DJIM Dalhousie Journal of Interdisciplinary Management

**Volume 9 – Spring 2013**
**djim.management.dal.ca**
**doi:10.5931/djim.v9i1.3341**

# Controlling the Clouds: Privacy Law and Cloud Computing in Canada's Legal Sector

**Abstract:** This paper examines the promises and problems posed by the legal profession's adoption of cloud computing platforms in service of its business objectives. Cloud computing models, defined as third-party managed software, are rapidly becoming ubiquitous within technology-centric businesses. The legal profession is ostensibly an excellent candidate for the integration of cloud computing models due to its deep-seated information management needs. Nonetheless, this profession finds itself in an unnerving position in the face of government-mandated privacy laws and professional ethical standards, which make any compromise of private information potentially devastating to a wide variety of stakeholders. Exploring the tenuous line upon which the legal profession treads in relation to cloud computing, the author ultimately concludes that what is most conspicuously absent within this current debate is information policies which would provide the legal industry directives on how it should negotiate its way through this complex issue.

**About the Author:** Shauna Hall-Coates is a joint JD/MLIS student at Dalhousie University. Before embarking upon her joint degree, Shauna completed an M.A. in English Literature at Dalhousie University. Her deep interest in the intersection between the law and the information industry was the impetus for this paper. It was originally comprised for Professor Paul McKenna's course Information Policy (Winter, 2012).

# Controlling the Clouds: Privacy Law and Cloud Computing in Canada's Legal Sector

Cloud computing services have been hailed as the future of both public and private sector business to the extent that it has been said that "organi[z]ations that fail to embrace cloud computing as part of a new way of working will struggle to survive beyond the next decade" (Martindale, 2011). Cloud computing services — largely defined as third-party managed software designed to store and process an aggregate of organizations' data — significantly reduces the technological infrastructure companies need to build in order to house their digital information. With this reduction in technological infrastructure comes budgetary savings, since an organization's reliance upon cloud computing services allows it to outsource many of its costly IT responsibilities alongside its data.

Information is a major source of currency within the legal sector, as its practitioners are continuously involved in the procurement of volumes of evidentiary documents. To this end, cloud providers have designed cutting-edge software in order to address the professional needs of this community. Nonetheless, this availability does not imply adoption, as the legal sector has been markedly wary of cloud computing as a service model. Professional apprehension is principally due to the risks third-party managed software poses to lawyers' professional code of ethics, largely defined by rules of confidentiality and privilege as well as to their federally-mandated compliance with private sector privacy laws shaped by Canada's *Personal Information Protection and Electronic Documents Act*. As one analyzes these barriers to implementation what becomes evident is the absence of authoritative information policies that would provide the legal industry with directives on how to negotiate its way through these unfamiliar waters. Ultimately, the legal industry's complicated stance on cloud computing provides insight into the ethics of privacy and policy as they intersect within the 21st century, as well as on the central role information policies will necessarily play within the growing digital age.

## Cloud Computing: Definition and Applications

Cloud computing has become a ubiquitous component of the 21st century's technological landscape, yet, as its nebulous name suggests, the concept itself is hard to define. The National Institute of Standards and Technology supplies an often-cited definition of cloud computing, which works to distinguish this service from a typical consumer owned and operated product. NIST states, "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2010, p. 6). As a communally accessible service platform, cloud computing first and foremost allows individuals to store data and run software programs from remote locations. Users' information, in turn, is

stored on the cloud providers' servers, and is accessible to its creators/owners through a simple Internet connection and password.

Accordingly, cloud computing is often defined as "third-party" managed software, and is characterized by products such as online file storage, social networking sites, online business applications, and web mail. To this end, cloud computing can be *public*, where third party managed applications, storage, and software are free (for example, Google's Gmail, GoogleDocs, and Google Talk), or *private*, where third party managed software is operated solely for a single organization's use at a cost (for example, Amazon is the sole client of cloud computing service Elastic) (Foley, 2008). Despite the presence of different cloud computing models, what remains common to all is the fact that, at its basic level, "cloud [computing] is the keeping of one's information on another entity's server" (Baker, 2011, p. 57).

