How to safely put your data in the cloud

Cloud services help you access and store data on someone else's server. You may not realize it, but Dropbox, Gmail, Facebook, and legal specific applications like Clio are all examples of cloud services.

Putting data on the cloud raises issues like maintaining confidentiality, usability, cost, portability and applicability to your area of practice. Keeping in line with the *Rules of Professional Conduct* is the primary concern.

Balancing your needs with these concerns may likely take time and effort – talk to colleagues about their preferred cloud services, read up on the terms of service, and decide which works best for you.

What is the cloud?

"The cloud" is a metaphor for information that is transmitted over the internet and stored on a server outside of your firm.

It helps to obtain your client's consent to store data in a cloud service. This is also a good opportunity to talk with your client about both the benefits and the risks involved with cloud services. A practical place to request the client's consent is the retainer agreement. Take a look at LawPRO's precedent retainers on the practicepro.ca website.

Whether you are keeping your clients' data on a cloud service or in a filing cabinet, the *Rules of Professional Conduct* require you to maintain confidentiality.

Here are some key questions to ask when you are considering using a cloud service from a confidentiality point of view.

Is your data encrypted at-rest or in-transit?

Your data is more secure when it is encrypted. Encryption takes your data and scrambles it so that it is unintelligible, and only someone with the decryption key can unscramble the data. There are two places that your data should be encrypted in the cloud. *Encrypted at-rest* means that data is encrypted while it is stored on the cloud-based server. If the data is stolen or retrieved from the cloud by someone other than you, it is likely impenetrable if the encryption cannot be broken.

Encrypted in-transit means that data is encrypted while it travels from where you are inputting it to the cloud-based server. If the data is stolen while traveling to and from the server (snooping), that data will remain unintelligible so long as the encryption holds. Check the terms of use of the cloud service to determine if the data is encrypted both at-rest and in-transit. Although encryption at rest and in transit are the gold standard some commonly used legal software application providers may have reasons why they do not encrypt data at-rest. You may want to discuss that with your provider and make an informed decision.

Who holds the encryption key?

The level of security achieved when data is encrypted at-rest and in-transit depends, in part, with the number of people who hold the key to unlock the encryption. If you are the sole owner of the key, then if anyone other than you retrieves the data they can only read it if they can crack the encryption. If you lose the key, no one at all can easily decrypt and access the data. You may need extra IT support in this case. On the other hand, if the keys are held by the owners of the cloud service, then they have the ability to access your information at any time. If a cloud service is compelled by law to release data, it could be forced to decrypt your data and release it, possibly without notifying you. In terms of maintaining confidentiality, it is better if you are the sole owner of the encryption key.

Where is the data stored?

Data that is stored on servers located out side of Canada may be subject to the laws in that jurisdiction. Foreign laws such as the U.S. *Patriot Act* or the Prism program may allow foreign entities to access the cloud service (and your data), with or without your knowledge or permission. This may also apply to servers located in Canada as digital laws evolve. Read the terms of service to obtain information regarding when or how a cloud service responds to a legal notice or request for the release of data.

In addition, it's worth noting that cloud services may need to comply with privacy and regulatory laws in the server/company's jurisdiction, such as the *Personal Information Protection and Electronic Documents Act (PIPEDA)* in Canada and the *Sarbanes-Oxley Act (SOX)* in the United States.

What are the default security settings?

Some cloud applications allow for security settings to be managed, while others do not. If security settings are not properly set, your data may, by default, be available to others. For this reason it is important to learn about the security measures the cloud application uses and makes available to you, including the default settings.

How strong is your password?

The longer a password is, the harder it is to guess. Until very recently the convention for secure passwords was 12 or more random characters. It is now suggested that four random words are more secure (there are websites that can help you pick four random words). Do not use the same password for multiple websites or applications. More and more people are using password managers to help them manage and remember multiple passwords. LastPass, 1Password, Dashlane and KeePass are widely used password managers.

Is there two-step verification?

