CLOUD COMPUTING

Posted on July 24, 2015

Categories: Insights, Publications

In recent years there has been an exponential growth in cloud computing. As more organizations begin to explore whether some form of cloud computing would be beneficial to their businesses, it is important to consider relevant legal obligations.[1] In particular, since cloud computing almost inevitably involves cross-border transfers of information, if the data involved includes personal information,[2] organizations should be cognizant of privacy laws applicable to such transfers. In addition, cloud computing can give rise to some unique risks that will need to be taken into consideration.

What is cloud computing? What are the benefits?

There are many different definitions of cloud computing, each of which is slightly different. One helpful definition states that cloud computing is: "Internet-based computing in which large groups of remote servers are networked so as to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources."[3] In other words, cloud computing is a broad term that can encompass a range of online services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).

Some organizations have found that cloud computing can offer a range of benefits, which may include:

- **Cost savings** - Organizations may not have to invest in building their own information technology infrastructure, buying hardware or obtaining software licenses (depending upon the nature of the cloud computing services obtained);
- **Scalability** - Organizations can contract for as much or as little data storage/processing as they need at any given time, and services can be adjusted as needs change;
- **Accessibility** – Data can be accessed and/or processed from anywhere in the world where there is Internet access; and
- **Security** – In some respects, cloud service providers may offer a higher level of data security for some organizations, especially small or mid-sized businesses that do not have advanced controls in place.

Cloud computing may also offer other benefits, such as enhanced computing power, access to new innovations, and the potential for rapid deployment. However, although there may be benefits to cloud

computing, there are also legal requirements and restrictions, as well as other risks, that organizations should take into account.

Cross-border data transfers

Before "moving to the cloud", organizations should be aware of applicable laws and guidance from the privacy commissioners respecting cross-border transfers of personal information. Some legislation contains specific requirements or restrictions related to such activities. For example:

- *An Act* respecting protection of personal information in the private sector (Quebec)[4] provides that enterprises that communicate personal information outside Quebec or entrust a person outside Quebec with holding, using or communicating such information on their behalf, must first take all reasonable steps to ensure that the information will not be used for unauthorized purposes, and if the enterprise cannot ensure that it will not be used for unauthorized purposes it must refuse to transfer the information outside Quebec;
- The *Personal Information Protection Act* (Alberta) contains certain notice and policy requirements if an organization uses a service provider outside Canada;
- Public sector privacy legislation in British Columbia and Nova Scotia generally requires that personal information be stored and accessed only in Canada (subject to certain exceptions, including where consent is obtained); and
- Health information privacy legislation in Ontario, Nova Scotia and Newfoundland & Labrador also contains some limitations on cross-border transfers of personal information without consent.

In addition, organizations must ensure that cross-border transfers of personal information in the course of commercial activities comply with the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), including the requirement to obtain knowledgeable consent to collection, use and disclosure of personal information, as well as general security, openness and accountability obligations. There are a number of cases that provide guidance on complying with PIPEDA when transferring personal information outside of Canada, and the Office of the Privacy Commission of Canada (the "OPC") has published "Guidelines for Processing Personal Data Across Borders", which indicate that:[5]

- Although PIPEDA does not prohibit cross-border transfers of personal information, certain rules apply;
- Organizations remain accountable for information that is processed by third parties, and must protect such information;
- Protection of personal information processed by third parties is primarily accomplished through contract, however, contracts cannot override the laws of the recipient country;
- Organizations must assess risks to the integrity, security and confidentiality of personal information that

is transferred outside of Canada, including by taking into account the laws of, and the political, economic and social conditions in, the recipient jurisdiction; and
- Organizations must be transparent about their personal information handling practices, including advising individuals that their information may be sent to another jurisdiction and may be accessed by the courts, law enforcement and national security authorities in such jurisdiction.

