

# Data Security — The Case Against Cloud Computing

*Bernice Karn*

*Partner, Cassels Brock & Blackwell LLP*



CASELS BROCK  
LAWYERS

MARCH 31, 2011

# Data Security – The Case Against Cloud Computing

March 31, 2011

Bernice Karn

Partner, Cassels, Brock & Blackwell LLP<sup>1</sup>

## Introduction

From a legal perspective, the need for data security by cloud users is a given. The user wants the data to be secure, period. At its most basic level, this means that the data entrusted to a cloud provider should not be subject to unauthorized access or disclosure or to modification or corruption. However, other risks are also inherent in cloud computing. This paper takes the position that, in spite of the perceived economic advantages of cloud computing such as scalability, speed to market, lack of capital investment by the user, and leaving computing functions to the experts (i.e., cloud providers) key business should never be entrusted to the cloud.

## What Does “Cloud Computing” Mean?

Although definitions of cloud computing vary among experts in the field, the National Institute of Standards and Technology (“NIST”) in the U.S. defines cloud computing in terms of characteristics, service models and deployment models.<sup>2</sup> According to Peter Mell and Tim Grance of NIST, cloud computing means “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.”<sup>3</sup>

---

<sup>1</sup> The author gratefully acknowledges the assistance of Rashesh Mandani, Student-At-Law in the preparation of this paper.

<sup>2</sup> Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing* (2009), online: National Institute of Standards and Technology <<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>>.

<sup>3</sup> Peter Mell & Tim Grance, “Effectively and Securely Using the Cloud Computing Paradigm” (Presentation delivered at the National Institute of Standards and Technology, 7 October 2009), online: NIST <<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt#313.81>>.

## Characteristics

NIST describes five characteristics of cloud computing that attract users. The five characteristics identified by NIST are:

1. *Cloud computing is an “On Demand” service.* Classifying a service as “on demand” means that the user can unilaterally provision computing capabilities automatically without the need for any human interaction with each service’s provider. So, through the user interface the user may be able to order additional network storage space or possibly schedule server time.
2. *Broad network access.* Whether the user is accessing infrastructure, platforms or software, all are available over the network and accessed through standard mechanisms that promote use by various types of thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
3. *Resource pooling.* The cloud provider uses a multi-tenant model to pool computing resources. These resources, both physical and virtual, are dynamically assigned and reassigned according to consumer demand. In addition, the resources may be varied by type of equipment and may be located in any number of disparate jurisdictions.
4. *Rapid elasticity or scalability.* In a cloud computing model, the computing resources can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in as required by user demand.
5. *Measured Service.* Cloud systems have the ability to measure the service and therefore control and optimize resource use (e.g., storage, processing, bandwidth, and active user accounts). This monitoring and control ability provides transparency for both the provider and consumer of the utilized service.

Other widely recognized benefits of cloud computing include: the cost savings of using a multi-tenant model; centralization of resources making maintenance, sustainability, management and control of resources easier; the perceived environmental benefits of building and operating fewer servers; standardized and hardened images offering better resilience against malicious attacks, and leaving the operation of sophisticated systems to the experts (i.e., the cloud provider).

## Service Models

NIST has identified three “service models” through which cloud computing is offered. They are:

1. *SaaS* The concept in “Software as a Service” is the simple use of the cloud provider’s applications running on a cloud infrastructure. The user does not manage or control the underlying cloud infrastructure such as the network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. This is a very “commercial off the shelf” example of cloud computing.
2. *PaaS* The next layer of complexity in cloud computing, “Platform as a Service”, as far as the user is concerned, is to deploy onto the cloud infrastructure consumer-created or acquired applications using programming languages and tools supported by the provider. As in the case of a SaaS model, the user does not manage or control the underlying network, servers, operating systems, or storage, but in the case of a PaaS model, the user does have the ability to control the deployed applications and potentially application hosting environment configurations.
3. *IaaS* The most comprehensive model of cloud computing is known as “Infrastructure as a Service”. In this model, the provider supplies the required processing, storage, networks, and other fundamental computing resources and the user is able to deploy and run any software that it may require, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

## Deployment Models

Finally, NIST identifies four different types of deployment models for the foregoing service models. These deployment models are:

1. *Private cloud*. The cloud infrastructure is operated solely for one organization. It may be managed by the organization or a third party and may exist on premise or off premise. Arguably this may be the most secure type of infrastructure, depending on the nature of the controls deployed and the diligence of the operator.
2. *Community cloud*. In this model, the cloud infrastructure could be shared by several organizations and supports a specific community or interest group that has shared concerns (e.g., mission, security requirements, policy, and

compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

3. *Public cloud*. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
4. *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

