LTT LAW TECHNOLOGY TODAY

May 18, 2015

NAVIGATING CLOUD COMPUTING SECURITY IN LIGHT OF RECENT DATA BREACHES

BY JOE KELLY

Five years ago, when most attorneys thought of the cloud, they pictured the white fluffy ones in the sky. Now, many law firms use cloud computing applications to store at least some of their information. The ABA Rules of Conduct, as well as most state ethics rules, have concluded that using cloud computing applications to store client data aligns with professional obligations as long as attorneys practice some due diligence. Yet many attorneys who have become comfortable with cloud computing may now be tempted to rethink their security processes, following recent high-profile data breaches.

When successful hacker attacks against Anthem, Target, Home Depot and others become front-page news, law firms should rightfully be concerned about keeping client data secure. Yet despite conventional wisdom or the assumptions of many attorneys, data can be safer residing in the cloud than on servers down the hall.

In order to maintain all their legal obligations toward their clients, attorneys must understand the rules that govern their actions and utilize cloud options that provide the proper safeguards.

Legal Responsibilities and Ethics

Several ABA Model Rules are relevant to attorney duties and obligations around cloud storage. They include:

Model Rule 1.1

Under this rule, lawyers must provide "competent" representation to their clients. That means lawyers must have enough knowledge about cloud computing and their specific providers to adequately safeguard their clients' data.

Model Rule 1.6

Lawyers also must protect the confidentiality of their client information. With recent data breaches, attorneys should be particularly thoughtful about the cloud services they utilize to store any type of client information.

States Recommendations

Along with the ABA Model Rules, many states have also weighed in on the use of cloud computing. Those that have spoken up so far have allowed cloud computing, as long as attorneys do their due diligence. These include:

Alabama

Lawyers must know how the provider handles storage and data security. They must also reasonably ensure that confidentiality agreements are followed and remain knowledgeable about data safeguards.

Arizona

The standards in Arizona apply to all types of technology and require "reasonable security precautions." Attorneys need to regularly review their security measures and develop or work with someone who is competent with online security.

California

Attorneys must evaluate the type of technology and security measures, as well as control the access of third parties. Lawyers must also be familiar with the sensitivity of the data, what clients have allowed and how disclosure could affect clients.

Connecticut

Lawyers must maintain access to and ownership of data they store in the cloud, and security procedures must keep the lawyers' data separate from any unauthorized access.

Florida

Lawyers must research a cloud provider's security measures and ensure that the provider will preserve confidentiality and security. They must also take precautions against reasonably foreseeable attempts to hack information.

Iowa

Cloud service providers must allow complete access to data, whenever necessary. Lawyers must also research how much protection is granted to the data within the cloud.

Maine

Lawyers need to review the cloud service provider's service level agreements and technology, particularly the security and backup processes. Lawyers must also verify that the technology generally meets professional responsibility obligations.

Massachusetts

On a regular basis, attorneys need to review the terms of service and access to data, as well as security practices and portability. Law firms must also specifically follow clients' orders regarding storing and transmitting data in the cloud.

Nevada

Lawyers must instruct and require providers to keep client information confidential and choose one that can be reasonably relied on to do so.

New Hampshire

A basic understanding of technology and current changes is required, along with a reasonable effort to ensure that providers behave in a way that meshes with lawyers' professional responsibilities. Attorneys must also think about getting a client's informed consent when using the cloud for highly confidential information. When the information no longer needs to be kept or the representation has ended, attorneys must also return the client's information and delete it from the cloud.

New Jersey

When dealing with technology in general, attorneys must ensure that vendors have an enforceable obligation to preserve confidentiality and security, and use technology to protect against foreseeable attempts to infiltrate data.

New York

Contracts with cloud service providers must include enforceable obligations to preserve confidentiality and security, along with requirements to contact lawyers when served with process for client data. Lawyers must ensure technology is being used to protect data against foreseeable attempts to infiltrate it. Attorneys must also investigate potential security breaches and review security practices to make sure they are current.

North Carolina

When reviewing terms and policies around cloud services, lawyers must consider ethical obligations and renegotiate them if necessary. They must also review the provider's security measures and backup policies and ensure data can be retrieved if the service is canceled or the vendor goes out of business.

Ohio

When selecting an appropriate provider, lawyers must be sure the provider maintains confidentiality and safeguards client property, while communicating with clients as appropriate. Law firms also must provide reasonable supervision of the vendor.

Oregon

When developing service agreements with providers, attorneys must require that confidentiality and security are preserved and adequate backup procedures are in place. They must also require notice if their data is accessed by someone without authorization. As technology advances, lawyers must also regularly re-evaluate precautions.

Pennsylvania

Lawyers must take reasonable care that information in the cloud remains confidential and use reasonable safeguards to protect the data.

Vermont

Along with taking precautions to make sure client data is safe and accessible, lawyers must consider whether to keep some types of data in their original paper format. If data is particularly sensitive, attorneys must discuss with clients whether storing it in the cloud is appropriate.

Virginia

Along with carefully selecting the provider, the attorney should have a reasonable expectation that the provider will keep data confidential and inaccessible. Attorneys must provide instructions on preserving the confidentiality of the data.

Washington

With regard to technology in general, attorneys must conduct due diligence on any potential provider, stay up to date on changes in technology and regularly review the security procedures of providers.

What to Look For in a Cloud Provider

While attorneys must carefully consider the specific mandates in their jurisdictions, there are several general factors to consider:

Security Features

Keeping client data secure should be a primary focus for every attorney. While many firms may have avoided the cloud because of concerns over keeping data safe, those fears are often misdirected. As long as any type of data is connected to the Internet, whether it sits on a server in the law firm's office or resides in the cloud, it is still vulnerable to hackers.

In fact, cloud-based services often have better security than all but the largest law firms can support. A dedicated cloud provider can offer the most up-to-date operating systems, enterprise-grade firewalls

and frequently updated patches and anti-virus software to thwart the constantly changing approaches that sophisticated hackers develop.

Along with virtual precautions, attorneys should look for partners that offer different levels of physical security at their sites, such as requiring badges, keys and codes for those on the premises. They should also specifically ask about data encryption.

Disaster Recovery

Through a cloud-based approach, law firms can also improve disaster recovery with extra layers of redundancy and protection. When data is stored in the cloud, supported across multiple locations, firms can insulate themselves against the loss of important information if one site is compromised.

24/7/365 Access

With the rise of laptops, tablets and smartphones, many attorneys and office staff take advantage of access and flexibility to work away from the office. However, some cloud services that are not specifically geared toward law firms can be vulnerable to data breaches. By working with a cloud provider that offers flexible, secure access, attorneys and staff can work safely from anywhere.

Conclusion

While lawyers should rightfully be concerned about security and abiding by professional responsibilities, the cloud can help firms offer greater confidentiality and service to clients. By understanding their obligations and working with the right service providers, law firms can benefit from improved flexibility and access and reduced infrastructure and support costs, while knowing client data is safer and more secure than ever before.

Joe Kelly, founder and CEO of Legal Workspace, formally launched the company in 2010. In 2006, he first saw the potential for the Legal Workspace solution because of his broad exposure to how law firms operate. The evolution of virtualization, connectivity and hosting technologies made Legal Workspace a commercially viable solution, and it went live with its first client firm in 2008.

Originally published May 18, 2015 by ABA Law Technology Today ABA Law Technology Today