Internet and E-Commerce Law in Canada

Editor-in-Chief: Professor Michael A. Geist, Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law

VOLUME 13, NUMBER 9 Cited as (2012-13) 13 I.E.C.L.C. JANUARY 2013

• STORMY WEATHER: JURISDICTION OVER PRIVACY AND DATA PROTECTION IN THE CLOUD—PART 1 •

Patrick D. Flaherty and Giancarlo Ruscio
Torys LLP

In recent months, "the Cloud" has worked its way firmly into the lexicon of the popular media.[1] Often, the Cloud is presented as a choice—convenience and efficiency or privacy. On the one hand, Cloud providers, tech gurus and private enterprise, expound the benefits of a mass migration to Cloud-based computing—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 several jurisdictions by numerous 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 of 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 which law applies, and when, in the transnational Cloud environment can seem insurmountably complex and uncertain, making some organizations reluctant to move to the Cloud for fear of violating their obligations.

In this article, we discuss 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 what organizations might consider in light of compliance obligations. Although the jurisdictional questions can be confounding, many major jurisdictions have a substantial body of law and resources that offer guidance on how best to meet privacy and data protection obligations while not losing the benefits of the evolving and expanding Cloud environment.

• In This Issue •

LexisNexis®

INTERNET AND E-COMMERCE LAW IN CANADA

Internet and E-Commerce Law in Canada is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ontario L3T 7W8

ISBN: 0-433-42472-9 **ISSN 1494-4146**
ISBN: 0-433-44385-5 (print & PDF)
ISBN: 0-433-44674-9 (PDF)

Subscription rates: $220 per year (print or PDF)
$325 per year (print & PDF)

Please address all editorial inquiries to:

Boris Roginsky, Journals Editor
LexisNexis Canada Inc.
Tel. (905) 479-2665; Toll-Free Tel. 1-800-668-6481
Fax (905) 479-2826; Toll-Free Fax 1-800-461-3275
Internet e-mail: ieclc@lexisnexis.ca.

Background

What Is Cloud Computing and What Are the Benefits?

Cloud computing[2] generally refers to the delivery of computing services over the Internet, which allows individuals and businesses to use software and hardware managed by third parties from 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.[3] What is important from the perspective of legal obligations is that the computer power of the Cloud is frequently located in many places across the network, often with different entities involved in delivering service to Cloud users.

Many businesses are moving their IT infrastructure to the Cloud. This allows organizations to focus on their primary business activities rather than 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."[4] What is important for smaller organizations is that Cloud providers have specialized expertise and can bring advanced services that would be difficult and costly to develop and maintain in-house. The benefits offered by the Cloud attract both private and public institutions, 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.

Privacy and Data Protection Concerns with the Cloud

Although the benefits of moving an organization's IT infrastructure to the Cloud are numer-

ous, potential privacy and data protection risks must be addressed. A movement to the Cloud can and typically will entail a broad outsourcing of IT functions, thus frequently requiring a transfer to the Cloud provider of the personal information collected, used, and maintained by an organization. This can include data about employees, customers, patrons, and suppliers. The Cloud, like any outsourcing arrangement, 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 many parties (and sub-parties) that operate in several 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

- the increased risk of improper use and disclosure of stored personal information accessible by several parties in many locations across many jurisdictions;
- the risk of disclosure to foreign law enforcement or regulatory authorities through data storing and processing outside the home country of individuals from whom the information was collected;
- the compliance with an organization's data retention and destruction obligations; and
- the meeting of an organization's transparency obligations regarding its privacy and data protection practices, when often the full knowledge of how and where data are stored, processed, and shared can be obscured in the Cloud environment.

The Cloud and Privacy/Data Protection Regulation: The Jurisdictional Conundrum

Since the Cloud is "distributed" (across locations) in nature, data are collected, used, stored, processed, and duplicated (for fault tolerance) in many places, often, at the same time.[5] 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 in Ireland.

As has been observed, there can be a false sense of so-called jurisdictional neutrality among users of the Cloud who confuse the seamless nature of the technology with its implications for parties' legal rights and obligations.[6] In the scenario described above, potentially six different bodies of national privacy, as well as their data protection laws, would touch this particular Cloud and those who use and provide it. As to be expected, not all 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 alone the IT person charged with determining how to outsource to the Cloud in a cost-effective and compliant 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 single set of national laws that will apply to most Clouds to the exclusion of others. Rather, as in our scenario above, the laws of each jurisdiction will most likely apply to a party that has a presence in that jurisdiction, irrespective of the

contractual choices parties make about which law will govern their rights and obligations.