## **Security Benefits to the Cloud**

Reasonable arguments do exist that security is enhanced through the cloud rather than degraded. Cloud service providers pose the following types of arguments in support of the position that cloud computing is secure:<sup>4</sup>

- Cloud providers use built-in backups and safeguards that are not found in many desktop and enterprise servers;
- In a cloud application, security upgrades and patches can be deployed immediately to all users (unlike in a desktop model where installation depends on the user and, as a result, often does not happen);
- All users receive the same high level of security regardless of their size or industry;
- Most organizations operating systems in-house cannot match the technological expertise of a cloud provider;
- Because data are fragmented and dispersed throughout the cloud, the data are not readable by humans;
- Compliance analysis may be simplified since the user has only one cloud system to deal with versus many in house systems;
- The cloud provider is an uninterested third party, so it has no motivation to see the user's data;
- Disaster recovery and data storage are cheaper in the cloud due to volume;

---

<sup>4</sup> Barry Reingold & Ryan Mrazik, "Cloud Computing: The Intersection of Massive Scalability, Data Security and Privacy (Part 1)" (2009) 14:5 Cyberspace Law 1 at 2-3, online: Perkins Coie <[http://www.perkinscoie.com/files/upload/PS\\_09-06\\_Cloud\\_Computing\\_Article.pdf](http://www.perkinscoie.com/files/upload/PS_09-06_Cloud_Computing_Article.pdf)>.

- Cloud providers use real time intrusion detection systems and on-demand security controls.

Although the concept of cloud computing or software as a utility has been around since at as early as 1965<sup>5</sup>, mainstream adoption of cloud computing is a relatively new phenomenon, so the track record of cloud providers in upholding these standards is not yet well known or documented. Many of the arguments above only hold water if the cloud provider is truly professional and is dedicated to the highest level of security and due diligence. So, what are the risks that should concern the cloud user?

### **Security Risks in the Cloud**

In 2008 Gartner identified the following seven major security issues users face when entrusting data to the cloud:<sup>6</sup>

1. Privileged user access – who at the cloud provider has access to the data?
2. Regulatory compliance – will the cloud provider be prepared to allow external audits for regulatory purposes?
3. Data location – where are the data? In the cloud, data could be stored in any or many jurisdictions.
4. Data segregation – what does the cloud provider do to ensure that each user's data remain segregated from the data of others?
5. Data recovery – if the cloud provider experiences a disaster, what happens to the user's data?
6. Investigative support – how can a user respond to e-discovery requirements and other investigations into its records?

---

<sup>5</sup> Yanpei Chen, Vern Paxson & Randy H Katz, *What's New About Cloud Computing Security?* Technical Report No. UCB/EECS-2010-5 (Berkeley, CA: University of California at Berkeley for Electrical Engineering and Computer Sciences, 2010) at 3, online: University of California at Berkeley <<http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf>>.

<sup>6</sup> Jon Brodtkin, "Gartner: Seven Cloud-computing Security Risks", online: (2008) Network World <<http://www.networkworld.com/news/2008/070208-cloud.html?page=1>>.

7. Long term viability – how can the user protect itself in the event that the cloud provider goes out of business or is acquired by another company?

### **What Risks Aren't New?**

Some commentators have observed that risks in the cloud encompass existing and new threats. At a very basic level, cloud computing really is a combination of web applications and data hosting. Therefore, cloud computing is not immune to issues such as “phishing”, downtime, data loss, password weaknesses and compromised hosts running botnets, all of which are issues that have been around for some time.<sup>7</sup>

### **What Special Security Risks Does the Cloud Pose?**

In the “cloud” environment, however, creative purveyors of malicious code have new tools at their disposal. For example, one cloud risk for users is the other “tenants” in a multi-tenant model. In a virtualized computing world where virtualized servers exist on one physical box, it is possible to place an “attack” virtual server on the same hardware as a target virtual server and then build a side channel between the two that could enable an SSH (which means “secure shell”, a network protocol that allows data to be exchanged using a secure channel between two networked devices) keystroke timing attack to learn passwords.

Any time that computing resources are shared by a number of users, the potential exists for virtual neighbours to gain visibility to a user’s activity patterns, which might potentially enable the creation of covert and side channels into the neighbour’s data. It has also been posited that the activity patterns themselves may be confidential information that could lead to reverse-engineering of a digital customer base or discovery of revenues.<sup>8</sup> A complicating factor is that in a multi-tenant environment, it may be difficult to actually identify the user that is conducting the malicious activity.<sup>9</sup> Types of malicious activity conducted by co-tenants or even possibly the cloud provider

---

<sup>7</sup> *Supra* note 4.

