# Cloud Computing: Privacy and Other Risks

**by George Waggott, Michael Reid and Mitch Koczerginski, McMillan LLP**

## Introduction

While the benefits of outsourcing organizational data storage to the cloud are plentiful, so are the legal risks. An organization must be sensitive to the fact that it has legal obligations to protect the personal information for which it is responsible. The implementation of accompanying policies, the performance of appropriate due diligence and the maintenance of proper documentation are each essential to minimizing the risk of liability which may result from the improper use or disclosure of outsourced personal information. By transferring data to the cloud, an organization relinquishes a degree of control and, as a result, must manage the relationship between its privacy obligations in the jurisdiction where it collects personal information, and the governing privacy laws in the jurisdictions to which the data is transferred in order to limit its exposure to liability.

This paper seeks to outline the legal risks associated with the outsourcing of organizational data storage to cloud systems with a focus on Canadian privacy law. Part I discusses Canadian organizations' privacy obligations with regard to the collection, use, and disclosure of personal information pursuant to Canadian privacy legislation. Part II discusses some of the risks and possible liability associated with outsourcing data storage to the cloud. This section will provide an example of these risks and provide further insight about the *USA PATRIOT Act*. Finally, Part III supplies some guidance for organizations on how to implement cloud solutions while minimizing relevant risk.

# Part I – Canadian Privacy Legislation

## *Personal Information Protection and Electronic Documents Act* (PIPEDA)

*PIPEDA*[1] is Canada's private sector privacy legislation that governs the collection, use and disclosure of personal information in the course of commercial activity. It applies to organizations in the private sector, as well as federal works and undertakings (such as

[1] Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (PIPEDA).

banks and airlines). *PIPEDA* defines personal information to broadly encompass almost any information that can be attributed to an identifiable individual. The Ontario Court of Appeal has previously found that personal information, within the meaning of *PIPEDA* has a "...very elastic definition and [it] should be interpreted in that fashion to give effect to the purpose of *[PIPEDA]*.[2] The purpose of the Act is to recognize the right to individual privacy in a technological era that increasingly facilitates the exchange of information, by imposing obligations on organizations with access to individuals' personal information.

*PIPEDA* applies to all provinces and territories in Canada, except where a jurisdiction has enacted substantially similar legislation, in which case that jurisdiction's legislation applies instead of *PIPEDA*. Currently Alberta, British Columbia and Québec have each enacted substantially similar legislation, while Manitoba has very recently passed its own legislation which is awaiting proclamation to come into force.

In the provinces where *PIPEDA* applies, both individuals and the federal Privacy Commissioner may initiate complaints where they believe an organization is not in compliance with the legislation. The Commissioner is empowered by *PIPEDA* to investigate complaints, issue reports that include findings, and to make recommendations. Following the release of a Commissioner's report, an individual may make an application to the Federal Court. The Court may then order the offending organization to comply with *PIPEDA* and award damages.

According to *PIPEDA*, personal information may generally only be collected, used and disclosed with the knowledge or consent of the individual. Therefore, it is important for organizations to explain to individuals what personal information will be collected, how it will be used, and to whom it may be disclosed, and then to ensure that such personal information is always dealt with in such a manner. The use of cloud-based data outsourcing can add an extra layer of information to be disclosed to individuals regarding their personal information, and additional consent may be required. It is also important that personal information that is collected is necessary for the purposes indicated to the individual as *PIPEDA* prohibits collection, use or disclosure of personal information that goes beyond what is actually necessary for those purposes.

[2] Citi Cards Canada Inc. v. Pleasance, 2011 ONCA 3.

## *Alberta's Personal Information Protection Act* (Alberta PIPA)

While *Alberta PIPA*[3] has been declared substantially similar to *PIPEDA*, there are two important requirements that an organization considering outsourcing data storage should be aware of which do not exist under *PIPEDA*.

First, *Alberta PIPA* imposes notice and policy requirements on organizations that outsource data storage to foreign service providers. These requirements apply to any organization that directly or indirectly either transfers personal information to a service provider outside Canada, or uses a service provider outside Canada to collect personal information. At the time of collection or transfer of information, the organization must inform the individual to whom the information relates about certain matters. In particular, notice is required regarding the way the individual may obtain access to the organization's policies and practices with respect to service providers outside of Canada, together with the name and title of a representative who is able to answer questions. Further, if an organization uses a service provider outside of Canada to collect, use, disclose or store personal information, it must be able to provide individuals with written information regarding its privacy policies and practices with respect to foreign service providers, which must include a listing of the applicable foreign countries, as well as the purpose for which the service provider has been authorized to collect, use or disclose the information.

Second, *Alberta PIPA* imposes a mandatory breach reporting procedure in the event personal information is accessed or disclosed without authorization. While other Canadian Commissioners recommend that organizations report privacy breaches, currently only *Alberta PIPA* specifically requires notice. The legislation provides that the responsible organization must notify the Commissioner with details about the breach without unreasonable delay. Further, where there is a risk of harm to the individual with whom the information is concerned, the Commissioner may require organizations to notify the individual directly with the details of the breach.