As a service, cloud computing can be very attractive to a wide variety of businesses due to its technological and economic benefits. Chiefly, cloud computing offers a high degree of scalability, since sophisticated cloud services often provide unlimited processing and storage capacity to customers at little to no cost. Cloud computing is similarly enticing from a collaborative perspective, as services such as GoogleDocs permits groups of individuals to work on the same document concurrently. Organizations which amass large volumes of information may also benefit from the relative security of cloud computing storage, given the ease at which physical documents, hard drives/thumb drives, and digital devices can be misplaced, lost, or stolen. This is a risk Canadians know all too well, as on January 11, 2013 the federal government announced that the personal information of approximately 583,000 Canadian student loan applicants was lost after a portable hard drive was misplaced (Rennie, 2013). Following this scandal, critics were quick to suggest that this security breach would not have occurred if cloud infrastructure had been relied upon instead of a physical storage device (Brown, 2013).

Likewise, the fiscal savings possible through an organization's conversion from self-contained software to cloud computing can be immense. A recent study of the U.S. government's 2013 IT budget indicates the level of savings achievable. The U.S. government, known as the "world's largest organization," is forecasted to save approximately 12 billion dollars annually from 2013 onward by adopting cloud services through its "Cloud First" initiative–savings which amount to roughly the annual budget of NASA (McKendrick, 2012). Principally, this type of savings stems from the fact that organizations who use cloud computing software will not have to invest in the amount of technological infrastructure they once did, including the continued purchasing of electronic storage devices and additional servers. Likewise, fewer budgetary resources would be absorbed by the cost of constant technological upgrades. Organizations, accordingly, can rely upon the cloud service provider to stay abreast of technological

developments, effectively outsourcing a number of their costly managerial responsibilities alongside their information.

Due to the fact that law firms handle, process, and store vast amounts of client and company information, proponents of the cloud have lauded the “mobility, versatility, and ease of access to documents [that] cloud [computing] offers allows [lawyers] to practise anytime, anywhere with an Internet connection” (Millan, 2011). As a response to the perceived applicability of cloud computing within this field, there has been a recent surge of cloud products marked towards legal professionals. Virtual law offices, such as Total Attorneys and DirectLaw, have been designed to mimic the physical data processing and storage features of law firms. Document sharing tools, such as Dialawg and Ejuris, have also been marketed on the premise that they expedite the collaborative design of legal cases. Additionally, public email providers such as Gmail permit legal professionals to register their law firms as their domain names, a practice which allows legal firms to maintain the illusion of having a corporate email account housed on a private server at no cost. As a result, lawyers now find themselves in a unique position to reap the benefits of third-party managed software specifically designed to satisfy their professional needs.

Nonetheless, while the number of cloud products marketed specifically toward the legal industry continues to grow, adoption of them has been distinctly slow, particularly when compared to their wide-scale implementation in other private sectors such as the retail industry (Millan, 2011; Fraser, 2011). At its root, this reticence stems principally from the commonly-held notion that moving information from the physical confines of the office to the clouds causes law practitioners to “lose – or at the very least appear to lose – control over client and firm data” (Millan, 2011). Crucially, this loss of control would not simply be injurious to a firm’s reputation, but would be in direct violation of the strict professional and federally mandated codes of ethics which govern information privacy within the justice system. Accordingly, it is important to lay bare these strict codes of professional conduct before analyzing the types of damage that novel technologies such as cloud computing may have on these entities.

## Personal Information Policies and Privileges within the Canadian Legal Sector

During the course of a civil litigation, a litigant’s personal records – often comprised of his or her medical, employment, and banking files – are typically disclosed to his or her acting solicitor. While the unwarranted release of these documents can be extremely detrimental to any individual, the gravity of unintended disclosure of classified legal material only increases with the profile and magnitude of the client. Due to the unrivalled sensitivity of the information in which they deal, legal professionals have been historically bound by “[r]ules of personal conduct, rules of court and other rules and regulations” (Dodek, 2011, p.3) which collectively aim to curb unwarranted third-party access of classified materials placed within their care.

One major rule-issuing body is the Canadian Bar Association, whose *Code of Professional Conduct* provides directives on the proper management of personal information for legal professionals in Canada. These practices are predominantly placed within the context of two distinct privacy principles: the duty of confidentiality and the duty of privilege. Although these two duties are often seen as synonymous, their application is meant to address two separate privacy concerns. The Supreme Court of Canada in *R v McClure* defined the duty of privilege, commonly known as solicitor-client privilege, as follows:

> Where legal advice of any kind is sought from a professional legal advisor, in his capacity as such, the communications relating to that purpose, made in confidence by the client, are at his instance permanently protected from disclosure by himself or by the legal advisor, except the protection be waived. (Dodek, 2011, p. 6)

In light of this rule, any communication between client and counsel – verbal, written, or electronic – is to be kept in absolute confidence between the two parties (Dodek, 2011).