<sup>8</sup> *Ibid.*

<sup>9</sup> *Ibid* at 3.

could include “brute force” attacks (a method used by hackers to break data encryption by trying all possible keys until the correct one is found<sup>10</sup>), botnets (a collection of software agents, or robots, that run autonomously and automatically and are often used to conduct spam or denial of service campaigns<sup>11</sup>) or scanning of co-tenants’ confidential information. These problems can be particularly troublesome when co-tenants are business competitors as well.

Association with bad virtual neighbours in a cloud model can pose reputational risks for the cloud user. An example of this was Amazon’s elastic compute cloud (“EC2”) service that allowed users to write applications that ran in and used computing capacity in the cloud. In this 2009 example, Spamhaus, a real-time blacklist provider, listed all Amazon EC2 IP addresses on its blacklist for spamming. ISPs and various other network participants such as email servers, network devices and antispam appliances rely on Spamhaus for up to date lists of IP addresses that are generating spam<sup>12</sup>. The result was that most network devices would automatically reject email emanating from anyone using an EC2 IP address. Non-spamming EC2 users were forced to deal directly with Spamhaus to have their IP addresses de-listed.

Another reputational risk incident on a more low-tech level involved FBI raids on a datacenter in Texas in 2009. On suspicion of facilitating cybercrimes, the FBI seized equipment at various datacenters and co-tenants in the facility suffered disruptions or business closures. According to Wired Magazine<sup>13</sup> the raids were a result of complaints by ATT and Verizon about unpaid connectivity bills by VoiP providers. Regardless of the reason for the raids, apparently the agents seized not only the suspects’ equipment but also the equipment of many other cloud customers who were essentially innocent virtual bystanders, severely, if not completely, disabling their operations.

---

<sup>10</sup> *Brute-force Attack*, online: Wikipedia <[http://en.wikipedia.org/wiki/Brute\\_force\\_attack](http://en.wikipedia.org/wiki/Brute_force_attack)>.

<sup>11</sup> *Botnet*, online: Wikipedia <<http://en.wikipedia.org/wiki/Botnet>>.

<sup>12</sup> Carl Brooks, “Amazon EC2 Email Blocked by Antispam Group Spamhaus”, online: (2009) SearchCloudComputing.com <<http://searchcloudcomputing.techtarget.com/news/1371369/Amazon-EC2-email-blocked-by-antispam-group-Spamhaus>>.

<sup>13</sup> Kim Zetter, “FBI Defends Disruptive Raids on Texas Data Centers”, online: (2009) Wired <<http://www.wired.com/threatlevel/2009/04/data-centers-ra/#>>.

The three service models described by NIST complicate matters. Users could conceivably be using SaaS from one vendor, but that vendor in turn operates its SaaS offering on another supplier's PaaS. (One example of this is ClaimVantage, a cloud-based insurance claim processing SaaS offering that is based on the Salesforce.com platform.) Further, the possibility exists (subject to the availability of sufficient application program interfaces) for PaaS providers to operate on yet another provider's IaaS. Therefore, the user could be dealing with a multi-vendor and multi-tenant problem. This extended chain of participants complicates the risk in using the cloud.

Other data security concerns that users can legitimately raise about a cloud environment are:

- *Data commingling* – How robust are the controls by the cloud provider to isolate one user's data from that of another? What memory/disk partitioning methods are used by the cloud provider? Is the provider able to segment its network in any way? If competitors are using the same cloud provider, is there a danger that their data may become commingled and available to each other?
- *Data ownership* – While there would seem to be no question about the ownership of data that the user uploads to the cloud, what position does the cloud provider take about derivatives of this data that the cloud provider generates in the performance of cloud services? Typical cloud contracts put the onus on the customer to represent its ownership right to the data that it uploads; the contracts are often silent on the ownership of derivatives.
- *Data Location* – By now many of us are familiar with the concern over U.S. government agencies accessing data stored in the U.S., sometimes without warrant, by virtue of extraordinary powers made possible through the amendments to various U.S. statutes by the *USA PATRIOT Act*. In a cloud model where, because of the networked environment, data could be stored in many jurisdictions around the world, users face the possibility that the "laws of the land" of the countries in which data are stored could enable local governments or other third parties to obtain access to the data, in spite of what the contract between the cloud user and provider says.
- *Data retention* – How long are data retained by the cloud provider and is the retention period long enough to satisfy the user's legal obligations? If the cloud provider does destroy the data, what process does it use and is it robust enough to actually destroy the data? Is the process secure?

