Cloud 101 for Legal Professionals

A review of the applicable ABA rules, their implications and the ethical guidelines surrounding the use of cloud computing technology in the legal industry.

You've probably heard the term 'cloud' with reference to computers before. More specifically, the notion of cloud computing or cloud data storage as a way to increase your efficiency and mobility while practicing law. The visual the name conjures, one of unconnected and free floating data, probably does not engender confidence in this technology as a way to protect privileged and valuable client information. Technically speaking, the term cloud is used to describe a distributed or on-demand computing model where various elements of the user interface, process or storage is handled by remote machines linked together via the internet.

You probably use cloud computing already, and have for several years, without realizing it. Internet based email programs, such as Gmail, mobile applications like maps or instant messaging are examples of cloud services. Pretty much anything on your phone other than your flashlight and calculator app is a cloud-based product or service. Software that you access using the Internet, versus installing locally on your computer, is known as software-as-a-service, or SaaS.

While no state has found the use of cloud computing unethical, the available guidance about how law firms can and should use such services has been vague. Fewer than half of states have weighed in on the issue of cloud computing, and opinions frequently raise more questions than answers. This paper compiles and discusses relevant model rules and various rulings regarding cloud-based services to provide clarity and a best-practice recommendation.

Review of applicable ABA Rules and their implications:
There are generally five of the ABA model rules that have implications for cloud-based products:

Rule 1.1 Competence: A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation

Comment 6: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.

This is largely self-explanatory. In terms of cloud storage the 'thoroughness and preparation' would extend to immediate and continual access to information,

information protection and encryption, and disaster preparedness (disaster in this case including cyber-attacks as well as acts of god).

Rule 1.6 and Rule 1.15: in the cloud storage context overlap a great deal, so it's helpful to talk about them together.

Rule 1.6 Confidentiality of Information

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Comment 16: Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision. The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Rule 1.15 Safekeeping Property

While the comments focus on fiduciary responsibilities and client funds, files, information, documents, and other intellectual property must also be appropriately safeguarded.

Comment 1 makes this clear: "A lawyer should hold property of others with the care required of a professional fiduciary."

Rule 1.4 requires the lawyer to consult with the consult with the client about representation. Some State Ethics rulings about cloud computing, discussed below, suggest discussing with a client about the use of cloud computing or storage, or placing a provision about cloud services into an engagement letter.

Rule 5.3 requires the oversight of non-lawyer assistance. Comment 1 states that this rule "requires lawyers…make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that non-lawyers outside the firm who work on firm matters act in a way compatible with the professional obligations of the lawyer." Comment 3 explicitly states "A lawyer may use non-lawyers outside the firm to assist the lawyer in rendering legal services to the client…Includ[ing] using an Internet-based service to store client information." It is helpful here to review a SaaS-providers Terms of Service agreement to ensure that client information is kept confidential and secure in accordance to a lawyer's ethical obligations.

Review of applicable state ethics opinions

At present 22 states have issued official or unofficial opinions on cloud computing. While ethics opinions are not controlling, they are the most current thinking of a lawyers ethical obligations when using SaaS products.

Every state that has issued an opinion has found that it is acceptable for a lawyer to use SaaS products, so long as 'reasonable care' is used when evaluating a given cloud product. The most recent opinion, that of Wisconsin, provides a broad survey of previous opinions to come up with 12 factors to consider when assessing risks. While all of these elements are

not required in every state, they comprise a good general checklist to determine if it is 'reasonable' to store client data in the cloud:

1. the information's sensitivity;
2. the client's instructions and circumstances;
3. the possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party;
4. the attorney's ability to assess the technology's level of security;
5. the likelihood of disclosure if additional safeguards are not employed;
6. the cost of employing additional safeguards;
7. the difficulty of implementing the additional safeguards;
8. the extent to which the additional safeguards adversely affect the lawyer's ability to represent clients;
9. the need for increased accessibility and the urgency of the situation;
10. the experience and reputation of the service provider;
11. the terms of the agreement with the service provider; and
12. the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.

Wisconsin also provides a few pieces of general guidance culled from previous ethics opinions from other states. These constitute a good series of best practices for attorneys initially evaluating moving some or all of their data into a cloud-based service:

1. Lawyers should understand the importance of computer security, such as the use of firewalls, virus and spyware programs, operating systems updates, strong passwords and multifactor authentication, and encryption for information stored both in the cloud and on the ground.
2. Lawyers should also understand the security dangers of using public Wi-Fi and file sharing sites.
3. Lawyers who outsource cloud-computing services should understand the importance of selecting a provider that uses appropriate security protocols. "While complete security is never achievable, a prudent attorney will employ reasonable precautions and thoroughly research a cloud storage vendor's security measures and track record prior to utilizing the service." Knowing the qualifications, reputation and longevity of the cloud-service provider is necessary, just like knowing the qualifications, reputation, and longevity of any other service provider.
4. Lawyers should read and understand the cloud-based service provider's terms of use or service agreement.
5. Lawyers should also understand the importance of regularly backing up data and storing data in more than one place.
6. Lawyers who do not have the necessary understanding should consult with someone who has the necessary skill and expertise, such as a technology consultant, to help determine what efforts are reasonable.
7. Lawyers should also consider including a provision in their engagement agreements or letters that, at the least, informs and

> explains the use of cloud-based services to process, transmit, store and access information. Including such a provision not only gives the client an opportunity to object, but it also provides an opportunity for the lawyer and client to discuss the advantages and the risks.

By following the above recommendations, and choosing the right cloud-based partners, lawyers can not only increase the efficiency of their practice, but also protect themselves and their client's valuable data.

For information on how Citrix can help your firm benefit from the cloud, visit www.ShareFile.com.

CITRIX®

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud services to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.