Summer 2010 Vol 3 No 4

The Winston Report

a publication of The Canadian Association of Professional Access and Privacy Administrators

Highlights:

ISBN 978-0-9810758-7-7

Privacy in the Clouds
for Canadians

By Alec Campbell

The emergence of cloud computing, in which data is stored remotely on network servers and applications are delivered from the network as well, raises new issues for the management of privacy risk. Because neither data nor applications are stored locally, direct user control over privacy and data security is much reduced. This shifts the focus of risk management from the local computing environment to the environment managed by the application service provider.

This has advantages and disadvantages. On one hand, the user is largely spared the necessity of developing and maintaining privacy and security measures for his or her applications and data. (Some local responsibilities remain, such as local access control.) On the other hand, the user is left at the mercy of the service provider for most such measures and the service provider may have different standards than the user does.

The business benefits of cloud computing can be considerable (and they will increase over time as cloud computing services improve, especially on the application front) but so can the privacy and security risks. The trick is to find an acceptable balance between the benefits and risks.

Just as cloud computing is emerging as a viable alternative to locally installed applications and data, new requirements are emerging related to the protection of third-party privacy, especially by private sector organizations. In the United States, breach notification laws are becoming the norm. In Canada, the first breach notification legislation came into effect on May 1, when Alberta's amendments to its Personal Information Protection Act came into effect. Among those amendments are requirements for the reporting of privacy breaches to the Information and Privacy Commissioner when they involve a significant risk of harm to individuals. The Commissioner may then order that notification be provided to affected individuals. Also included in the amendments are provisions for notification of individuals when their personal information may be stored outside Canada. This is a significant issue for organizations that are considering the use of cloud computing.

Continued on page 2

Privacy in the Clouds
Continued from page 1

It is reasonable to expect that other Canadian jurisdictions will implement similar requirements over time. Even if they don't, good privacy practice will demand that the users of cloud computing take measures to address the unique privacy issues created by remote data storage and application delivery.

While we don't have room in this brief article to discuss all the implications of cloud computing in detail, here are some of the factors to consider:

- Contracts
  Cloud computing service providers usually have standard service agreements, which they do not like to customize. Canadian organizations considering cloud computing need to carefully review the service agreements to ensure that they include privacy and security provisions adequate for compliance with whatever Canadian privacy legislation applies. In some cases, hard negotiations may be required to arrive at a contract that adequately mitigates the privacy risks for Canadian users. This is especially the case if data and/or application servers are located outside Canada. The largest cloud computing service providers today are located in the United States, although some may have servers in Canada as well.

  Cloud computing service agreements must provide adequate security for, and access to, personal information to satisfy Canadian privacy legislation. From the limited non-scientific sample of service agreements I have reviewed, it appears that few American service providers could meet this standard.

  Canadian cloud computing service providers are emerging to specifically address the needs of Canadian organizations, especially for Canadian data storage. These service providers will guarantee Canadian data storage locations for such services as remote backup, hosted Microsoft Exchange services, hosted data storage, and application hosting. When they are available, the use of Canadian cloud computing service providers by Canadian organizations is advisable.

- Notice
  If there is any possibility that personal information will be stored outside Canada, affected individuals should be provided with notice of that fact, whether or not such notice is required in law. There is sufficient concern about such issues as the USA PATRIOT ACT in Canada that any organization that stores personal information outside Canada without notifying affected individuals runs a significant risk of privacy complaints.

- Audit Capability
  One of the potential problems associated with cloud computing is the ability to audit the service provider's facilities in the event that it is necessary for the investigation of a privacy breach. This is another area in which the negotiation of contract provisions with non-Canadian service providers may become difficult. Even Canadian service providers may be reticent to grant access to their facilities for investigation purposes, but at least they will be subject to the investigative powers of the privacy Commissioner for the jurisdiction in which their servers are located. The ability to access service provider facilities for investigation and audit purposes remains a significant issue for the use of cloud computing by organizations with significant privacy responsibilities.