Most Canadians are familiar with two-step verification (or two-factor authentication), such as when you use an ATM to withdraw money from a bank account. An ATM requires two security steps to gain access to your account: inserting a bank card with a unique identification, and inputting a PIN number. Similarly, in the cloud context, two-step verification can include requiring both a password and a separate code sent to your mobile phone. The extra layer of security means that if a hacker steals your password and attempts to log-in through an unrecognized IP address (e.g., using a computer or location that you have never used), the hacker cannot login without having access to your mobile phone too.

The cloud service acts as the steward of your data. It is important to ensure that your data is always available and won't be lost. If the cloud service becomes hacked or goes out of business, can you get your data back? It isn't as simple as it is with a paper file, where you can walk down the hall and take a look at a file and search for a missing memo. Nor is it like driving to the backup storage container and taking a look at the file there. Data on a cloud service is typically located in a secure location far, far, away. It may require special tools to retrieve the data in a legible format. And you may be totally dependent on the cloud service to retrieve your data. If the cloud service is not available, will you be left holding an empty bag? With some cloud services, these concerns can be addressed. Consider the following questions when selecting a cloud service.

Can you backup locally to your own computer/server?

While most cloud services have their own backups, some allow you to take a "belt and suspenders" approach to maintaining your data, which means that you can keep a copy of the backup yourself on your own computer (called a "local" backup). If your internet becomes unavailable or if the cloud service becomes unavailable (due to a hack or any other reason), you can use the local backup to continue working. You would also likely need another application, typically provided by the cloud service, installed on your computer so that you can access the local data. This is an excellent feature, as it means you aren't completely reliant on the cloud service's uptime to do your work. If a cloud service goes down, you can still use your local backup in the meantime.

How can the backup be retrieved and how long will it take?

Most cloud services perform backups, which includes making an extra copy of your data elsewhere in their system. If the data is destroyed, some cloud services may be able to restore your data quickly, while others may take days if not weeks to do so. Can your law firm function while the data is stuck on the cloud service and they are "working on it"? How long will it take before the cloud service is able to restore your data? The lost time can be costly.

How often is backup done?

By now virtually every cloud service has a backup system. However, it may be more difficult to obtain information about how often a backup can be done. Can information be restored from one hour ago, one day ago, or one week ago? Backup should be segregated into different time periods, so that you can restore your data from different time intervals.

If the cloud service ceases to operate or closes down, how can you extract your data?

A cloud service can suffer from business problems like any other business. It can cease to be profitable and close down, it can be hacked, it can upgrade and leave users who refuse to upgrade in the dust. Is there a way to extract your data in a timely manner and in a form that is usable? Data that is extracted may be kept in proprietary databases, making the data nonsensical except to the most advanced user. You may have to spend extensive money and time to move the data into a new cloud service or database if the data is hard to extract and hard to read.

The seemingly inevitable trend is that law firm data will shift to cloud services. Whatever its limitations in practice, it is already an acceptable way to run a law firm and store data. Both clients and lawyers appreciate the speed, ease-of-use and accessibility of data that cloud services provide. Remember to keep up-to-date with patches and perform regular backups. It also helps to understand the terms of use of a cloud service. The Law Society of British Columbia has an excellent cloud computing due diligence guideline[1] and cloud computing checklist[2]. Be professional and keep an eye on the *Rules of Professional Conduct* to maintain confidentiality and your law firm's uptime when using a cloud service. ■

Avoid Ransomware

Typically, a ransomware infection happens when you have clicked on a link on a website in a phishing email. Over a period of time (it could be days or weeks), the ransomware will encrypt Word documents, PDF files, pictures and other data files on the computer without your knowledge. At some point when you attempt to open an encrypted data file, a window will pop-up demanding a ransom payment in bitcoin (so it is untraceable) worth several hundred to several thousand dollars. The ransom demand promises a decryption key when the ransom is paid. One way to avoid paying the ransom is to restore your data to a time before the ransomware attack happened. To do this you must have a full backup of your data from a point in time that is days or even weeks earlier. You'll likely lose the data you have created in the meantime.

Ian Hu is Counsel, Claims Prevention and practicePRO at LawPRO.

[1] lawsociety.bc.ca/docs/practice/resources/guidelines-cloud.pdf

[2] lawsociety.bc.ca/docs/practice/resources/checklist-cloud.pdf