

Cloud Computing

The information provided and the opinions expressed in this monograph are solely those of the author. Neither the State Bar of Texas nor the author are rendering legal, accounting or professional advice and assume no liability in connection with the suggestions, opinions, or products mentioned.

What is cloud computing?

Cloud computing is a term used to describe off-site storage or software as a service that utilizes Internet connectivity to access its benefits. In other words, instead of being stored on a local computer or server, data is stored on a remote server.

Why does it matter?

The cloud is significant to attorneys because it provides inexpensive storage, networking, and collaborative capabilities as well as an off-site backup for your files. Instead of buying an expensive server and having to install LAN,¹ you can simply share files through a service called “Dropbox.” Dropbox is a program that stores your files off-site and immediately uploads when you save it to the file. If you have Dropbox installed on your other computers and mobile devices, it makes the changes on those devices as well. In 2013, it was free for the first 2 GB of storage, and \$100 per year for 100 GB. I have been using Dropbox for all of my files, and I have only used 32 GB to date. This is inexpensive insurance to safeguard your files and make them accessible wherever you are. If any of you have had a hard drive fail, you know how valuable this service can be.

There is a true story of an attorney in Alabama whose computer and hard drives were stolen from her office. Because she had all her files on Dropbox, she was able to have her office up and running within hours after purchasing new computers. You never know what kind of human or natural disaster can destroy your paper and electronic files. If the courts and attorneys who lived in New Orleans at the time of Katrina had had access to a service like Dropbox, they could have worked remotely on their files wherever they fled to and nothing would have been lost.

I emphasize Dropbox because it is the service I use, but there are multiple options available. Other options to consider:

- Google Drive
- SkyDrive
- SugarSync
- Bitcasa Infinite Drive
- Rackspace Cloud Files
- Jungle Disk
- Justcloud.com
- Carbonite
- Mozy
- SOS online backup

¹ Local Area Network

- zipcloud

In choosing a provider for your cloud services, be sure to look at the provider's reputation. It is important to have a stable provider that will not go bankrupt and has good uptime for their services. Also look at the ease of transition to getting your data to this cloud provider and from this cloud provider. Consider the level of customer support. Free services often have none. Review the service level agreement (SLA) with the provider. Make sure you are comfortable with their policies for handling your confidential client information and that the service provider is not obtaining any right to use the data.²

How it is useful to your practice

The cloud is becoming more and more a part of the legal practice. Cloud storage, networking, e-filing, and the paperless office are becoming more prevalent in the practice of law. In 2013, the Supreme Court of Texas ordered that every jurisdiction in the state of Texas will have to accept e-filing by July 1, 2016, with deadlines for some counties rolling out earlier.

The cloud is being used by attorneys to back up their computer systems on a daily and weekly basis. It is an inexpensive alternative to buying servers and having to hire IT people to work on your computer. It is simple and seamless. And you have flexibility of where you work. You can also share folders with others. I had a case in which there were many documents being produced by both sides. We agreed to have a shared Dropbox folder so both sides could produce documents without mailing or printing, and any question about whether a document had been produced was quickly answered.

Are my files safe?

Lawyers are always concerned about confidentiality. By 2013, nineteen state bar associations had addressed this issue, and collectively the standard is reasonable care. Model Rule 1.6 states that lawyers must take reasonable steps to protect the electronic information related to the representation of the client. The lawyer has a duty to use reasonable care to prevent the inadvertent or unauthorized disclosure of or unauthorized access to information related to the representation of the client.

How is "reasonable care" defined? It is a little different in each state, but some of the factors that indicate reasonable care including encrypting your data, keeping up-to-date with technology, and reviewing the requirements of the service provider in terms of who owns the data or who has access to the data.

Encryption means that the data is stored in a form that is unreadable unless you enter a key or password. There are encryption programs available and most of them are free. No one can read the file unless they have your password. But the downside is that neither can you if you forget your password.

If you decide to use Dropbox or some other cloud storage, I encourage you to advise your clients in writing (like in your legal services agreement) that you are using it and that if they have any objections, they need to let you know.

² This is reportedly an issue with Google Drive.

Other advantages to using the cloud:

- It enables you to have a paperless office.
- All your files are stored and accessible on your computer or mobile device.
- You don't have to look around for that certain document in the piles of paper on your desk.

Also, at the end of a case you can provide the file to your client by giving them a DVD containing the file. You have no storage costs at some off-site storage facility that bills you monthly but that you can't bill your client for because the representation is concluded.

One suggestion—get a really good scanner. The Scansnap line by Fujitsu is excellent and used by lawyers throughout the world, but there are options.

Electronic communications and cloud computing continues to expand for lawyers. We are also using more tablets, smart phones, jump drives, and other portable devices in our practice. As such, a basic understanding of encrypted communications and data storage is critical for attorneys attempting to protect their clients' confidential information in cyberspace. This pamphlet is designed to provide a basic understanding of encryption technologies available for use in a law practice. *This is a starting place only*, and you should evaluate in more detail which encryption and security requirements best fit the needs your law practice.