On the other hand, the law of confidentiality applies to "all information obtained by the lawyer about the client's affairs during the retainer, however obtained" (Dodek, 2011, p. 18). This information may be communicated by the client to a wide variety of parties involved in the proceedings, but is nonetheless prohibited from being disclosed to the general public by the acting solicitor. Thus, if solicitor-client privilege applies to what can and cannot be divulged in front of members of the court, the duty of confidentiality regulates that can and cannot be disclosed to the general public, regardless of form or forum. Failure to uphold these professional duties could result in discipline and even disbarment, harsh repercussions that underscore the rigidity of the code of ethics that governs the internal management of classified information within the legal sector.

Furthermore, legal firms, like all private sector businesses within Canada, are subject to the privacy laws and regulations of the federal government. The most critical piece of legislation that regulates the Canadian private sector's management of personal information is the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Passed into law in 2001, PIPEDA provides "rules [which] govern the collection, use and disclosure of personal information [in an] era in which technology increasingly facilitates the circulation and exchange of information" (Office of the Privacy Commissioner of Canada, 2009). At its foundation, PIPEDA recognizes that private organizations must have the right to collect, use, and disclose clients' personal information in order to effectively conduct business. Under PIPEDA, personal information is defined as "any factual or subjective information, recorded or not, about an identifiable individual" which is consensually disclosed to a business during the course of

commercial activity.[1] Although the law recognizes the right of organizations to collect this information, it nonetheless stipulates that this right is contingent upon their ability to maintain confidentiality of this information during its procurement, management, and disposal. Likewise, under the law, an organization's information management practices must remain transparent to the public. To this effect, it must be able to disclose *why*, *where*, and *how* personal information is being stored, if a customer or client makes such a request.

Crucially, PIPEDA's directives on information handling for all private sector businesses extend to third-party managed software services such as cloud computing. Addressing this issue is the 2010 Office of the Privacy Commissioner's "Report on Online Tracking, Profiling, and Targeting, and Cloud Computing," which was produced to help "explain how PIPEDA applies to transfers of information to a third party, including a third party operating outside of Canada, for processing" (*Guidelines for Processing Data*, 2009). In it, a key distinction is made therein between "data controllers" and "data processors" that works to differentiate between the responsibilities of cloud service providers and their users under Canadian law. Crucially, when cloud services are offered directly to general consumers through platforms such as Facebook, it is the provider who acts as the data controller and the individual the data processor. Therefore, it is the cloud provider's responsibility to ensure privacy measures are in place to shield user information from unintended disclosure. However, where cloud services are used by private businesses, the cloud computer provider also acts as a data processor. The private business thus maintains the primary status as the data controller, and is responsible for the information's protection.

Accordingly, organizations who utilize cloud computing in the course of business must ensure that a "*comparable* level of protection [is upheld] while the information is being processed by the third party" (*OPC Report*, 2010, p. 36). "Comparable," in this sense, does not indicate that the private organization and the third-party processor's electronic privacy measures should be identical; rather, it stipulates that the third-party processor's measures should be commensurate with those that would have protected the information had it not been outsourced by the private organization. As way of conceptual elucidation, the OPC states that a service provider with a "comparable" level of protection under Canadian law must be "based in a jurisdiction with a mature and fair legal system," and that it must have "policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times" (Fraser, 2011).

The necessity for comparable information protection for third party servers has, moreover, been specifically levelled at the legal industry by the OPC. In a publication entitled *PIPEDA and Your Practice* (2011), the OPC asserts,

[1] PIPEDA does not extend the definition of personal information to include an individual's name, telephone number and business name, due to the public nature of these entities.

> [w]here any third party service provider may have access to or otherwise handle personal information on behalf of a lawyer, including cloud computing services, it is strongly recommended that a written agreement be put in place between the third party and the lawyer. Such a contract should include provisions governing the jurisdiction where information will be processed or stored, ownership and use of information, the level of privacy controls used by the service provider, access and correction procedures, audits, and deletion procedures. (p. 8)

Ultimately, a legal firm's failure to properly secure these measures would signal an inability to meet its privacy obligations under Canadian law. While these OPC mandates are direct, they nonetheless can be seen as extremely problematic within the context of the legal industry's adoption of cloud computing, since third-party processers pose substantial risks to lawyers' dutiful adherence of professional and federally mandated codes of privacy ethics.