- *Transition Out/Timing* - When the cloud contract expires, what assurance does the user have that all of its data is effectively returned to it or destroyed without the cloud provider retaining any copies? How can the user determine the extent of the data that it has in storage with the cloud provider? What type of “off ramp” is available to the user – i.e., if the cloud provider can end the contract on fairly short notice, the user may not have the ability to easily bring all of the data back in house or the time to find another acceptable service provider.
- *Consolidation of providers* – If the user becomes reliant on cloud computing services and no longer maintains the requisite data processing capabilities in house, what position is the user in if the industry consolidates and there are fewer choices of providers? The user loses leverage (if it ever had any in the first place) to demand strong data security protection.

## **Regulatory and Industry Concerns**

Any Canadian organization seriously contemplating cloud computing services really needs to start with an analysis of the regulatory framework that applies to it.

Government ministries or agencies that would be subject to freedom of information legislation will have different concerns from private enterprises that would be subject to the *Personal Information Protection and Electronic Documents Act*. Similarly, financial institutions subject to OSFI oversight may have different concerns from other non-regulated entities. However, a few statutes and rule making organizations bear note.

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

PIPEDA applies to the collection, use and disclosure of personal information in the course of commercial activities. Although PIPEDA does not prohibit the transfer of personal information outside of Canada and does not explicitly speak of cloud computing applications per se, Principle 7 of Schedule 1 of PIPEDA, provides as follows:

#### **4.7 Principle 7 — Safeguards**

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

##### **4.7.1**

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or

modification. Organizations shall protect personal information regardless of the format in which it is held.

#### **4.7.2**

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

#### **4.7.3**

The methods of protection should include

- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
- (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and
- (c) technological measures, for example, the use of passwords and encryption.

#### **4.7.4**

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

#### **4.7.5**

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

Therefore, organizations that collect, use or disclose personal information about individuals in Canada have certain obligations under PIPEDA to maintain security safeguards in respect of that information. In addition, Clause 4.1.3 of Principle 1 states:

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Therefore, not only does PIPEDA require that organizations maintain security safeguards in respect of personal information, it goes further to require that any third party processing that information be subject to comparable safeguards. It's safe to say that a cloud provider would fall under that “third party” category.

PIPEDA also places limits on the retention of personal information. Principle 5 of Schedule 1 states that “personal information shall be retained only as long as necessary for the fulfillment of those purposes” (for which it was collected). The use of personal information for new purposes requires fresh consent of the data subject. In a cloud context, the cloud provider cannot be permitted to retain personal information indefinitely or to use it or its derivatives for new purposes. If the cloud provider does either of these things, it will be the cloud user who will most likely bear the brunt of any investigation or sanctions, especially if the cloud provider is not resident in Canada.

Other PIPEDA obligations that need to be passed on to a cloud provider (and which a cloud provider may resist in the form of a contractual commitment) include:

- Designating an individual to oversee privacy compliance;
- Implementing policies and practices to give effect to PIPEDA’s privacy principles;
- Limiting collection of personal information and collecting it only by “fair and lawful means” – this could be an issue if the cloud’s interface collects more information than necessary for the user’s requirements and if the information is collected and then used for other purposes, particularly such as data mining;
- Maintaining personal information in an accurate, complete and up-to-date state as necessary for the purposes for which it was collected;
- Making information readily available about the organization’s personal information practices; and
- Providing individuals with access to their personal information when requested.

The challenge for a cloud customer is to try to satisfy these statutory requirements when faced with a cloud provider, particularly a cloud provider in another jurisdiction, where the cloud provider is only willing to point to its own

privacy policy as evidence of its privacy practices and insists on reserving the right to change those practices at any time.

### OSFI Guideline B-10

Financial institutions in Canada subject to oversight by the Office of the Superintendent of Financial Institutions (“OSFI”) must comply with Guideline B-10, *Outsourcing of Business Activities, Functions and Processes*.<sup>14</sup> This Guideline prescribes various contractual requirements that financial institutions need to ensure are present in material outsourcing contracts that they might sign. The Guideline defines “outsourcing” as: “an agreement between an FRE and a service provider, whereby the service provider performs a business activity, function or process that is, or could be, undertaken by the FRE itself”.<sup>15</sup> (“FRE” is a reference to “federally regulated entity”.) As financial institutions turn to cloud providers to perform functions that the institutions no longer wish to perform in-house, those contracts with cloud providers, if material to the business, will need to meet the requirements of this Guideline.