Second, a party should first focus on complying with its local laws affecting that party most directly, which, typically, will be the laws of the jurisdiction where a party is physically present. An organization will not want to proceed if the collection, use, storage, and/or disclosure of personal information required by the Cloud arrangement offend its local laws.

Third, even if the local laws of other parties in the Cloud arrangement do not apply to a party directly, so as not to offend the Cloud user's legal obligations in its own jurisdiction by permitting outsourcing to places whose laws may breach those obligations, the Cloud user should understand where and to whom personal information will be transferred in the Cloud and how information can be used and disclosed (lawfully or otherwise) in those jurisdictions.

Libraries and the Cloud: Some Special Considerations

Before we review some jurisdictions' laws on privacy and outsourcing, 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.[7] 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 those of government organizations, which are generally more limited than private sector organizations in the kinds of personal information that they can collect, use, and disclose.[8] Further, as public institutions, some libraries are prevented from outsourcing data processing outside their own jurisdiction or may do so if they comply with additional obligations applicable to the private sector[9] (as is the case, for example, in the provinces of British Columbia and Nova Scotia). In addition, many public libraries are limited by statute as to how long they can maintain personal information[10] (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 ethical obligations with respect to privacy and data protection.[11] The difference in privacy regulation applied to public libraries and archives, compared with 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 do as other organizations and collect their patrons' names, addresses, telephone numbers, and e-mail addresses. In addition, though, libraries and archives collect—from library terminals—users' reading preferences, records of materials borrowed, program attendance, financial information, opinions, and information about Internet use.[12] This is all potentially highly sensitive information about an individual's interests, beliefs and practices, including information that is sometimes of interest to law enforcement and other governmental authorities.[13] Because of the sensitive nature of some of the information that libraries maintain and the interest of law enforcement authorities and others in it, outsourcing data processing in the Cloud by libraries raises unique implications and questions.

Compliance with Substantive Law

Not all countries have comprehensive privacy legislation. The United States, for example, has yet to regulate the collection, use, processing, and disclosure of personal information across all industries. Most jurisdictions that have adopted

privacy laws have based their laws on the Organisation for Economic Co-operation and Development's 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.[14]

An understanding of the jurisdictional issues regarding the Cloud requires some appreciation of 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.[15]

Collection and Use of Information

Under Canadian law, public libraries generally are not free to collect their patrons' personal information for any purpose; they can do so only if 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.[16] 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, the individual's written consent is necessary.[17]

As noted above, the United States has 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."[18] Compliance, therefore, is largely dependent on the nature of the information in issue, from whom it is collected, and state or industry-specific laws.[19] Adding to this complex maze of legislation are enforcement actions by the Federal Trade Commission ("FTC"), which "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."[20] In exercising this jurisdiction, the FTC typically considers, when determining compliance, whether Cloud users have been given adequate notice of how the service was collecting, using, transferring, and storing their personal information.

For the protection of personal information, a European Union ("EU") directive enumerates a list of principles that member states must adhere to. For example, personal information must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.[21] Unambiguous consent obtained from the data subject serves to ensure that the information collected is legitimate. In compliance with EU law in the Cloud context, an individual whose data has been collected must be informed of the identity 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.[22]

In Australia, the federal *Privacy Act 1988*, as amended in 2000, 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 federal and applicable provincial laws: 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.[23] Furthermore, a library can use information only for the same purpose it was collected or for a consistent purpose unless there has been additional consent.[24]

Limitations on Disclosure

In Canada, libraries are prohibited from disclosing personal information except in accordance with applicable legislation—for example, for public access according to law where there is informed consent, for the purpose for which it was obtained; and for assistance 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 that individual's consent.

Under U.S. law, the limitations on disclosure are 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 California's *Reader Privacy Act of 2011* (which took effect on January 1, 2012) protects information about the books people browse, read, or purchase from electronic services. If statutes similar to these apply to a particular organization, that organization will 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. An organization that has a privacy policy in place cannot disclose information in a way that contradicts its policy.

EU law also limits the disclosure of information 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 legitimize the processing has not been met, 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 of that information. For example, an organization may disclose personal information in its possession if required by law or if there is informed consent. If disclosure is consistent with the same purpose as collection, additional consent is not required. Nor is it required 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.

