

Moving to the Cloud: Is It Ethical?

by Robert E. Dean

“Let’s move our client files to the cloud.”
To where?

Among many locations, the cloud can be found in Ashburn, Virginia. That’s where Amazon Web Services recently leased two factory-sized, climate-controlled data centers, powered by independent generators, and staffed 24/7 by engineers and security personnel, to store files.¹ In other words, the cloud is a real place.

The cloud is also in Prineville, Oregon, the so-called “Silicon Forest,” named for the many data centers that have sprung up at the base of the Cascade Mountains.² The air is cooler and dryer there. Thus, it is less costly to chill the thousands of computer servers built by Google, Microsoft, and Amazon for off-site storage of consumer files and business data.

Storing files in the cloud is an alternative to the way most law firms currently store client files. Most law firms use local storage. They buy computer servers, put them in a room or closet, and hire local IT staff to connect the servers to the firm’s various desktop computers. The same IT staff must be available whenever the servers break down.

The cloud offers a way to store client files at an off-site data center, rather than on local servers. Instead of purchasing servers, law firms lease space on data centers. Services such as Dropbox for Business, SpiderOak, and Box.net transfer the files through encrypted channels over the Internet, as opposed to an internal office network. The cost-savings and economies of scale are apparent. Given the size of the data centers, each user shares the cost of 24/7 security and IT engineers.

Plus, the data is often stored redundantly at locations on both coasts. For example, Dropbox for Business uses Amazon Web Services to store its data. The Dropbox service is merely a broker between a computer and Amazon’s data center. The data is transferred via Dropbox onto Amazon’s computers via AES-256 encryption, the same secure encryption standard used by banks.³ Once the files are deposited onto Amazon’s data centers, redundant copies of the files are kept at each of its locations, including presumably the data centers in Virginia and Oregon.⁴ Therefore, should anything happen to the Ashburn data center, the files are safely backed up thousands of miles away.

What a contrast to local storage. Even with local servers, client files are susceptible to a variety of security risks, including fire, flood, and employee theft. By contrast, cloud storage seems to offer a safer, more affordable solution to store client files.

Until recently, however, there was a lingering concern whether storing files in the cloud is ethical under the Virginia State Bar Rules of Professional Conduct. When a file leaves the attorney’s office, there is a remote, unlikely possibility that a data center employee could decrypt the file to access its contents. Therefore, some worry that cloud computing violates the duty of confidentiality.

Legal Ethics Opinion 1872 addressed whether “using cloud computing or any other technology that involves the use of a third party for the storage or transmission of data” complies with Rule 1.6 (“Confidentiality of Information”).

The Standing Committee on Legal Ethics stated that “the lawyer is not



© shutterstock.com

required, of course, to absolutely guarantee that a breach of confidentiality cannot occur when using an outside service provider.” But there are certain guidelines that a lawyer must follow when using a third-party provider of file storage. First, the lawyer must exercise care in the selection of a vendor and have a reasonable expectation that the client’s information will be kept confidential. Second, the lawyer must review the vendor’s terms of service to determine whether they are adequate to protect the client’s confidences. Finally, if lawyers cannot make these evaluations on their own, they must consult a qualified person to assist them.

Virginia joins Alabama⁵, Arizona⁶, California⁷, and North Carolina⁸, among many states, in approving the use of cloud computing in law practice.⁹

For years, Virginia attorneys have used third-party providers to store client information away from the office, such as in safe deposit boxes or off-site storage units. The use of cloud computing is perhaps no different, and the principles are the same: attorneys must use good judgment in the selection of a reputable vendor; exercise reasonable diligence in protecting their client’s information

Cloud continued on page 34

Cloud continued from page 33

through strong passwords, encryption keys, and other information technology best practices; and, of course, advise their client in advance.

Endnotes:

- 1 <http://www.datacenterknowledge.com/archives/2013/01/15/amazon-to-add-capacity-to-us-east-region/>
- 2 <http://www.wired.com/2011/12/facebook-data-center/>
- 3 Eliu Mendez, Dropping Dropbox in your Law Practice to Maintain your

Duty of Confidentiality, 36 Campbell L. Rev. 175 (2014)

- 4 Amazon Web Services: Overview of Security Processes, AMAZON WEB SERVICES (Sept. 5, 2008, 5:33 PM), <http://aws.amazon.com/articles/1697>
- 5 <http://www.alabar.org/ogc/fopDisplay.cfm?oneId=425>
- 6 <http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704>
- 7 <http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836>
- 8 <http://www.ncbar.com/ethics/printopinion.asp?id=855>
- 9 <http://bit.ly/1rFSnwa>



Robert E. Dean is a litigation associate with Gentry Locke Rakes & Moore LLP and has successfully tried cases in the areas of personal injury, medical malpractice, business disputes, and employment law. Before joining the firm, he worked as a prosecutor with the Office of the Commonwealth's Attorney in Lynchburg.