not possible. For example, in California, the *California Government Code* protects an individual's privacy when using online library resources and the *California Reader Privacy Act* protects information about the books people browse, read or purchase from electronic services. If statutes similar to these apply, an organization will be not be able to disclose customer information without limitation. Additionally, the FTC has the power to investigate and reprimand organizations if they fail to comply with their own privacy policies. To the extent that an organization has a privacy policy in place, it cannot disclose information in a way that contradicts its policy.

European law also limits when information can be disclosed to third parties. As discussed above, information cannot be processed by any party, including third parties to whom information has been disclosed, unless the processing is "legitimate". If one of the criteria to

---

[22] In order for personal data to be legitimate it must meet one of the specified criteria for collection. This can include processing that is necessary to fulfill a contract, to comply with a legal obligation, or to protect vital interests of the data subject (see EC Directive, article 7).

[23] A service provider may subcontract to different entities in different jurisdictions and they may subsequently parcel the data in different ways. Knowing who controls *particular data* may not be possible in this context, thereby exposing the collecting organization to the risk of breaching this obligation.

[24] IPA, No. 98 of 2000, Principle 1.

[25] *Ibid*, Principle 2

legitimize the processing has not been met, then the organization seeking to disclose must obtain unambiguous consent from the data subject.

In Australia, disclosure of information to third parties is restricted in the same manner as use. For example, an organization may disclose personal information in its possession if required by law or where there is informed consent. If disclosure is consistent with the same purpose as collection, additional consent is not required. This includes when the secondary purpose is related to the primary purpose of collection and the individual would reasonably expect the organization to disclose the information for that purpose. Providing notice to patrons that their data will be transferred to third parties will likely suffice to create such a reasonable expectation.

(c) Ability to Transfer Information to Foreign Jurisdictions

In Canada, there is generally no prohibition on the outsourcing of data processing to third parties in foreign jurisdictions. As discussed above, however, some public institutions (such as libraries) in certain jurisdictions may be prohibited from outsourcing data processing outside their own jurisdiction. Apart from these particular cases, an organization can outsource data for processing to foreign jurisdictions, as long as the individual whose information is being transferred has been notified that outsourcing to foreign jurisdictions may occur. Nonetheless, the collecting organization remains obliged to safeguard the information being transferred from improper use or disclosure by means of contractual and other means.

It is unclear if there are any restrictions under U.S. law to outsourcing of data processing to foreign jurisdictions. Typically, an organization would be permitted to outsource data for processing unless specific legislation prohibits it. Additionally, as discussed below, if an American organization is subject to an EU safe harbour, it will be prohibited from transferring data to other American third parties (except other safe harbour organizations) or to other restricted countries.

Knowing what jurisdictions the data will reside in is necessary in order to be compliant with EU law. The EC Directive stipulates that the transfer of personal data to a third country may only take place if that country has an adequate level of data protection. Where the EU determines that the country in question does not provide enough protection for the personal information, an organization cannot transfer data there, unless a safe harbour is obtained.[26] Transfer to third parties is only permitted when the third party is subject to EU law, has adequate protections (e.g. subject to laws of an approved country) or is itself a safe harbour organization.

[26] The EU has established safe harbour principles "whereby the personal data protections offered by an organization are certified as meeting acceptable standards" (see for example MacIsaac et. al., *supra* note 16 at 5.3.6). Organizations subscribing to these principles will be bound by certain obligations, ensuring a minimum level of data protection as imposed by the EU. These obligations include notice of purposes for collection, how information will be used and disclosed, opt-out policies, access to one's own personal information, as well as data protection and integrity.

In Australia libraries are prohibited from transferring personal information outside of the jurisdiction unless certain conditions have been met.[27] Libraries, therefore, may use the services of a Cloud Provider, but must first ensure that the provider (and any subcontractors) are required either by law or contract to comply with privacy obligations similar to those under the IPA.