Ability to Transfer Information to Foreign Jurisdictions

In Canada, there is generally no prohibition on outsourcing data processing to third parties in foreign jurisdictions. As discussed above, however, some public institutions (such as libraries) in certain provinces 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 use contractual or other means to safeguard the transferred information from improper use or disclosure.

It is unclear whether U.S. law restricts 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 a U.S. organization is subject to an EU safe harbour, it will be prohibited from transferring data to other U.S. third parties (except other

safe harbour organizations) or to other restricted countries.

Knowing what jurisdictions the data will reside in is necessary for compliance with EU law. The EU Directive mentioned above stipulates that the transfer of personal data to a third country may take place only if that country has an adequate level of data protection. If 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.[25] Transfer to third parties is permitted only 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.

In Australia, libraries are prohibited from transferring personal information outside the jurisdiction unless certain conditions have been met.[26] Libraries may therefore use the services of a Cloud provider but must first ensure that the provider (and any subcontractor) is required by either law or contract to comply with privacy obligations similar to those under the *IPA*.

[*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.]

---

1 "There Is a Battle in the Cloud for Your Business," *Wall Street Journal*, August 3, 2012; "Getting Your Head into the Cloud," *Globe and Mail*, July 31, 2012; "Keep Your Head in the Cloud," *Times* (London), May 1, 2012.

2 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 businesses alike. "Reaching for the Cloud(s): Privacy Issues Relating to Cloud Computing," Office of the Privacy Commissioner of Canada, March 29, 2010, <http://www.priv.gc.ca/information/pub/cc_201003_e.asp> ("Reaching for the Cloud").

3 "Fact Sheet: Introduction to Cloud Computing," Office of the Privacy Commissioner of Canada, October 2011, <http://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf>.

4 *Ibid.*

5 See Stephen Mutkoski, who describes Microsoft's Cloud service, Azure, in "Jurisdiction in the Cloud: Clear Rules to Build Confidence in Cloud Computing," The Centre for Innovation Law and Policy at the University of Toronto Faculty of Law.

6 Reaching for the Cloud, *supra* note 2.

7 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.

8 *Ibid*., s. 2(1), the definition of "personal information."

9 See for example, *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165, s. 30.1.

10 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 so 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.

11 For example, "Ethics and Information Ethical Principles of the Library and Information Professionals," International Federation of Library Associations, <http://www.ifla.org/en/node/6496>.

12 "What Are the Privacy Responsibilities of Public Libraries?," Office of the Information and Privacy Commissioner/Ontario, December 2002, <http://www.ipc.on.ca/images/Resources/library-e.pdf>.

13 See, for example, Eric Lichtblau, "F.B.I., Using Patriot Act, Demands Library's Records," *New York Times*, April 26, 2005, <http://www.nytimes.com/2005/08/26/politics/26patriot.html>, which reported on a U.S. law enforcement agency seeking to access, under the *USA*

PATRIOT Act, borrowing records from a Connecticut library.

14 Barbara MacIsaac, Rick Shields & Kris Klein, *The Law of Privacy in Canada* (Toronto: Carswell, 2000) at 5.1.1.

15 This is not an exhaustive review of the law, particularly for jurisdictions outside Canada. Parties should consult legal counsel in their own jurisdiction for informed views on compliance.

16 See, for example, Ontario's *MFIPPA*, *supra* note 7, s. 32.

17 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 consent, and the institution to which consent is given.

18 Robert Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing," World Privacy Forum, February 23, 2009, <http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf> at 5.

19 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 of 1988*, the *Gramm-Leach-Bliley Act of 1999* (financial information), and the *Children's Online Privacy Protection Act of 1998*.

20 Fran Maier, "Can There Ever Really Be Privacy in the Cloud?," Mashable, October 19, 2011, <http://mashable.com/2011/10/19/Cloud-privacy/>.

21 *Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and the Free Movement of Such Data*, EU directive, art. 7. For personal data to be legitimate, it must meet one of the specified criteria for collection. There can be processing that is necessary to fulfill a contract, to comply with a legal obligation, or to protect vital interests of the data subject.

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

23 *IPA*, No. 98 of 2000, Principle 1.

24 *Ibid.*, Principle 2.

25 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, Shields & Klein *supra* note 14 at 5.3.6). Organizations subscribing to these principles will be bound by certain obligations, thereby 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.

26 Unless the collecting body has obtained consent from the individual, it must ensure that (a) it reasonably believes that the recipient is subject to a law with similar obligations to those 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 transferor to fulfill the obligations under a contract or the best interests of the individual whose data are being outsourced (see *IPA*, *supra* note 24 at Principle 9).