- Knowing the Physical Location of Your Data
  One of the characteristics of cloud computing is that data may be spread over multiple physical locations, based on load balancing algorithms and other factors. At one point, I considered the use of a particular remote backup service, until I found out that the data could be distributed over any one of 23 servers located in half a dozen different countries. Even

Continued on page 4

The Winston Report
Summer 2010 edition

Editor In Chief — Sharon Polsky

Contributors

Alec Campbell
Barry Cahill
David T.S. Fraser
Mark Grady
Patrick Kenny
Carmen Mann
Toby Mendel
Monica Muller
Sharon Polsky
Hasnain Rizvi

September 28
International
"Right to Know Day"

though the data would be encrypted, this caused me some concern. For example, how was I to notify any individuals that might be affected where their personal information was backed up? Because of load balancing measures, the service provider moved its data around regularly. It was almost impossible to determine where all backup data were located at any one time. Certainly, such information was not routinely available from the service provider.

I later learned that this example was an extreme one, but cloud computing service providers deal with large volumes of data and need to actively manage the location of that data to maintain the efficiency of their data storage. Large cloud computing service providers may utilize multiple servers in multiple physical locations, and it won't always be possible to readily ascertain the physical location of any particular data.

- Encryption
  In my opinion, whenever one entrusts a third-party organization with the storage of personal information (or any other sensitive information), it is preferable that such information be encrypted. Therefore, I look for encrypted data storage in any third-party organization that will be storing sensitive information on my behalf. Any good remote backup service provider will offer encrypted data storage, although many of them retain secondary encryption keys to give them access to data in the event that is required for law enforcement purposes or customer support. I prefer to retain complete control over access to encrypted backup data, by holding all encryption keys, but others may be willing to allow the service provider to have limited access for emergency recovery purposes.

  Service providers who focus on cloud-based applications, as opposed to data backup, often do not offer encrypted data storage, although I expect this to change over time. Until it does, the lack of encrypted data storage for remotely hosted applications may be risky for Canadian organizations, especially if they are dealing with non-Canadian service providers.

- International Privacy Legislation
  If you are dealing with a non-Canadian service provider, it is important to know what privacy legislation governs them. In the United States, as we all know, there is no blanket federal privacy legislation, although companies are bound by FTC fair trade provisions to honor any privacy or security promises they make in their service agreements or privacy notices. Sector-specific US privacy legislation is unlikely to cover a cloud computing service provider, unless it offers services to healthcare organizations that are subject to HIPPA.

  Other countries, of course, have a variety of legislated privacy and security requirements. European Union privacy regulations are strict but differ in important details from Canadian legislation. Legislation in New Zealand, Australia, and Hong Kong bears resemblance to Canadian legislation in many respects, but differs in others. Elsewhere the privacy landscape varies widely, but rarely meets the standard imposed by Canadian legislation.

  Differences in privacy regulation and related security requirements are one more reason to look first for Canadian cloud computing service providers. To me, it's always preferable to deal with a service provider who is subject to legislation that is the same as, or very similar to, the legislation with which your own organization must comply.

These are just some of the considerations that an organization should keep in mind when looking at the benefits and risks of cloud computing. As noted at the outset, cloud computing can offer considerable business benefits. If you can adequately mitigate the privacy and security risks associated with such services, they may be of considerable value. If not they can be problematic, to say the least.

Alec Campbell is the president of Excela Associates Inc., which provides privacy consulting services across Canada from its base in Edmonton, Alberta. Before establishing Excela in 2006, Alec held senior privacy positions in the Government of Alberta and Alberta's Office of the Information and Privacy Commissioner. In the Commissioner's office, he led the development of that office's privacy impact assessment process. At the Government of Alberta, he founded the *Information Access and Protection of Privacy Certificate Program* at the University of Alberta and led government IT privacy functions, including the development of the award-winning GAEA Privacy Architecture.