---

[3] Personal Information Protection Act, SA 2003, c P-6.5 (Alberta PIPA). As of this writing, the *Alberta PIPA* has been declared unconstitutional by the Supreme Court of Canada (in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62), which found that the legislation acted to unduly restrict a union's Charter-protected right of free expression by limiting its ability to collect, use and disclose personal information in the furtherance of a labour dispute. While *Alberta PIPA* was declared unconstitutional in its entirety, the Court suspended application of its ruling for 12 months in order to allow the Alberta legislature to bring the *Alberta PIPA* into compliance, where balance must be struck between individual privacy rights, and freedom of expression.

## British Columbia's *Personal Information Protection Act* (BC PIPA)

While substantially similar to *Alberta PIPA* in many respects, for the purposes of an organization outsourcing data storage to the cloud, *BC PIPA*[4] does not require much in addition to what is required under *PIPEDA*. However, it should be noted that the BC Commissioner is empowered to make binding orders to organizations to change their practices and to levy fines if an organization does not comply with *BC PIPA*.

## British Columbia's *Freedom of Information and Protection of Privacy Act* (BC FIPPA)

Unlike the other Canadian privacy legislation reviewed in this paper, *BC FIPPA*[5] addresses personal information that is in the custody or control of a public body. While *BC FIPPA* does not directly apply to private organizations, it does affect any organization which provides a service to a public body governed by *BC FIPPA*, where that service involves personal information in the custody or control of the public body.

Subject to certain limited exceptions, *BC FIPPA* requires that personal information in the custody or control of a public body is only stored in and accessed from inside Canada. Individuals may provide consent for the storage or access of their personal information outside Canada. However, practically speaking, the consent requirements often make it impractical to seek such consent. Similar requirements can be found in Nova Scotia's *Personal Information International Disclosure Protection Act*[6].

## Québec's *An Act Respecting the Protection of Personal Information in the Private Sector (Québec Private Sector Act)*

While the *Québec Private Sector Act*[7] has been declared substantially similar to *PIPEDA*, there are some important differences that an organization outsourcing data storage to cloud systems should consider. For instance, the *Québec Private Sector Act* has a broader scope than *PIPEDA* and applies to non-commercial activities and contains restrictions on the transfer of information outside of Québec. In addition, the *Québec Private Sector Act* enshrines the protection of a fundamental right to privacy. Therefore, a violation of the Québec legislation could constitute a violation of an individual's right to privacy, permitting

---

[4] Personal Information Protection Act, SBC 2003, c 63.

[5] Freedom of Information and Protection of Privacy Act, RSBC 1996, c. 165.

[6] Personal Information International Disclosure Protection Act, SNS 2006, c.3.

[7] An Act respecting the Protection of personal information in the private sector, RSQ, c P-39.1.

the affected individual to bring a claim for punitive damages, in addition to any other damages available.

# Part II – Risk Of Outsourcing Data Storage To The Cloud

## Outsourcing Service Does Not Outsource Risk

It is crucial for organizations considering implementing a solution using the cloud to understand that outsourcing data storage to a cloud service provider does not outsource an organization's privacy obligations pursuant to Canadian privacy law. The Ontario Privacy Commissioner, Ann Cavoukian, recently opined that "the critical question for institutions which have outsourced their operations across provincial and international borders is whether they have taken reasonable steps to protect the privacy and security of the records in their custody and control. I have always taken the position that you can outsource services, but you cannot outsource accountability."[8] Therefore, an organization considering making use of cloud services must understand the associated risks. Some of these risks, which are discussed below, include the creation of new data streams and jurisdictional issues that arise from transferring personal information across borders. However, these are not the only inherent risks related to cloud-based data storage. There are additional practical and legal risks not discussed in this brief paper, some of which include security of information in the cloud, misuse of processed data, ownership of data while in the cloud, and the permanence of data once in the cloud.

## Creation of New Data Streams

The nature of cloud computing and storage creates an additional concern for organizations which are under an obligation to protect the personal information they are responsible for pursuant to Canadian privacy legislation. Every time data in a cloud system is accessed, processed, transferred, or stored, a substantial amount of transactional information is documented. To the extent this secondary data can be attributed to an identifiable individual, the relevant data may itself also constitute personal information under Canadian privacy legislation in which case it needs to be afforded the same protection as the primary data.

---

[8] Privacy Investigation Report, *Reviewing the Licensing Automation System of the Ministry of Natural Resources*, (June 27, 2012), Online: <http://www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf>.

### Jurisdictional Considerations

It is important to remember that information that is uploaded to the cloud may be sent from one jurisdiction, processed in a second jurisdiction, and stored in yet a third jurisdiction. Depending on the application of the data protection laws and relevant approaches, the data may be accessed in a way that does not comply with the governing Canadian privacy legislation. Therefore, the organization responsible for the data must be concerned with both the protection of the information in each jurisdiction that it is transferred through as well as the safeguards used to protect the data while it resides in the cloud.