Guideline B-10 requires the financial institution to undertake a risk assessment of outsourcing an activity and due diligence on the service provider. These risks will vary with the nature of the outsourcing, and the location of the service provider. OSFI expects that financial institutions will pay “particular attention to the legal requirements of that jurisdiction, as well as the potential foreign political, economic and social conditions, and events that may conspire to reduce the foreign service provider’s ability to provide the service, as well as any additional risk factors that may require adjustment to the risk management program”.<sup>16</sup>

---

<sup>14</sup> Canada, Office of the Superintendent of Financial Institutions, *Guideline B-10: Outsourcing of Business Activities, Functions and Processes*, revised ed (Ottawa, OSFI, March 2009), online: OSFI <[http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/b10\\_e.pdf](http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/b10_e.pdf)>.

<sup>15</sup> *Ibid* at 4.

<sup>16</sup> *Ibid* at 11.

Guideline B-10 provides specific and helpful guidance on contractual provisions that financial institutions must ensure are included as part of the final outsourcing contract. Among these provisions are requirements related to the security of information. The Guideline requires that the outsourcing contract:

- reflect the financial institution's requirements for confidentiality and security. The Guideline suggest that the security and confidentiality policies adopted by the service provider must be commensurate with those of the FRE and be appropriate and meet a reasonable standard in the circumstances;
- identify the party that has the responsibility for data protection mechanisms, the scope of the information to be protected, the powers of each party to change security procedures and requirements;
- outline the notification requirements if there is a breach of security;
- identify the party that is liable for any losses that might result from a security breach; and
- require that the service provider logically isolate the financial institution's data, records, and items in process from those of other clients at all times, including under adverse conditions.

Although at one time the processing of data by a financial institution outside of Canada required an exemption order, that is no longer the case, but federal financial institution legislation such as the *Bank Act* still requires that certain records of financial institutions (such as daily transaction records) be maintained in Canada at the financial institution's head office) and that OSFI have access to them.<sup>17</sup>

Guideline B-10 has detailed audit requirements that a financial institution would be expected to impose on a cloud provider in order to verify that the service is being provided in the manner expected under the contract. This audit right includes a review of not just the service and its controls, but also the service provider's financial strength, prospects, technical competence and use and

---

<sup>17</sup> SC 1991, c. 46, s 239(1).

performance of significant subcontractors.<sup>18</sup> This type of ongoing and extensive due diligence is beyond that which many cloud providers will permit and, therefore, those cloud applications would not be good candidates for federally regulated financial institutions.

### E-Discovery

Another thorny issue that comes up in cloud computing is e-discovery. Organizations involved in litigation are required by the rules of court in the jurisdiction in which the lawsuit is conducted to produce documentation relevant to the suit in question. The fact that the information may be stored by a cloud provider is not an excuse for not providing the required information. A discussion of e-discovery issues is beyond the scope of this paper, but suffice it to say that it is an issue that needs to be addressed when entering into a contract with a cloud provider. The cloud provider will not want to tie up computing or human resources to deal with e-discovery requests while the customer will need the widest possible rights to access its data to satisfy discovery requirements.

### PCI DSS Compliance

PCI DSS refers to the “Payment Card Industry Data Security Standard”. Although this is a standard created and maintained by a consortium of payment card organizations and is not a statute, for those entities who are involved in credit card transactions such as retail merchants, PCI DSS compliance is critical and is mandated by the terms of the various merchant agreements with the payment card brands.

Although the PCI Security Standards Council has created and maintains these operational and technical standards to protect cardholder data, the actual payment card brands enforce compliance. The standards apply to all organizations that store, process or transmit cardholder data, so cloud providers that deal with payment card information should be extremely familiar with these

---

<sup>18</sup> *Supra* note 13 at 17.

standards. If they are not, then warning bells should sound for the cloud customer.

The PCI DSS is based on twelve security principles. Although the form entitled “Attestation of Compliance for Onsite Assessment – Service Providers”.<sup>19</sup> lists the following requirements for PCI compliance, these are described in much more detail in other PCI publications.<sup>20</sup> The twelve security principles are:

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.
- Use and regularly update anti-virus software.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data by business need to know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security.

---

<sup>19</sup> PCI Security Standards Council, *Attestation of Compliance for Onsite Assessments – Service Providers, Version 2.0* (2010), online: PCI Security Standards Council <[https://www.pcisecuritystandards.org/documents/pci\\_dss\\_aoc\\_service\\_providers.doc](https://www.pcisecuritystandards.org/documents/pci_dss_aoc_service_providers.doc)>.