The Cloud Implies Multiple Applicable Laws

As noted above, there is no true jurisdictional neutrality in moving to a Cloud-based provider of IT services. Potentially applicable laws will include any jurisdiction in which data is stored or accessible from, in which a person whose information has been collected is present, or where a party contracting for or providing services is located. Conflicts in applicable laws are possible. Any party contemplating a Cloud service should at a minimum ask the following questions:

1. Where is the data transferred stored and to whom will it be accessible?

2. Is there a robust set of laws that protects the privacy of personal information in each of those jurisdictions?

3. How do these laws differ from the local law that I am subject to? Are these differences material?

4. By transferring data to these jurisdictions, is there a risk that my organization will be in breach of its privacy obligations under local law?

As a matter of private international law, Courts in most countries assert legal jurisdiction in one of two ways: personal jurisdiction over parties that are within a country's territorial or legal domain; and/or, subject matter jurisdiction, where jurisdiction is taken over a particular type of dispute or case dealing with a specific subject matter. In addition, many legal systems will only assert jurisdiction over parties or matters that have a "real and substantial connection" to them, so as to constrain the application of their laws in appropriate circumstances. As discussed below, however, there is no "one size fits all" approach for jurisdiction over data protection, which varies from country to country.

As applied to the Cloud, personal jurisdiction is a possibility over parties in a jurisdiction who are either providing or collecting personal information, or using, holding or storing it (for example, the party to whom the data is outsourced). In theory, as a matter of subject matter jurisdiction, a country could enact legislation that applied to all Cloud Providers who have any connection to that jurisdiction, irrespective of where the regulated activity takes place.

[27] Unless the collecting body has obtained consent from the individual, it must ensure that either (a) it reasonably believes that the recipient is subject to a law with similar obligations of the IPA or (b) it has taken reasonable steps to ensure that the information will be handled in a manner consistent with the IPA. Other exceptions can apply such as the requirement of the transfer to fulfill the obligations under a contract or if it is in the best interests of the individual whose data is being outsourced (see IPA, *supra* note 25 at Principle 9).

The test under Canadian law to determine whether an organization is subject to Canadian privacy law is whether it has a "real and substantial" connection to Canada, and collects, uses or discloses personal information in the course of commercial activity[28]. Typically, Canadian privacy law will apply if personal information is stored within Canada and is collected, used or disclosed by parties in Canada.[29] Although a basic test for all private international law, the "real and substantial connection" test applies to the Internet as well[30], and as a consequence also to the Cloud.

In Canada, the manner in which a Cloud Provider establishes a platform for Canadian customers and advertises to them will impact whether Canadian courts will assert jurisdiction over their activities.[31] Furthermore, the Privacy Commissioner of Canada has the power to investigate notwithstanding the extraterritoriality of a company or website, where the Commissioner has jurisdiction over the subject matter of a complaint and there is a real and substantial connection to Canada.[32]

U.S. courts assume jurisdiction over any Cloud Provider server located anywhere in the world, so long as the provider itself is subject to U.S. jurisdiction. This will be the case "when the entity is based in the U.S., has a subsidiary or office in the U.S., or otherwise conducts continuous and systematic business in the U.S."[33]. Similar to Canada, the U.S. test for asserting jurisdiction is one of "minimum contact"[34]. U.S. courts also assert jurisdiction where the effects of extraterritorial behaviour adversely affect commerce or harm citizens within the U.S.

---

[28] The Supreme Court of Canada established in *Morguard Investments Ltd. v. De Savoye*, [1990] 3 S.C.R. 1077 that the exercise of jurisdiction for a province in Canada is appropriate where there is a "real and substantial connection between the jurisdiction and the wrongdoing". The *Morguard* test has been extended to the enforcement and recognition of foreign judgments (*Beals v. Saldanha*, [2003] 3 S.C.R. 416)

[29] Note that this, of course, does not preclude laws of other jurisdictions applying as well.

