CLOUD COMPUTING 101

By Brian S. Legum, Esquire

The term "the cloud" is part of the daily lexicon used when discussing computer technology. Whether it is creating a web-based email, viewing documents on a Smartphone or iPhone, or using products like Dropbox or Google Docs, lawyers are engaging in cloud computing. It is essential for legal professionals to understand the benefits and risks of using this developing technology, especially with regards to the confidentiality of client information.

What is "cloud computing"?

The ABA broadly refers to cloud computing as a "category of software that is delivered over the Internet via a Web browser rather than installed directly onto the user's computer." The Pennsylvania Bar Association Committee on Ethics and Professional Responsibility states that, "If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (email) such as Gmail, Yahoo!, Hotmail, or AOL Mail, or uses products such as Google Docs, Microsoft Office 365, or Dropbox, the attorney is using 'cloud computing.'"

Cloud computing can be a very cost-effective option for a law firm, especially a small firm or solo practitioner — instead of purchasing software and servers to store information, one can contract with cloud computing services at a fraction of the cost.

Nevertheless, the use of this technology places data, such as confidential client data, on computers outside of one's control. Therefore, there are significant concerns regarding the use of cloud computing services and the applicable ethics rules.

Different Types of Cloud Storage Services

There are many options when it comes to using the cloud to store information, which can be divided into three categories: public, private, and hybrid.

Public cloud storage options provide the users with an account where they can store their information on servers owned by the provider and accessible through almost any computer or mobile device. A few examples of public cloud storage options are Dropbox, Google Drive, SkyDrive, and iCloud. The cost of these services range based on the amount of storage leased from the provider. Many providers offer basic accounts at no cost, while larger storage options require payments billed monthly or annually.

Private cloud storage increases the level of security through having a dedicated server within an organization protected with restricted access.

The hybrid cloud storage model combines the two by having the ability to grant public access to specific information, while keeping other information private and protected.

Professional Responsibility & Cloud Computing

Several considerations should be taken into account when choosing to use the cloud to store information. As the Rules of Professional Conduct require protecting the confidentiality of client information, using the cloud to store information raises a concern as to whether the information is protected from being viewed.

For example, many of the service providers have policies that allow technical support staff to view documents under specific conditions. Before using any of the public cloud services, a lawyer should determine if usage of the cloud to store firm/client files is permissible. The ABA suggests considering the following questions when researching a cloud computing service provider:

Who is my vendor?

Similar to the way in which a decision is made to use one lawyer over another, one should consider the reputation of a vendor when shopping a cloud computing vendor. Are other firms using the provider? Have there been any problems with the service? How important is confidentiality to the vendor?

How and where will client data be stored?

Along with benefits of having access to data remotely, it is essential to know where the data is actually stored. Many cloud computing vendors contract with third-party vendors to store data at dedicated data centers. It is important to know who these third parties are, where they are located and how the data is stored/protected. Data centers might be located in other states, even other countries. This can lead to several issues regarding privacy of confidential information, as laws are different, especially outside the United States. Furthermore, it is important to know what procedures are in place to protect the data from destruction or a security breach.

Who can access my data and is the data still mine?

While data stored through cloud computing services might be encrypted through the use of a password, it is likely that the vendor has access to the password as well. It is important to ask who has access to the data and what procedures are in place to protect the data. Additionally, it is essential to retain ownership of the data, as some services providers have made claims that data uploaded to provider becomes the provider's property.

What are my terms of service?

It is imperative to read the terms of service. For example, it is important to know what happens if the service provider is issued a subpoena to produce information and whether notice will be provided to the customer.

Additionally, the terms of service will explain what happens to the data when the contract ends. It is important to know how the data is transferred to a new provider or destroyed.

What are the Courts Saying?

Several courts throughout the United States have issued opinions regarding attorneys use of the cloud to store confidential information and client data. While specific requirements and recommendations vary state by state, several options have defined a "reasonable care standard" which attorneys are to follow in protecting confidential information. Various suggestions included:

- Know how provider handles storage/security of data.
- Reasonably ensure confidentiality agreement is followed.
- Stay abreast of best practices regarding data safeguards.
- Discuss appropriateness of cloud storage with client if data is especially sensitive (e.g. trade secrets).
- Consult an expert if lawyer's technology expertise is lacking.
- Weigh the sensitivity of the data, the impact of disclosure on the client, the urgency of the situation, and the client's instructions.
- Vendor must have an enforceable obligation to preserve confidentiality and security, and should notify lawyer if served with process for client data.

A map of the states and relevant opinions can be found on the ABA website link:

http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

Brian S. Legum is an associate attorney of Kimmel, Carter, Roman, Peltz & O'Neill, P.A. where he practices in the fields of personal injury and workers' compensation. Mr. Legum is a member of the Delaware Supreme Court Commission of Law and Technology as well as the Richard K. Herrmann Technology Inn of Court.