## Cloud Computing Risks within the Legal Sector

As previously indicated, the reluctance of the legal industry to embrace cloud computing largely stems from the fact that these services could increase the risk that "an unknown party may gain access to a lawyer's digital information, while that information is stored on a third party's cloud servers, whoever that infiltrator may be" (Baker, 2011, p. 57). This risk can be seen as an insidious symptom of the cloud computing platform in general; however, the fact that cloud computing servers house an aggregate of information causes the problem to be particularly pressing within the context of the legal industry. Essentially, while cloud computing servers themselves are often said to be more secure than private IT software due to their privacy safeguards, enhanced user identification software, and constant technological upgrades, the very presence of aggregate data has been shown to significantly "increase[e] the scale of exposure, [. . .] [causing] cloud data center[s] [to be] attractive to criminals" ("OPC Report," 2010, p. 10). This risk is unquestionably compounded when the content of a cloud is comprised of numerous legal documents – which are essentially nesting dolls in which a vast amount of sensitive and highly classified information can be housed – from a variety of different firms. Accordingly, cloud computing services that cater exclusively to the legal industry may be seen as marked targets for cyber criminals hoping to unlock a treasure trove of heavily privileged, and thus potentially valuable, information.

Within the context of unauthorized access of data stored on cloud servers, the issue of jurisdiction is crucial. In particular, the vast scalability of cloud computing infrastructures means "one document might be stored in 16 different locations, some of which may be politically unstable nations" (Baker, 2011, p. 57). While PIPEDA outlines this fear in relation to governments who lack mature and fair legal systems (for example, North Korea and China are

two of the OPC's flagged 'no-fly zones' for third-party managed software), it is important to note that the threat of unsolicited government access of information stored in the cloud has been manifest most acutely in relation to the United States' USA PATRIOT Act (commonly known as the *Patriot Act*). The *Patriot Act*, a controversial law that allows the American government to obtain intelligence in the course of anti-terrorism investigations, gives this federal body the unrivalled "ability to retrieve data stored on U.S. soil and scour it without the need to inform the owner of the data" (Jackson, 2010). While those in the private sector, and even those in the legal profession, often believe that is it "illegal to put data in the cloud if that means it will be stored south of the border because of [the] provisions in the U.S. *Patriot Act*," Canada does not currently hold any laws which would prevent cloud computer companies from housing data on American servers (Buckler, 2011; Banks, 2012).

As a result, fear looms over the extent to which American law sanctions covert access to Canadian legal documents. This fear has not abated over time, as controversy recently sparked over the similar impact that the U.S.'s *Foreign Intelligence Surveillance Act* (FISA) may have on data sovereignty. Affirmed by the Senate in 2012, FISA authorizes the U.S. government to monitor data and communications stored on U.S. cloud servers by foreign political organizations or their agents in the course of terrorist investigations (MacLeod, 2013). Thus, like the *Patriot Act*, FISA makes U.S.-stored data subject to domestic law, and overrides any guarantee of privacy offered by cloud providers. The European Parliament recently spoke out against these laws, stressing in a report produced by its Committee on Civil Liberties, Justice, and Home Affairs that the U.S.'s ability to conduct surveillance in the clouds undermines data sovereignty and the protection of citizens' rights (*Fighting Cyber Crime*, 2013). Correspondingly, fear of the U.S.'s covert, yet lawful, access of foreign data has without question stood as "the most real, tangible and widely known challenge to its implementation within the legal sector" (Jackson, 2010).

Fuelling this complex web of fears surrounding cloud computing within the legal sector is the fact that, in the cloud computing industry, there exists "little traceability of the location at which one's documents are stored" (Baker, 2011, p. 57). Details such as server location are often undisclosed in cloud computing contracts, which often appear as "take it or leave it" standard term contracts which leave little room for any type of legal manoeuvring (Chabrow, 2012). Moreover, since contract negotiation with major cloud computing companies is often done remotely, legal professionals are typically unable to truly negotiate the specifics of each party's contractual obligations as they relate to privacy controls. Accordingly, it has been said that "cloud computing contracts [are often] *incomplete* in comparison to [. . .] standard long and thick outsourcing contract, which [are typically] extremely detailed" in terms of their security measures and server locations (italics added, Himmelsbach, 2011).