Cases decided by the OPC and provincial privacy commissioners provide additional guidance for cross-border transfers of personal information. In addition, there are some industry-specific laws and guidelines that are relevant to cross-border data transfers. For example, the Office of the Superintendent of Financial Institutions has issued guidelines on "Outsourcing of Business Activities, Functions and Processes", which include some guidance on cross-border data transfers.[6]

Risks related to cloud computing

One of the risks of cloud computing is that it is a relatively new and largely unregulated industry. Therefore, a number of issues are still unresolved, including questions of legal jurisdiction and ownership of data. For example, it is unclear whether the data protection laws and government disclosure requirements of multiple jurisdictions could apply simply based upon the location of servers, even if the contracting parties and affected individuals are not located in such jurisdictions.

Other risks associated with cloud computing may include:

- Difficulty complying with the legal requirements described above. For example, it may be difficult to assess risks related to the legal, social and political condition of the recipient country, if the data passes through a number of different jurisdictions (and the cloud service provider may not disclose the countries where its servers are located);
- Since cloud computing can involve storing and transferring data across multiple servers, it may be difficult (or even impossible) to comply with legal obligations respecting disposal of personal information when it is no longer required to accomplish the purposes for which it was collected and/or when an individual revokes consent;
- Major cloud service providers often hold a vast repository of data, which can make them a target for cyber criminals;
- Since cloud computing relies on the Internet, there may be a higher potential for "crashes" or other service interruptions; and
- Many cloud service providers have standard terms and conditions of service, including broad waivers of liability respecting service levels and security, which they may claim are non-negotiable.

These risks should be taken into account when considering any form of cloud computing arrangement.

Best Practices

Given the risks involved in cloud computing, it would be prudent for organizations to consider performing a privacy impact assessment before implementing any such arrangement that would involve personal information. Such an assessment would include consideration of applicable legal requirements and restrictions, as well as the sensitivity of the information and the reasonable expectations of affected individuals.

It is also essential to carefully review and consider contracts governing cloud computing arrangements. Although privacy and data protection provisions are important in any contract with a service provider, they are particularly important in the context of cloud computing because of the high likelihood that the organization will not be able to determine the jurisdiction(s) where data will be transferred, stored and/or processed. Therefore, the organization may not be able to evaluate the data protection laws or the political, economic and social conditions of the recipient jurisdiction. Consequently, the organization may need to rely heavily upon the contract terms to ensure the integrity, security and confidentiality of personal information that is stored or processed in the cloud.

Wholesale acceptance of standard contract terms and conditions may not satisfy the organization's obligations under PIPEDA and other applicable legislation, if they do not provide for reasonable protection of personal information. In particular, the organization may need to negotiate: broad waivers of liability; provisions related to service levels and security standards; and terms governing ownership of data, including the right to have all data returned/deleted on demand or upon termination of the agreement. In some cases, it may also be possible to negotiate some restrictions upon the location where data will be stored.

For additional guidance on privacy and data protection provisions in contracts with service providers (including cloud service providers), see *McMillan's Privacy Basics Issue #6, Data Protection Agreements.*

Finally, organizations should consider the sensitivity of the information under their control. As noted by the OPC, it is not possible for any contract to override the laws of recipient countries. Therefore, for certain highly sensitive personal information, even the strongest contract terms may not provide sufficient protection. In such cases, organizations should consider whether the potential benefits of cloud computing outweigh the associated risks.

by Lyndsay A. Wasser

1 Note: This bulletin primarily focuses on issues related to the public cloud. Different considerations may apply to private clouds, community clouds and/or hybrid clouds.

2 Pursuant to applicable privacy legislation, "personal information" is information about an identifiable individual.

3 Cloud computing. Dictionary.com. Dictionary.com Unabridged. Random House, Inc. *http://dictionary.reference.com/browse/cloud computing* (accessed: July 09, 2015.

4 Quebec public sector privacy legislation contains similar requirements.

5 *https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp.*

6 *http://www.osfi-bsif.gc.ca/eng/fi-if/rg-ro/gdn-ort/gl-ld/pages/b10.aspx.*

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.