[30] See *Disney Enterprises Inc. v. Click Enterprises Inc.*, (2006) 267 D.L.R. (4th) 291, where the Ontario Superior Court recognized the exercise of jurisdiction of a New York court in favour of Disney. Click, a registered Ontario corporation with its address in Ontario, provided tools and technology for assisting Internet users in downloading copyrighted material. The Court held that since Click's websites were available through normal distributive channels to the residents of New York and since their products caused harm there, there was a real and substantial connection to that jurisdiction.

[31] See *Desjean v. Intermix Media Inc.*, [2006] F.C.J. No. 1754 and *Pro-C Ltd. v. Computer City Inc*, 1999 CanLII 14926 (Ont. S.C.)

[32] *Lawson v. Accusearch Inc.*, [2007] 4 F.C.R. 314.

[33] Maxwell, Winston and Wolf, Christopher, *A Global Reality: Governmental Access to Data in the Cloud*, May 23, 2012, A Hogan Lovells White Paper at 5.

[34] In the context of the Internet, the leading case is *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D.Pa. 1997) . In *Zippo*, the court held that jurisdiction is proportionate to the nature and quality of the commercial activity that an organization conducts over the Internet. Recent cases, however, have subsequently departed from the *Zippo* test, instead holding that minimum contact is established by purposeful direction, a forum related claim, as well as reasonableness, fair-play and substantial justice (see, for example, *Boschetto v. Hansing*, 539 F.3d 1011 (9th Cir. 2008)) .

Although all EU Member States' privacy legislation follows the EC Directive, jurisdiction is a matter of local law and may be different from country to country. However, many EU countries have similar private international law rules as Canada and will assert jurisdiction when there is a connection between the harm and the country in question. Generally, if an organization is collecting information about European residents or if data is collected, stored or processed in the EU then the appropriate EU country will assert jurisdiction.

The EC Directive also requires Member States to apply privacy rules to all data controllers who process personal data in the context of the activities of their European establishment. If the company is not established in the EU, it may nonetheless be subject to EU privacy laws if it makes use of equipment situated in the EU for purposes of processing personal data.[35]

Australia asserts jurisdiction when an entity is "present" in the jurisdiction. Typically, the "presence of a foreign corporation is determined by whether the company has transacted business for a definite period of time at some fixed place within the forum"[36]. The presence does not need to be physical and can be conducted through intermediaries or agents.[37] Although the analysis does not change for cases dealing with the Internet, this fact can add complexity to the issue of determining presence. In struggling with this question, the Australian High Court has asserted that "activities that have effects beyond the jurisdiction in which they are done may properly be the concern of the legal systems in each place" where a tort has occurred in the context of a foreign website.[38] Under this principle, even if there is not a substantial connection to Australia, the courts there may assert jurisdiction if a privacy breach abroad nonetheless affects Australia.[39]

Issues to Consider When Moving to the Cloud

As discussed above, as a general proposition, the organization that has collected and outsourced personal information to the Cloud Provider remains responsible for its proper safeguarding and use. Organizations, therefore, must adequately address security of the information and how to bind the Cloud Provider to privacy controls and standards that meet the organization's own privacy obligations when outsourcing. Furthermore, libraries need to ensure

---

[35] EC Directive, article 4. Note that this provision remains vague and most commentators agree that it is still not entirely clear in what circumstances non-EU entities will be subject to the EC Directive when using European data centers or providers, particularly where layers of providers are involved (See *Cloud computing and EU data protection law*, September 28, 2011 from http://blogs.computerworlduk.com/Cloud-vision/2011/09/Cloud-computing-and-eu-data-protection-law/index.htm).

[36] *Dunlop Pneumatic Tyre Co Ltd v A.G. Cudell & Co* [1902] 1 KB 342.

[37] See *BHP Petroleum Pty Ltd v Oil Basins Ltd* [1985] VR 725.

[38] *Dow Jones & Company Inc. v. Gutnuck* [2002] HCA 56.