The terms and conditions of these agreements are, furthermore, frequently subject to change without client notification; thus opening up potential for cloud computing providers to bounce information from one server to another without notifying customers (Himmelsbach, 2011). The fact that the nebulous nature of cloud computing extends to its service contracts is potentially fatal to the private sectors' adherence to PIPEDA, a law which expressly states that the location of the information, including jurisdiction, *must* be disclosed if requests to this effect are made. Consequently, it appears that legal professionals involved in cloud computing may have the burden of disclosing the location of client information stored on remote servers without having the benefit of being contractually notified of the location of this information. The OPC recognizes this paradox, admitting, "it is often impossible for an organization to know precisely where information is flowing while in transit" (*Guidelines for Processing Personal Information*, 2009, p. 6). However, it cautions that this lack of information does not excuse private organizations from their duties under PIPEDA, noting that "the law is clear on where accountability lies and organizations must in their own best interests, as well as those of their customers, do what they can to protect the information" (ibid).

## Information Policy & Cloud Computing in the Legal Sector

Although wholly legal, cloud computing services may hold the potential to threaten the legal industry's adherence to PIPEDA's private sector privacy mandates. Similarly, in the event that third-party protective measures are breached, information which is classified under solicitor-client privilege and confidentiality duties would be rendered public, an occurrence which would effectively undermine the professional code of ethics to which the legal professional is bound. Making this issue more complex is a lack of cloud computing policies and procedures published for the legal industry, by the legal industry, as it has been observed that "[f]ew Canadian professional associations have developed rules or positions on the subject" (Michel-Adrien, 2011). Centrally, while the American Bar Association implemented amendments to the Model Rules of Professional Conduct, including the duty of confidentiality, in 2012, neither the Canadian Bar Association, nor the Barreau du Québec, have formulated a stance on cloud computing and its management (Millan, 2011). Likewise, as of March 2013 the only provincial law society to publish policies on cloud computing in a regional context has been the Law Society of British Columbia (Law Society of British Columbia, 2013). Prolonged absence of policies at the federal and provincial levels will only continue to perpetuate confusion over the benefits and risks of cloud computing within the legal industry, and further stall its wholesale adoption within the profession.

Ultimately, while the outsourcing of information is becoming a ubiquitous business practice within the digital age, it seems legal responsibility over this information cannot pass hands as easily. With liability always a risk, private organizations such as law firms must remain cognizant of the implications of their information management practices, and fully interrogative

of how they fall within the ethical confines of both professional and federal codes of conduct. Accordingly, policies on cloud computing must be developed to address legal professional's duties under PIPEDA and professional ethical codes, and work to reconcile these legal impetuses with the risks and benefits imbedded within cloud computing service models. To this end, these cloud computing policies should carefully assess the risks involved in the outsourcing of legal data to third party servers, including the sensitivity of the data, the risk of breach, and the legal ramifications of a breach.

Although cloud computing policies should, arguably, be implemented widely within the private sector, their necessity is particularly acute within the legal industry due to the strict codes of confidentiality that form the backbone of the judicial system. This implementation of uniform cloud computing policies within the Canadian legal sector may also afford individual legal firms or legal practitioners the type of leverage needed to exact more flexible and tailored cloud computing service contracts. Likewise, the legal profession – defined by those who understand the law and are able to mould it to meet their needs – holds the unique ability to create comprehensive and legally sophisticated cloud computing policies that could be easily adopted by other private sector organizations. Ultimately, in a world in which information is used to manage information, legal professionals need to be very careful to craft relevant policies before embarking on potentially perilous investments in cloud computing services whose latent risks are still only just emerging.

## References


Baker, Jonathan. (2011, January). Flying in the clouds: practicing law by cloud computing. *Florida Bar Journal*, *85(9*), 57-59.

Banks, Timothy. (2012, July 31). Cloud computing and the USA Patriot Act: Canadian implications. *Internet and E-Commerce Law in Canada*, *13(3),* 20-23. Retrieved from http://www.fmc-law.com/Publications/0712_Cloud_Computing_and_USA_Patriot_Act.aspx.

