dentons.com

DENTONS

Insights and Commentary from Dentons

On March 31, 2013, three pre-eminent law firms—Salans, Fraser Milner Casgrain, and SNR Denton—combined to form Dentons, a Top 10 global law firm with more than 2,500 lawyers and professionals worldwide.

This document was authored by representatives of one of the founding firms prior to our combination launch, and it continues to be offered to provide our clients with the information they need to do business in an increasingly complex, interconnected and competitive marketplace.

f) Next steps

This tariff proposal was first filed for 2010, and has not yet been heard by the Copyright Board.

The deadline to file objections to the 2013 tariff proposal was **June 27, 2012**.

B. Record Labels/Performers

Performance of Sound Recordings: Re:Sound (Simulcasting and Webcasting)

a) Tariff proposal

For 2012, Re:Sound sought rates of up to **45%** of gross revenues for semi-interactive webcasting, subject to a minimum annual fee of **$720**.

For 2013, Re:Sound seeks **30%** of gross revenues for simulcasting or webcasting, subject to a minimum annual fee of **$30,000.**

b) Next steps

The Copyright Board hearing for the 2009-2012 proposals will begin in Ottawa on September 24, 2012.

Objections to the 2013 tariff proposal may be filed with the Copyright Board **by August 8, 2012.**

[*Editor's note*: Margot Patterson is certified by the Law Society of Upper Canada as a Specialist in Intellectual Property: Copyright, and represents music users in proceedings before the Copyright Board.]

---

1 The revenue base refers to the revenues used to calculate the royalty payable. See "Rates" in the section below.

2 The SOCAN proposed rates are based on a formula of A x B ÷ C, where "A" is the % of gross revenue; "B" is the number of plays/downloads requiring a SOCAN licence; and "C" is the total number of plays/downloads.

3 Like the SOCAN proposed rates, CSI proposed rates are based on a formula of A x B ÷ C, where "A" is the % of gross revenue; "B" is the number of plays/downloads requiring a SOCAN licence; and "C" is the total number of plays/downloads.

4 CSI is seeking the greater of 6.8% and the equivalent rate payable to SOCAN.

5 CSI is seeking the greater of 9.9% and twice the equivalent rate payable to SOCAN.

6 *Ibid*.

• CLOUD COMPUTING AND THE *USA PATRIOT ACT*: CANADIAN IMPLICATIONS •

Timothy M. Banks, Fraser Milner Casgrain LLP

A perennial issue in Canadian privacy law is what to do about the *USA Patriot Act*. Just when we think we have things reasonably sorted out, issues pop up again in a new context. This time, it is cloud computing.

What is the USA Patriot Act?

The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*[1] (usually referred to as the *USA Patriot Act* or just the *Patriot Act*) is United States legislation that was passed following the September 11, 2001, attacks on the World Trade Centre in New York City. Among other things, the *Patriot Act* made it easier for U.S. law enforcement officials to intercept electronic communications and business records. One of the controversial measures was that officials were granted the power to issue a National Security Letter to electronic communication service providers requiring them to hand over information without informing the affected parties (in some cases without any judicial oversight).

For the purposes of this discussion of cloud computing, one of the most important provisions of the *Patriot Act* is s. 215, which deals with access to business records. Section 215 repealed and re-enacted provisions of the U.S. *Foreign Intelligence Surveillance Act*.[2] Pursuant to s. 215 of the *Patriot Act*, the Federal Bureau of Investigation may apply to a federal judge for

an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities. U.S. commentators agree that this definition covers electronic business records.

What is cloud computing?

In its most complete form, cloud computing involves outsourcing applications (*e.g.*, e-mail, customer relationship management, and accounting software), platforms (*e.g.*, database architecture) and infrastructure (*e.g.*, servers). All of these IT functions are offered as a service to organizations either independently or as a package. An organization's data (*e.g.*, its e-mails) may be stored in segregated servers or intermingled with the data of other organizations and segregated through the functionality of the service provider's information technology. The organization accesses its data through Internet portals.

Where is the Cloud?

The cloud isn't in the sky. Data sent over the Internet in a cloud computing arrangement may be (and often will be) stored outside of Canada and may be intermingled with data from other organizations. In many cases, the cloud computing service provider may subcontract the storage of data to one or more organizations operating data centres. If these data centres are in the U.S., well, therein lies the rub. The data is going to be subject to the laws of the United States, including the *Patriot Act*. Actually, if the data is even accessible from the U.S. or by an organization subject to the jurisdiction of the U.S., the data is likely to be subject to the laws of the United States.

Is there a Canadian privacy problem?

All transfers of information create legal issues, particularly where the transfer is to a third party across borders. Organizations have a privacy "problem" every time they transfer data. This is because under Canadian federal and provincial private sector privacy laws, the organization that collected and is entitled to use the personal information remains responsible for its security throughout its lifecycle. Indeed, in many cases, organizations will have created a contractual obligation with individuals by incorporating the organization's privacy policy (and privacy commitments) into terms of service or use or other customer e-commerce contracts. An organization will need to assess carefully with legal advisors how commencing cloud service transfers of personal information will affect existing legal commitments. It may be necessary, for example, to give special notice to individuals and to provide them with opt-out or termination opportunities.