[39] The extent of the effects doctrine under Australian law is not clear, however. The Australian Privacy Commissioner has investigated complaints about improper access of financial information from Society for Worldwide Interbank Financial Telecommunication (SWIFT) which occurred outside of Australia and concluded that it did not have jurisdiction over SWIFT's international operations (see Assistant Commissioner's Speech at http://www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=speeches&fullsummary=7133&Itemid=1021). It has yet to be determined by a court whether this type of decision would be upheld or whether it would be overturned based on the effects doctrine.

that both access to and correction of personal information in the Cloud is possible, and that deletion procedures are adequate to meet their obligations of data disposal.

The following are some important issues for libraries and archives to consider when transferring data to a Cloud Provider.

(a) Take steps to ensure that statutory obligations regarding destruction and retention of data are properly accounted for in the Cloud

As noted above, some libraries have a specific statutory obligation to destroy data after a certain period. In addition, most privacy and data protection laws require that organizations promulgate and observe guidelines for data retention of personal information that often prevent retention beyond the period which the information is in use as consented to by the data subject. When considering outsourcing data to Cloud Providers, organizations should carefully consider any clauses in the provider agreement that may be inconsistent with retention and destruction obligations. Since the nature of Cloud computing often implies data transfer to and back up in multiple places, it may be difficult to guarantee that information is properly disposed of in compliance with applicable law. Ensuring that the provider in question has an adequate policy dealing with the proper destruction of data is a minimum requirement. This alone, however, cannot guarantee that the information is not surviving somewhere "out there" in the Cloud.

The Privacy Commissioner of Canada for example suggests that "measures will need to be put in place to ensure that any copies of the data will be removed permanently from the Cloud infrastructure, and within what time period this will be done"[40]. As a practical matter, this can pose operational challenges given the proliferation of data in the Cloud.

(b) Evaluate the data security of the Cloud Provider

Some have expressed concerns that Cloud Providers do not uniformly employ robust data security measures.[41] Because data security remains an obligation of the organization who has collected the personal information, one should consider the security safeguards employed by the Cloud Provider. What will comprise adequate security safeguards is of course dependent on the sensitivity of the personal information outsourced to the Cloud Provider. As noted above, personal information collected by libraries often includes information about a patron's preferences and beliefs and is thus considered of a higher order of sensitivity. Typically, such information requires more stringent security safeguards such as encryption and physical barriers to access. Independent third-party certification seals can also be important trust indicators to evaluate if the provider is adequately protecting your data.[42]

---

[40] *Reaching for the Cloud*, *supra* note 3.

[41] Soglohan points out that Cloud Providers generally tend to "forgo strong security solutions" and advocates for providing, at a minimum, the same kinds of encryption currently used by online banks and retailers (see *Reaching for the Cloud*, *ibid*).

[42] Maier, *supra* note 21.

In assessing the adequacy of a Cloud Provider's security, tools such as Privacy Impact Assessments or Threat Risk Assessments can be valuable. Other steps that libraries can take to ensure that the personal information of their patrons is protected include limiting access to the information, and restricting further uses by the Cloud Provider. Ensuring that access is limited only to those individuals with the need to know, coupled with appropriate authentication and access controls in place, are common ways to meet obligations. In addition, the requirement of a Cloud Provider to maintain an audit trail can provide an additional layer of ensuring security.

(c) Managing Jurisdictional Risks Through Contractual and Other Means

While digital storage of data in the Cloud has a certain "borderlessness" to it, there are still things an organization can consider to manage the risks associated with exposing itself, and the personal information it transfers to the Cloud, to disparate privacy and data protection laws .