<sup>20</sup> *Ibid* at Documents Library, online: PCI Security Standards Council <[https://www.pcisecuritystandards.org/security\\_standards/documents.php?category=supporting&document=pci\\_dss\\_saq\\_navigating\\_dss#pci\\_dss\\_saq\\_navigating\\_dss](https://www.pcisecuritystandards.org/security_standards/documents.php?category=supporting&document=pci_dss_saq_navigating_dss#pci_dss_saq_navigating_dss)>.

## Tips for the Cloud User

As of the writing of this paper there is no international data security standard, regulation or treaty in place to police cloud computing. Whether one will ever be developed remains to be seen. Given the pace at which technology advances, it is a given that any such standard or regulation would seriously lag behind advances in cloud computing in any event. As a result, it is up to each individual cloud user to make an informed decision as to the type of data that it is prepared to entrust to the cloud and to negotiate the best cloud computing deal that it can. Given the “as is” nature of many of the cloud services, it may well be that the computing requirements for only trivial or non-critical aspects of an organization’s business will be off-loaded to the cloud.

However, if an organization does wish to press ahead with a cloud computing contract and if the organization does have concerns about the security of data, what types of protections should it seek? The following is a non-exhaustive list of suggestions:

- Confidentiality – Most cloud agreements will contain some form of confidentiality clause whereby the provider promises to maintain the confidentiality of the data and the user promises to maintain the confidentiality of the system itself. While this might sound like an iron-clad guarantee that there will not be a security issue, note that the service provider will also limit its liability and for confidentiality and privacy breaches by sheltering those liabilities under a limitation of liability.
- Acknowledgement of customer’s data ownership/No data mining – Related to confidentiality above is the issue of data ownership. As between the customer and the service provider, it is industry standard that the customer would own the data that it supplies to the cloud. However, as mentioned earlier in this paper, issues can arise about derivatives of this data or even meta data about the customer’s use of the service. The customer should strive to ensure that all derivatives, all usage data and all meta data are vested in the customer and that the provider is not entitled to use them. An assignment of ownership back to the customer of the derivatives and meta data should be included to evidence this ownership interest.
- Auditing controls – Ideally any type of cloud arrangement should permit the user to audit the provider’s security and control systems, including user authentication, its processing and storage of information procedures, its disaster recovery and backup procedures, and its physical and organizational safeguards in relation to user data. In reality, particularly for an “as is” type of cloud application, the provider will not permit this because, understandably, it cannot have hundreds of customers descending upon it to audit its operations. Customers sometimes

agree to accept a CICA 5790 or SAS 70 Type II report on the effectiveness of the service organization's controls. (Note that the SAS 70 reports have recently been revised by the American Institute of CPAs).<sup>21</sup>

- Physical, organizational, technical restrictions – As noted above, statutes such as PIPEDA refer to the requirement for these types of controls. The exact nature of the controls will vary by each user's tolerance for risk. Given the pace at which technology changes, it is often impossible to pinpoint in a contract the types of restrictions required – it is usually only possible to use a functional approach to speak to the types of harms to be avoided. However, it is suggested that some minimum requirements be inserted with a covenant for the service provider to upgrade them over time in accordance with leading industry practices acceptable to the user. For an “as is” service, that is likely a big “ask”, but for a customized cloud solution, it may not be.
- User authentication and management – Again, contractually it's not really practical to require compliance with a specific type of user authentication technology that is frozen at a point in time. It is more important to describe the desired outcomes such as:
  - only users with the “need to know” and appropriate user authorization should be able to access or modify customer data;
  - restrictions on archiving and backup so that the user knows where the data reside and who has access;
  - restrictions on accessing and moving data to and from a specific location.

These questions really go to the question of IT security governance and to what extent they are reflected in the contract. Does the agreement define standards for access control, authentication, encryption (discussed below), maintenance of data integrity, availability, handling, and backup? Does the provider use systems that are assessed or certified by any neutral third party? Does the provider practice good organizational governance by segregating duties amongst its staff so that no one person has too much control over the data? Does the cloud service have an adequate and auditable log of the accesses, views, uses, copying, printing, modifications and disclosures of the data?

