

Cloud Computing: Backup and Storage  
Brian Mauch  
October 2014

### *What is the cloud?*

If you've been living under a rock for the last five years, you might not have seen or heard the marketing efforts by Microsoft, Apple and the other technology giants regarding the benefits of *working in the cloud*. Even if you have been exposed to the hype, you may still be wondering what exactly *the cloud* is. To put it simply, cloud computing means keeping your data or software somewhere other than on your computers in your office, and accessing it via the internet. This includes everything from web-based services to remote access to watching movies on your phone. The term *cloud* comes from the use in diagrams of a cloud-shaped symbol as an abstraction for the complex infrastructure of the internet. The cloud is nothing new. Most people have been using the cloud since they got their first dial-up internet connection in the '90s – it just wasn't called that back then.

### *Why would lawyers use the cloud?*

The proliferation of high-speed internet connections and web-based application development has opened the door to a new option for law firms: cloud-based applications. There is no shortage of websites that are offering pay-as-you-go online services to small law firms, which previously would have required significant capital investment in on-premise hardware, software, ongoing maintenance and backup. The effect of these cloud-based applications has been to "level the playing field" by giving small firms access to productivity tools which formerly only large firms could afford.

### *What is cloud backup?*

One of the common uses for the cloud is offsite backup for a law firm's data. It is important to keep an onsite backup of data, in order to quickly recover from typical data loss such as deleted or misplaced files and emails. But it is equally important to keep an offsite backup of data, to protect against local disasters such as fire, flood or earthquake. While magnetic tape was the standard for backup for many decades, it has been overshadowed by hard disk and cloud backups due to shorter recovery times, falling price and increasing capacity of disks, as well as the increasing speed of broadband internet access. Hybrid disk (for onsite) and cloud (for offsite) backups can automate what was previously a manual process with tape cartridges, making it more reliable and not prone to human error and forgetfulness.

### *Is data in the cloud secure?*

Security and privacy are paramount at law firms in order to protect client confidentiality. For this reason, law firms should take reasonable steps to protect their clients' data against unauthorized access. While data security is not always assured in an on-premise network, there are more factors to consider when utilizing cloud backup and applications, because the data is stored off-premise.

In January 2013, the Law Society of BC published a due diligence checklist, intended for lawyers who are considering using cloud services. This checklist is available on the LSBC website at <http://www.lawsociety.bc.ca/docs/practice/resources/checklist-cloud.pdf>. The checklist is 13 pages long, and contains over 150 considerations when evaluating a specific cloud service. The substantial

length of the checklist was intentional – it was drafted to be inclusive of as many of the potential issues as possible.

While it is important for lawyers to review the entire checklist, I think there are four key considerations that should be taken into account when contemplating using cloud services in a BC law practice:

1. Utilize services that keep lawyers' data (and backups of their data) in Canada, and ideally within BC. This measure alone will satisfy many of the compliance questions in the checklist, and will remove any concerns about the USA Patriot Act or jurisdictional authority. Lawyers also need to be aware of circumstances where there is a statutory requirement to keep data within Canada. An example of this is ICBC's requirements for personal injury defence firms, which stipulates that client data cannot be stored in international services such as Gmail and Hotmail.
2. Ensure that the ownership and intellectual property rights of the data do not pass to the cloud provider, and that the confidentiality and privilege of clients' data is protected. To do this, lawyers must review the cloud provider's SLA (Service Level Agreement) and Privacy and Confidentiality Agreement. If the necessary provisions are not in place, the lawyer must negotiate the necessary changes to the agreements before proceeding.
3. Use services that are focused on the legal profession, and have therefore been designed with lawyer's requirements in mind. For example, Dropbox is a convenient file transfer utility designed for a broad audience including consumers and home users. However, Dropbox is not a good choice for BC lawyers, because it stores data in Amazon's Simple Storage Service (S3) which is located in multiple data centres across the USA, and it lacks some security features which are critical to the exchange of confidential data. Instead, the due diligence questions raised in the checklist should lead a lawyer to use a Canadian-based virtual data room service that is designed for law firms.
4. Refer to the due diligence checklist, and document the answers for each cloud service that is used. Lawyers should occasionally go back review the checklist, in case the cloud provider has changed an aspect of their service, or the law firm has changed how they are utilizing the cloud service. If something goes wrong in the future, it will be important to prove that the proper due diligence was done.