Because digital data must ultimately reside on a physical server, organizations should consider requiring that Cloud Providers only permit storage of, and subcontracting and access to data in jurisdictions that they have specified or approved. In this way, those jurisdictions where the data cannot be adequately safeguarded in a manner consistent with the organization's obligations can be avoided. For example, limiting the subcontractors to a closed list or inserting a clause in the agreement whereby the data outsourcing party must consent to the use of each subcontractor prior to data being transferred to it can achieve this goal. Similarly, it may be possible to negotiate a restrictive covenant restricting servers from being located in particular countries.[43]

"Choice of law" and forum selection clauses are another way of seeking to mitigate jurisdictional risks. Parties to a Cloud service contract can choose which jurisdiction's laws will govern any disputes between them and also specify the forum for litigation of any such disputes. These clauses are not binding on third parties to the agreement (such as customers, employees and others whose data is in the Cloud) and cannot override the application of many jurisdictions' privacy laws (that frequently prevent contracting out of privacy obligations), but they may still be useful to mitigate certain risks. For example a clause that requires the Cloud Provider to comply with the privacy and data protection laws of the organization who is outsourcing to the Cloud gives contractual assurances and remedies against the Cloud Provider in the event of a breach. Further, a forum selection clause can ensure that disputes with the Cloud Provider will be determined in the user's own jurisdiction , one that will recognize and enforce any public policy as it is applied to contracts.

The viability and utility of contractual means to manage the risk, however, is tempered by two realities. First, as a practical matter, most Cloud Providers operate with standard form contracts, where jurisdictional risks are allocated almost entirely on the user organization rather than Cloud Provider. Unless an organization has market power, amendments to the standard form may be difficult to obtain. Second, contractual safeguards can only provide so much protection. They typically provide a remedy in damages, which may be inadequate to

[43] See Kyer, C, Ian and Stern, Gabriel M.A., *Where in the World is My Data? Jurisdictional Issues with Cloud Computing*, March 30, 2011

compensate a party particularly in situations where disclosure of personal information may produce reputational rather than monetary loss.

(d) Consent and Notice Issues

As noted above, most privacy and data protection laws require an organization to be transparent about its data handling practices, and some will require consent of, or at least notice to, individuals when their data is outsourced for processing. To meet those obligations, an organization must know how the Cloud Provider will collect, use, store, process and maintain personal information, to either properly notify its customers how data is being outsourced, or, where required, to obtain meaningful consent to the transfer.

In addition, under some privacy and data protection laws (like in Canada and the EU) organizations are prohibited from making unreasonable consent a condition of service. Would consent to transfer data to a Cloud Provider be considered an unreasonable condition of service? The answer to this question may very well depend on *where* the data is being stored and processed. To the extent that the data is stored in a jurisdiction with a robust set of privacy laws and protections, it is most likely not unreasonable. Some jurisdictions, however, may not provide the same degree of protection and may even be plagued with problems of identity theft and fraud. In such cases, transfer of data to these jurisdictions could be interpreted as requiring unreasonable consent.

(e) Understand misconceptions about lawful access

There has been some negative attention associated with the Cloud business model due to the possibility of lawful access of information by foreign governments. In particular, much attention has been paid to the *Patriot Act* in the U.S., under which the government's powers to compel disclosure arguably have been expanded. For example, the *Patriot Act* prohibits recipients from disclosing that they are subject to an investigation, except as necessary to comply with or challenge a request.[44]

As has been observed, except in the very limited situations under the *Patriot Act*, the U.S. actually offers more protection than many other countries, requiring notice of an access request under *the Electronic Communications Privacy Act* (ECPA) and prohibiting voluntary disclosure by Cloud Providers. These protections are also extended to non-U.S. citizens.[45] In most EU countries voluntary disclosure to authorities is permitted without notification. Although there are strict privacy laws in the EU, expedited government access to Cloud data is also allowed under anti-terrorism laws.[46]

[44] Maxwell, Winston and Wolf, Christopher, *A Global Reality: Governmental Access to Data in the Cloud*, May 23, 2012, A Hogan Lovells White Paper at 5.

[45] *Ibid*.

[46] *Ibid* at 1.