- Strong passwords – The user could require that the cloud provider only accept strong passwords from all co-tenants and all provider administrators touching the system. Strong passwords would have a combination of letters, number and symbols and would not be easily discoverable.
- Encryption – As noted above, many providers already provide for encryption of data while in transit. However, data at rest is a more difficult issue. Encryption of

---

<sup>21</sup> American Institute of Certified Public Accountants, Service Organization Control Reports (formerly SAS 70 reports), online: American Institute of CPAs.  
<<http://www.aicpa.org/InterestAreas/AccountingAndAuditing/Resources/SOC/Pages/SORHome.aspx>>.

data at rest is not yet a widely accepted standard. For sensitive data this is a must and any user thinking of the cloud to store or process sensitive data should be considering this issue. It may not be achievable, but if nothing else, the user will make an informed decision about the service that it is procuring.

- *Incident Responses and Escalation Procedures* – These issues should form part of any service level commitment that the user is able to extract from the cloud provider. Ideally the cloud contract would provide that, when a security incident comes to the attention of the cloud provider, the incident is reported to the user, along with the description of the potential effects and the provider’s remediation efforts. Some negotiation will be required over what a “security incident” actually is. Does it mean an actual unauthorized disclosure of a customer’s data or is it something less obvious than that – an unauthorized access or modification or even just the routing of the data through a jurisdiction that is not acceptable to the user? What about keystroke logging that is detected? What of security incidents affecting co-tenants? For the “out of the box” cloud computing contract, it is likely that the user will only learn of unauthorized disclosures of its own data. However, for more sensitive data that are entrusted to the cloud, the customer should push for as much disclosure as possible in respect of as many threats as possible.

Of course disclosure of security incidents is only one piece of the puzzle. Now that a security incident (however defined) has occurred, what is the provider doing about it to remediate the problem? What is the “chain of command” on the service provider side so that the customer knows who to contact and to whom it may complain?

Many U.S. states now have data breach notification laws and, if the former Bill C-29 is re-introduced into Parliament after the May 2 election,<sup>22</sup> PIPEDA may soon follow suit. One would think that a security breach would be the provider’s responsibility. However, this writer has noticed that cloud contracts, when they do speak to breach notification, promise co-operation in notifying the customer of the breach and in sometimes remediating it, but generally stop short of taking responsibility for bearing any significant cost or liabilities in respect of the breach. In the realm of risk allocation, this is a risk that cloud providers do not incorporate into their pricing model. In other words, for the low cost of a cloud service, the cloud provider will argue that it is not an insurer in respect of these types of risks.

- *Change Management* – Most “out of the box” cloud solution contracts do not speak to change management. This is more of an issue for customized situations. However, it is something for users to think about in terms of the diligence that the provider uses in implementing changes to its security processes and the notice, if any, that customers might receive. From the

---

<sup>22</sup> Bill C-29, *An Act to amend the Personal Information Protection and Electronic Documents Act*, 3<sup>rd</sup> Sess, 40<sup>th</sup> Parl, 2010 (first reading 25 May 2010), online: LEGISinfo <<http://www2.parl.gc.ca/Sites/LOP/LEGISINFO/index.asp?Language=E&query=7020&List=toc&Session=23>>.

customer's perspective, the more transparency the better, and it is useful if the provider will provide firm contractual commitments to provide that transparency so that the user can decide whether or not it wishes to continue with the service following a change.

- Subcontracting – Many service providers take the position that “it’s our service, so why do you care how we deliver it as long as you get what you bargained for”? That’s true on some level, but it’s a bit trite to say that, especially when dealing with a large cloud computing contract involving vast amounts of sensitive information. The customer needs to manage its own risk and part of that risk management is having some level of comfort that the entity actually performing the work is bound by the contractual commitments that the cloud provider is giving to the customer. OSFI Guideline B-10 touches on this issue in that any material or significant subcontracting of any outsourced services is expected to provide that the subcontractor is subject to the security, confidentiality, and audit and inspection rights of the main agreement. The customer may also want to impose contractual qualifications on the types of persons engaged as subcontractors. Prison labour is not unheard of in the outsourcing world!<sup>23</sup>
- E-Discovery – As discussed above, access to records is required for e-discovery purposes. The cloud contract should provide a commitment as to the type of records that the customer will be able to track and access and for how long.
- Destruction/Retention – Whether to comply with the requirements of PIPEDA, a specific statute, or a company’s general records retention obligations, data destruction and retention is an issue that needs to be addressed in a cloud contract. The customer will need a commitment on what will be destroyed, how, where and when. Depending on the sensitivity of the information, the customer may also seek to audit this process.
- Transparent Metering – As most cloud services are sold on a “pay as you go” model, the contract should provide for some method for the user to verify its usage of the services.
- Rules for co-tenants – Most cloud providers have an “acceptable use policy”. This should be read carefully to determine the types of activities that are prohibited. As usual, the activities described in documents of this nature are usually well behind the technical capabilities and creativities of spammer and hackers, but the user should familiarize itself with the rules applicable to all users and extract a covenant from the provider that it will enforce the rules against all users without discrimination.
- Business Continuity - One of the benefits that cloud providers tout is that the service is “always available”. Google recently announced that it has removed its