Brown, Jesse. (2013, February 6). Cloud hate: why Ottawa keeps losing our data. *McLean's*. Retrieved from http://www2.macleans.ca/2013/02/06/cloud-hate-why-ottawa-keeps-losing-our-data/

Buckler, Grant. (2011, December 1). Never mind the *Patriot Act*, watch your thumb drives. *ITWorldCanada.* Retrieved from http://www.itworldcanada.com/news/never-mind-the-patriot-act-watch-your-thumb-drives/144397

Chabrow, Eric. (2012, March 15). Avoiding pitfalls of cloud contracts. *GovInfoSecurity*. Retrieved from http://www.govinfosecurity.com/interviews.php?interviewID=1497

Dodek, Adam. (2011). Solicitor-client privileges: challenges for the 21st century. *The Canadian Bar Association*. Retrieved from http://www.cba.org/CBA/activities/pdf/Dodek-English.pdf

European Parliament: Directorate General for Internal Policies. (2013, January 20). Fighting cyber crime and protecting privacy in the clouds. Retrieved from http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050

Foley, John. (2008, August). Private clouds take shape. *Information Week*. Retrieved from http://www.informationweek.com/news/services/business/209904474

Fraser, David. (2011, April 18). Cloud computing and privacy FAQs. *Canadian Cloud Law Blog*. Retrieved from http://www.cloudlawyer.ca/2011_04_01_archive.html

Gallagher, Ryan. (2013, January 8). U.S. spy law authorizes mass surveillance of European citizens: report. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2013/01/08/fisa_renewal_report_suggests_spy_law_allows_mass_surveillance_of_european.html

Himmelsbach, Vawn. (2011, June 8). Canadian cloud contracts: liabilities and limitations. *ITWorldCanada*. Retrieved from http://www.itworldcanada.com/news/canadian-cloud-contracts-liabilities-and-limitations/143294

Jackson, Brian. (2010, May 20). Canadian firms shy away from cloud computing. *Itbusiness.ca*. Retrieved from http://www.itbusiness.ca/it/client/en/home/News.asp?id=57655

Law Society of British Columbia. (2013, January). Practice resource: cloud computing checklist. Retrieved from http://www.lawsociety.bc.ca/docs/practice/resources/checklist-cloud.pdf

MacLeod, Ian. (2013, February 2). Cloud computing law puts Canadian users at risk of snooping by American spies. *Ottawa Citizen*. Retrieved from http://www.ottawacitizen.com/business/Cloud+computing+puts+Canadian+users+risk+snooping+American/7907562/story.html

Martindale, Nick. (2011, August). In the future, cloud computing will be the only choice. *The Telegraph.* Retrieved from http://www.telegraph.co.uk/sponsored/technology/microsoft-cloud-computing/8667512/In-the-future-Cloud-Computing-will-be-the-only-choice.html

McKendrick, Joe. (2012, April 30). Cloud could cut $12 billion from US government annual deficit. *Forbes*. Retrieved from http://www.forbes.com/sites/joemckendrick/2012/04/30/cloud-could-cut-12-billion-from-us-government-annual-deficit-study/

Mell, Peter, and Grance, Timothy. (2012). The NIST definition of cloud computing. *U.S. Department of Commerce's National Institute of Standards and Technology.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Michel-Adrien. (2011, April 25). Canadian law firms adopting cloud computing. *Library Boy: Legal Research News from an Ottawa Law Librarian* (Blog). Retrieved from http://micheladrien.blogspot.ca/2011/04/canadian-law-firms-adopting-cloud.html

Office of the Privacy Commissioner of Canada. (2009). *Guidelines for processing personal data across borders*. Retrieved from http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm

Office of the Privacy Commissioner of Canada. (2011). *PIPEDA and your practice: a privacy handbook for lawyers*. Retrieved from http://www.priv.gc.ca/information/pub/gd_phl_201106_e.pdf

Office of the Privacy Commissioner of Canada. (2009). *Personal Information Protection and Electronic Documents Act.* Retrieved from http://www.priv.gc.ca/leg_c/leg_c_p_e.cfm

Rennie, Steve. (2013, January 17). Government faces class-action lawsuits over student loan borrowers' lost data. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/news/politics/government-faces-class-action-lawsuits-over-student-loan-borrowers-lost-data/article7492261/

Thompson, Graham. (2011, January 20). Cloud computing, the *Patriot Act*, and you. *Ottawa Business Journal.* Retrieved from http://www.obj.ca/Opinion/2011-01-20/article-2139749/Cloud-computing,-the-Patriot-Act-and-you/1