In addition, some of the other negative criticism of the Cloud in relation to government access to personal information may be overstated. [47] Governmental and regulatory power to access personal information when necessary, and the existence of Mutual Legal Assistance Treaties (MLATs) among countries, often facilitate exchange of personal information among foreign states. The geographic boundaries of jurisdictions is perhaps becoming less important even outside of the Cloud context.

(f) Understand and evaluate the Cloud Provider's Standard terms of service

When contemplating moving data into the Cloud, your organization should review the Cloud Provider's standard terms of service. When doing so, careful attention should be paid to ensuring that personal information entrusted to the provider is treated in a manner that is consistent with your organization's privacy and data protection obligations.

Some providers, particularly those who offer free or low cost services, will often present "take it or leave it" standard form contracts, where the provider sets out all the terms of the relationship and the contracting party is required to accept those terms in order to use the service. As described by the Privacy Commissioner of Canada, there is a concern "that the terms of service that govern the relationship with the Cloud Service Provider sometimes allow for more liberal usage of personal information and retention practices"[48] than the transferring organization's privacy policies allow.

Of particular concern are provisions that allow the provider to unilaterally change the terms of the policy without notice, limit its liability for the information in the event of a security breach, and subcontract the storage and processing of data to other providers. The more latitude the provider is given, the higher the risk that an organization moving to the Cloud could violate an existing privacy obligation. In the event that an agreement would permit the provider to use the information transferred in a way that is inconsistent with the purpose for which it was collected, an organization would need to obtain separate consent from customers.

Another potential concern for organizations outsourcing to a Cloud Provider is the voluntary disclosure of customer data. Not all jurisdictions have legislation that prohibits the voluntary disclosure of customers' private information. Thus, when reviewing the provider agreement, it is important to ensure that the use of data being managed by the provider is restricted and that it cannot be disclosed unless compelled by an enforcement agency or court.

(g) Develop a Cloud Security Breach Response Plan

Security of personal information is always a concern, whether data is stored in-house, outsourced to a third party, or transferred to the Cloud. Although Cloud computing presents additional complexities, your organization should have a plan articulating how it manages security breaches. It should ensure reasonable steps are taken to prevent breaches from occurring in the first place. Understanding what regulators require in the event of a breach is also critical;

---

[47] Van Overstraeten, Tanguy, *law Enforcement and Cloud Computing*, October 2011 from http://linklaters.com/pdfs/mkt/london/Law%20Enforcement.pdf.

[48] *Cloud Computing for Small and Medium-sized Enterprises: Privacy Responsibilities and Considerations*, June 2012 from http://www.priv.gc.ca/information/pub/gd_cc_201206_e.asp.

as often prompt notice of the nature of the breach and the steps taken is required. Depending on your local law, customers should also be notified of the risks of breach, how your organization handles breaches, and when a breach occurs.

Libraries who are considering outsourcing to the Cloud, therefore, must review the service contract and understand when the Cloud Provider will provide notice to the organization in the event of a security breach. This will ensure that libraries meet their own obligations in relation to breaches.

In the event of a security breach, it is also important to be informed about the contractual remedies available to your organization. Assessing the limitation of liability clause in the provider agreement is important to understanding your organization's rights in the event of a breach. Furthermore, organizations should consider the ability to terminate the agreement with a Cloud Provider in the event of security breach.

(h) Termination procedure in place once the service contract has ended

Finally, it is important to "ensure the termination procedures permit the transfer of personal information back to the organization and require that the Cloud Provider securely delete all personal information within reasonable and specified timeframes"[49]. Prior to entering into a Cloud service agreement, organizations should confirm that there is a proper procedure in place for getting all data back and ensuring no copies are retained by the Cloud Provider irrespective of the reason for termination.

(i) Obtain proper legal advice

The legal issues posed by Cloud computing are complex and can depend largely on an individual organization's situation and needs. It would be wise for any organization considering a Cloud arrangement to seek local legal advice.

[49] *Ibid.*