The Cloud Implies Many Applicable Laws

As noted in Part 1 of this article, Cloud-based IT services have no true jurisdicational neutrality. Potentially applicable laws will include those from any jurisdiction in which data are stored or accessible from, in which a person whose information has been collected resides, or in which 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 are the data transferred stored, and whom are they accessible to?
(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 the organization is subject to? Are these differences material?
(4) By transferring data to these jurisdictions, is there a risk that the 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: 1) personal jurisdiction over parties that are within a country’s territorial or legal domain or 2) subject matter jurisdiction over a dispute dealing with a specific subject matter. In addition, to constrain the application of their laws to appropriate circumstances, many legal systems will assert jurisdiction only over parties or matters that have a “real and substantial connection” to them. As discussed below, however, jurisdiction over data protection varies from country to country.
For disputes about information held in the Cloud, personal jurisdiction is applicable over parties who are either providing or collecting personal information or using, holding, or storing it (for example, the party to whom the data are outsourced). In theory, for subject matter jurisdiction, a country could enact legislation that applies to all Cloud providers who have any connection to that jurisdiction, irrespective of where the regulated activity takes place.

Under Canadian law, the test 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. Typically, Canadian privacy law will apply if personal information is stored within Canada and is collected, used, or disclosed by parties in Canada. Although a basic test for all private international law, the real and substantial connection test also applies to the Internet and therefore to the Cloud, as well.

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

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.” Like the Canadian one, the U.S. test for assert-

...
ing jurisdiction is one of “minimum contact.” U.S. courts also assert jurisdiction where the effects of extraterritorial behaviour adversely affect commerce or harm citizens within the United States.

Although all EU member states’ privacy legislation follows the EU Directive, jurisdiction is a matter of local law and may be different from country to country. However, many EU countries have private international law rules similar to those of 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 are collected, stored, or processed in the EU, the appropriate EU country will assert jurisdiction.

The EU Directive also requires member states to apply privacy rules to all data controllers that 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 uses equipment situated in the EU for purposes of processing personal data.

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.” The presence does not need to be physical and can be conducted through intermediaries or agents. Although the analysis does not change for cases relating to the Internet, the fact of Internet involvement can add complexity to the issue of determining presence. In considering 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. Under this principle, even if there is no substantial connection to Australia, the courts there may assert jurisdiction if a privacy breach abroad nonetheless affects Australia or Australians.

**Issues to Consider When Moving to the Cloud**

As discussed earlier, 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. Therefore, when outsourcing, organizations must adequately safeguard the security of the information and determine how to bind the Cloud provider to privacy controls and standards that meet the organization’s own privacy obligations. Furthermore, libraries need to ensure that both access to and correction of personal information in the Cloud is possible and that deletion procedures are adequate to meet their obligations for data disposal.

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

(1) Ensure that the Cloud provides for the fulfillment of statutory obligations regarding destruction and retention of data

As noted earlier, 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. Those guidelines often prevent retention beyond the period when 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 agreements.
that may be inconsistent with retention and de-
struction obligations. Since the nature of Cloud
computing often implies data transfer to, and
backup in, many 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 for organiza-
tions. This alone, however, cannot guarantee
that the information does not survive some-
where “out there” in the Cloud.

The Privacy Commissioner of Canada, for ex-
ample, suggests that “[m]easures will need to be
put in place to ensure that any copies of the data
will be removed permanently from the [C]loud
infrastructure, and within what time period this
will be done.” As a practical matter, this can
pose operational challenges, given the prolifera-
tion of data in the Cloud.

(2) Evaluate the Cloud provider’s
data security

Some have expressed concerns that Cloud pro-
viders do not uniformly employ robust data se-
curity measures. Because data security remains
an obligation of the organization that has col-
lected the personal information, one should con-
sider 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 out-
sourced to the Cloud provider. For example,
personal information collected by libraries often
includes information about a patron’s prefer-
ences and beliefs and is thus considered highly
sensitive. Typically, sensitive information re-
quires more stringent security safeguards, such
as encryption and physical barriers to access.

Independent third-party certification seals can
also be important trust indicators to use when
evaluating whether the provider is adequately
protecting data.

In assessing the adequacy of a Cloud provider’s
security, tools such as privacy impact assess-
ments or threat risk assessments can be valu-
able. Other steps that libraries can take to ensure
that the personal information of their patrons is
protected include limiting access to the informa-
tion and restricting further uses by the Cloud
provider. Ensuring that access is limited only to
those individuals with the need to know as well
as ensuring appropriate authentication and ac-
cess controls are in place are common ways to
meet obligations. In addition, requiring a Cloud
provider to maintain an audit trail can provide
another layer of security.

(3) Manage the jurisdictional risks through
contractual and other means

While digital storage of data in the Cloud has a
certain “borderlessness” to it, an organization
can consider measures to manage the risks asso-
ciated with exposing itself and the personal in-
formation 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 permit storage of
information and access to data only in jurisdict-
ions that they have specified or approved as
well as subcontracting to organizations only in
those jurisdictions. In this way, organizations
can prevent having data sent to jurisdictions
where the data cannot be adequately safe-
guarded in a manner consistent with the organi-
zation’s obligations—for example, by 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 before data is transferred to
that subcontractor. Similarly, it may be possible
to negotiate a covenant restricting data being sent to or accessed from servers in particular countries.  