---

<sup>23</sup> Stephanie Overby, “Prison Labor: Outsourcing’s ‘Best Kept Secret’”, online: (2010) CIO <[http://www.cio.com/article/595304/Prison\\_Labor\\_Outsourcing\\_s\\_Best\\_Kept\\_Secret](http://www.cio.com/article/595304/Prison_Labor_Outsourcing_s_Best_Kept_Secret)>.

exclusion for scheduled downtime from its service level agreement for Google Apps.<sup>24</sup> From a security perspective, the customer needs to ensure that any provision of the service through any backup provider is subject to the same level of security requirements as the primary service provider.

- *Jurisdictional Issues in Disputes* - Of course, as in the case of every commercial contract, the cloud contract will provide for the governing law to interpret the contract and may provide for the dispute resolution venue as well. The user should consider this issue carefully in terms of the jurisdiction – are there any specific laws or case law in that jurisdiction that might negatively affect the outcome of a suit between the provider and the customer? In addition, when the service provider agrees to abide by “applicable law”, what does that really mean – the law that applies to the service provider in its home jurisdiction or the laws that apply to the customer? If the customer is concerned about ensuring that certain laws must be adhered to, then to avoid any disputes later, those laws should be specified.

The Cloud Computing Alliance has published useful materials that discuss, at a very granular level, the best practices, according to a number of different standards, for ensuring cloud security (to the extent possible). Readers are encouraged to consult these materials at [www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org).

### **Where Does This Leave the User?**

Unfortunately, many cloud providers take the position that, precisely because their service is a “multi-tenant” model that leverages the ability to provide exactly the same service for many users to provide a low-cost solution, the cloud provider is often not willing to contractually agree to any clauses that may require the provider to perform the service differently for any particular customer. For example, many providers will offer encryption for data in transit but not at rest, since encryption at rest goes beyond current industry standards and may degrade the performance of the service<sup>25</sup>. Any user who wants to ensure that their data are encrypted while at rest would be out of luck. In other words, you get what you pay for and as a user, you can take it or leave it.

---

<sup>24</sup> Jamie Yap, “Google: 100 percent uptime 'not attainable'”, online: (2011) ZDNet <<http://www.zdnetasia.com/google-100-percent-uptime-not-attainable-62206206.htm>>.

<sup>25</sup> *Supra* note 3 at 2.

Taking the service “as is” usually means agreeing to a general confidentiality covenant, a covenant to comply with the provider’s security and privacy policies that may change over time and very strict limitations of liability on the part of the cloud provider. Sometimes the provider will not even provide an actual covenant on security or privacy; instead, the contract will merely reference the applicable policies and provide a URL where they may be found, without ever actually contractually promising to abide by them. Unlike an extensively negotiated software licensing arrangement where representations and warranties about performance are an integral part of the deal, in a cloud environment the provider will often insist on the “as is” nature of the service.<sup>26</sup>

## **Conclusion**

Cloud computing does offer many possibilities for scalability of high-powered computing resources at low cost. Notwithstanding the hype, it is incumbent upon users to do their homework and investigate the provider, their operations, their security processes and their contractual commitments. As in any relationship where a third party is entrusted to perform a valuable service, make sure that the third party is reputable, qualified and responsive. Ignoring the risks may at best lead to disappointment and at worst lead to a reputational meltdown and loss of business. Caveat emptor.

---

<sup>26</sup> Simon Hodgett, “Cloud Computing Contracting and the Spectrum of Risk” (Paper delivered at the Thirteenth Annual Canadian IT Association Conference, 23 October 2009) at 14, online: <[http://www.it-can.ca/direct/membersonly/2009conf/cloud\\_computing\\_hodgett.pdf](http://www.it-can.ca/direct/membersonly/2009conf/cloud_computing_hodgett.pdf)>.

Cassels Brock & Blackwell LLP

2100 Scotia Plaza, 40 King Street West, Toronto, ON Canada M5H 3C2  
Phone 416 869 5300 Fax 416 360 8877 [www.casselsbrock.com](http://www.casselsbrock.com)

© 2009 Cassels Brock & Blackwell LLP. Cassels Brock and the CB logo are registered trade-marks of Cassels Brock & Blackwell LLP. All rights reserved.