However, organizations are not prohibited from using U.S.-based cloud services (assuming they are only operating in the private sector). Federal and provincial private sector privacy legislation does not prohibit the transfer of personal information to an organization in another jurisdiction for processing and storing, provided that

- The transfer does not entitle the organization receiving the personal information to use that information for purposes other than those for which individuals expressly or impliedly consented.
- The transferring organization remains accountable for the protection of the personal information that has been transferred.

- The organization receiving the personal information provides a comparable level of data security, as would be required under Canadian law, and the terms on which the collecting organization collected the information.
- Disclosure is made to individuals. As a general rule, this disclosure to individuals should include notice that (1) their personal information will be transferred outside of Canada for processing and storage; (2) their personal information will be subject to the laws of the foreign jurisdiction; and (3) the laws of the foreign jurisdiction may be different (and less protective) than those of Canada.

The transferring organization will wish to consider obtaining meaningful contractual commitments to administrative, technological and physical security protections from the organization to which the personal information is being transferred. The transferring organization will also wish to consider audit or other rights that would permit ongoing diligence of these security protections, as well as the use being made of the personal information.

The *Patriot Act* does not mean that personal information will necessarily be subject to lesser security in the U.S. than in Canada. An interesting survey and comparison of surveillance laws in Canada, the U.S., the United Kingdom, and France was conducted by the Office of the Privacy Commissioner of Canada in 2009, which remains an important reference.[3] Since 1990, Canada and the U.S. have had a *Treaty on Mutual Legal Assistance in Criminal Matters*[4] in which, each country has agreed to assist the other with the investigation, including seizure of records, of criminal activity. The *Canadian Security and Intelligence Service Act*[5] provides for secret warrants for the interception and seizure of, among other things, electronic data. The *National Defence Act*[6] permits the Minister of Defence (without judicial supervision) to authorize the Canadian Communications Security Establishment to intercept communications relating to foreign entities under certain circumstances. In addition, the *Criminal Code*[7] permits seizures of electronic data. The combination of this legislation has led the Office of the Privacy Commissioner of Canada to conclude in three decisions[8] not only that Canadians are at risk of personal information being seized by Canadian governmental authorities (including without the knowledge of the target), but also that there is already a risk of that information being shared with U.S. authorities.

This is not to say that reasonable people cannot still differ as to whether they wish to have their personal information stored outside of Canada. As such, organizations should factor into their business model the possibility that companies or individuals who do business with them may have legitimate concerns about the theoretical increased risk that their personal information could be shared with U.S. authorities without any gate-keeping function of a Canadian policing, governmental or judicial authority.

Final Caution

There are additional complications when entering into cloud computing arrangements in which government data regarding citizens may be involved. Although it is beyond the scope of this article to enter into a complete discussion, it should be noted that there are restrictions in British Columbia and Nova Scotia (and probably Alberta) to storing data outside of Canada. In British Columbia, public bodies that are subject to the *Freedom of Information and*

Protection of Privacy Act are required to ensure that personal information under their custody or control is only stored in and accessible from Canada, subject to certain exceptions.[9] Similarly, the Nova Scotia *Personal Information International Disclosure Protection Act* requires that public bodies and their service providers ensure that personal information under their custody or control is stored and accessed only in Canada, subject to certain exceptions.[10] In Alberta, organizations are prohibited from wilfully disclosing personal information in response to a subpoena, warrant or order issued or made by a court, person or body having no jurisdiction in Alberta to compel the production of information or pursuant to a rule of court that is not binding in Alberta.[11]

[*Editor's note*: Timothy M. Banks is a partner in the Business Law Department of Fraser Milner Casgrain LLP and head of the firm's Toronto Research Group. He blogs at <www.datagovernancelaw.com>.]

---

1 115 Stat. 272 (2001).

2 50 U.S.C. ch. 36.

3 Privacy Commissioner of Canada, *Surveillance, Search or Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States* by Jennifer Stoddart (Ottawa: Office of the Privacy Commissioner of Canada, May 9, 2009) <http://www.priv.gc.ca/parl/2009/parl_bg_090507_e.pdf >. In addition, the submissions of Professor Michael Geist and Milani Homsi to the B.C. Information and Privacy Commissioner entitled "The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy" remain foundational research in this area. See <www.michaelgeist.ca/resc/FINAL_UNB.doc>.

4 Can. T.S. 1990 No. 19 (Canada Gazette, Part I, 1990, p. 953).

5 R.S.C. 1985, c. C-23, ss. 21-24.

6 R.S.C. 1985, c. N-5, ss. 273.65-273.69.

7 R.S.C. 1985, c. C-46 (*e.g.*, the provisions in Part VI).

8 *PIPEDA Case Summary #313*, [2005] C.P.C.S.F. No. 27; *PIPEDA Case Summary #333*, [2006] C.P.C.S.F. No. 10; and *PIPEDA Case Summary #394*, [2008] C.P.C.S.F. No. 7.

9 RSBC 1996, CHAPTER 165, s. 30.1.

10 S.N.S. 2006, c. 3, s. 5.

11 *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25, s. 92(3).

INVITATION TO OUR READERS

Do you have an article that you think would be appropriate for *Internet and E-Commerce Law in Canada* and that you would like to submit?

AND/OR

Do you have any suggestions for topics you would like to see featured in future issues of *Internet and E-Commerce Law in Canada*?

If so, please feel free to contact Michael A. Geist
@mgeist@uottawa.ca
OR
ieclc@lexisnexis.ca