Choice of law clauses and forum selection clauses are other ways 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 can 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 are in the Cloud) and cannot override the application of many jurisdictions’ privacy laws (that frequently prevent contracting out of privacy obligations); however, 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 that 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 applies to contracts.

The viability and utility of contractual means to manage the risk, however, are tempered by two realities. First, as a practical matter, most Cloud providers operate with standard form contracts, whereby jurisdictional risks are imposed almost entirely on the user organization rather than on the Cloud provider. Unless an organization has market power, amendments to the standard form may be difficult to obtain. Second, contractual safeguards can provide only so much protection. They typically provide a remedy in damages, which may be inadequate to compensate a party, particularly where disclosure of personal information may produce reputational rather than monetary loss.

(4) Address consent and notice issues

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 are outsourced for processing. To meet those obligations, an organization must know how the Cloud provider will collect, use, store, process, and maintain personal information.

In addition, under some privacy and data protection laws (for example, 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 are being stored and processed. If the data are 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. Therefore, transfer of data to these jurisdictions could be interpreted as requiring unreasonable consent.

(5) Understand misconceptions about lawful access

There has been some negative attention associated with the Cloud business model, arising from the possibility of lawful access of information by foreign governments. In particular, much attention has been paid to the USA PATRIOT Act under which the government’s powers to compel disclosure have arguably been expanded. For example, the USA PATRIOT Act prohibits recipients of production requests or
orders from disclosing that they are subject to an investigation, except as necessary to comply with or challenge a request for production from law enforcement authorities.

As has been observed, except in the very limited situations under the USA PATRIOT Act, the United States actually offers more protection than many other countries, requiring notice of an access request under the Electronic Communications Privacy Act of 1986 and prohibiting voluntary disclosure by Cloud providers. These protections are also extended to non-U.S. citizens. 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.

Some of the other negative criticism of the Cloud in relation to government access to personal information may be overstated. Governmental and regulatory power to access personal information when necessary and the existence of mutual legal assistance treaties among countries often facilitate exchange of personal information among foreign states. The geographic boundaries of jurisdictions are perhaps becoming less important even outside the Cloud context.

(6) Understand and evaluate the Cloud provider’s standard terms of service

When contemplating moving data into the Cloud, an organization should review the Cloud provider’s standard terms of service. The organization should pay careful attention to ensuring that personal information entrusted to the provider is treated in a manner that is consistent with the organization’s privacy and data protection obligations.

Some providers, particularly those who offer free or low-cost services, will often present a standard form contract that 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 stated 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” 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 its data to the Cloud could violate an existing privacy obligation. If an agreement permits the provider to use the information 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.

(7) Develop a Cloud security-breach response plan

Security of personal information is always a concern, whether data are stored in-house,
outsourced to a third party, or transferred to the Cloud. Although Cloud computing presents additional complexities, an organization should have a plan articulating how it would manage security breaches. It should ensure that 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 because prompt notice of the nature of the breach and the steps taken are often required. Depending on the local law where the organization is located, customers should also be notified of the risks of breach, how the organization handles breaches, and if a breach occurs.

Libraries that 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, an organization should be informed about the contractual remedies available. Assessing the limitation of liability clause in the provider agreement is important to understanding the organization’s rights in the event of a breach. Furthermore, organizations should consider inserting a clause that specifically provides for the ability to terminate the agreement with a Cloud provider in the event of a security breach.

(8) Confirm that a termination procedure is in place when 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.” Prior to entering into a Cloud service agreement, organizations should confirm that there is a proper procedure in place for retrieving all data and ensuring that no copies are retained by the Cloud provider, irrespective of the reason for termination.

(9) Obtain 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.

[Editor’s note: Pat Flaherty’s practice focuses on civil litigation with an emphasis on corporate/commercial, product liability, intellectual property, information technology, and privacy. Pat has taught in the trial advocacy programs in several Canadian law schools, and he has written and spoken extensively on a wide range of legal subjects. He lectures at Osgoode Hall Law School. Giancarlo Ruscio was a student at Torys LLP. He has completed his BCL/LLB program at McGill University. This article was presented as a paper at the IFLA World Library and Information Congress, Helsinki, Finland, August 13, 2012. © 2012 Torys LLP. All rights reserved.]
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.


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, and also reasonableness, fair play, as well as substantial justice (see, for example, Boschetto v. Hansing, 539 F.3d 1011 (9th Cir. 2008)).


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 the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which occurred outside 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=y=7133&Itemid=1021>). A court has yet to determine whether this type of decision will be upheld or whether it will be overturned on the basis of the effects doctrine.

Reaching for the Cloud, supra note 2, Part 1 of this article, I.E.C.L.C. 13, no. 9 (2013): 71.

Christopher Soghoian 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. “Caught in the Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era,” 2009, <http://cyber.law.harvard.edu/events/luncheon/2009/05/soghoian>.

Maier, supra note 20, Part 1 of this article, I.E.C.L.C. 13, no. 9 (2013): 72.


Maxwell and Wolf, supra note 32 at 5.

Ibid.

Ibid. at 1.


Ibid.