### *USA PATRIOT Act* and Lawful Access

The jurisdictional issues discussed in the previous section are illustrated by the application of the *USA PATRIOT Act*[9] to cloud systems under US law. A major jurisdictional issue that can arise relates to lawful access which refers to the process of obtaining access to communications data pursuant to lawful authority. The *USA PATRIOT Act* is an acronym for the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, which the US Congress enacted in response to the terror attacks of September 11, 2001. Among other things, the *USA PATRIOT Act* makes it easier for the US government to obtain lawful access to electronic communications and business records. This arguably poses a serious risk to organizations that need to comply with Canadian privacy legislation as information may be disclosed for a purpose other than that indicated to the individual from whom it was collected.

## Part III – Tips To Minimize Risk

The privacy concerns discussed in the previous section are the cause of considerable apprehension for Canadian organizations contemplating outsourcing data storage to cloud servers subject to foreign jurisdiction. The concerns are not frivolous, as compliance with Canadian privacy legislation is essential to an organization in terms of both reputation and limiting financial liability. Fortunately, an organization hoping to enjoy the benefits of outsourcing data storage to the cloud can overcome these issues by understanding its privacy obligations and implementing adequate privacy policies and practices.

### Implement A Privacy Compliance Program For Your Organization

An organization considering outsourcing its data storage to a cloud service provider may significantly minimize its risk of liability by implementing a privacy compliance program that

[9] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub L No 107-156, 115 Stat 272 (2001).

addresses its collection and use of personal information in the cloud. The policy should be drafted in accordance with any applicable privacy legislation that is binding on the organization. While each of *PIPEDA*, *Alberta PIPA* and *BC PIPA* have their own unique characteristics, for example, the legislation is complementary, and a single privacy policy can generally address all applicable privacy legislation. If an organization will be storing information on a cloud system then such a practice should be included in the policy. A company should also ensure that any cloud service provider that it partners with has in place a clear and consistently applied privacy policy.

An organization must also identify the purpose for any collection, use or disclosure of personal information to the applicable individual and should also seek consent for these activities. It is important that customers and employees are aware of the organization's privacy policy and how it is applied.

## Be Selective with the Type of Data Being Outsourced

By outsourcing data storage to another service provider, an organization unquestionably loses a level of security and control over the data. As a result of such a loss of security and control, the organization's ability to ensure compliance with Canadian privacy legislation is limited. In some cases, the separation between the organization and the stored data might result in the organization not even being aware of a breach when it occurs. Therefore, understanding that outsourcing data storage necessarily creates a risk of misuse or unauthorized disclosure of personal information, an organization should be selective with the type of data being outsourced. For instance, an organization might outsource the majority of its data storage to a cloud service provider while storing its most confidential data locally. Such a practice should significantly minimize an organization's risk of liability while enjoying the benefits of cloud storage, as its most at-risk data remains under direct organizational security and control.

## Know Your Service Provider's Information Storage Practices

The best way for an organization to manage its risk is to understand the practices and policies of the cloud service provider it uses. An organization should consider where its information will be stored and whether jurisdictional issues arise. Additionally, an organization should consider whether its data will be stored in a way that intermingles it with the data from other organizations. If so, an organization should be aware of who else might have access to its data and insist on appropriate protections.

An organization should also consider the effect of storing, accessing, and processing its data using the service provider in the context of creating new data streams. For instance, a company should consider whether audit trails are generated, maintained, and whether it may gain access to such logs.

When negotiating with a potential service provider, an organization should be mindful to limit the service provider's use of data to the purpose for which it is collected, and require that information should be returned or destroyed when the contract is finished or terminated. An organization should also require that any data, whether primary or secondary, should not be disclosed without consent. To the extent lawful, an organization should also consider imposing an obligation to resist orders to disclose information without consent, or at least provide advance notice of any such order.

# Conclusion

This paper has provided a brief overview of some key issues for an organization to consider when planning to outsource data storage or processing to a cloud service provider. Part I discussed an organization's obligations with regard to the collection, use, and disclosure of personal information pursuant to Canadian privacy legislation. Part II discussed some of the risks and possible liability associated with outsourcing data storage to the cloud. Finally, Part III provided some tips for an organization to take steps to minimize these risks.

While the outsourcing of such tasks may provide extensive benefit to an organization, it also has the potential to impose legal liability. By providing a brief overview of the relationship between the cloud and a Canadian organization's privacy obligations, this paper has hopefully provided guidance on best practices in evaluating its needs with regard to switching to a cloud system.

*George Waggott practices workplace law and acts for management in employment and compensation matters. He may be contact at george.waggott@mcmillan.ca.*

*Michael Reid practices business law and has significant experience in technology matters, including IT issues. He may be contact at michael.reid@mcmillan.ca.*