Selecting a Law Firm Cloud Provider

Questions to Ask and Ethical/Security Concerns

By Sharon D. Nelson and John W. Simek

It seems like everybody is talking about the "cloud" and new uses it provides for lawyers and law firms, which got us thinking about how little the typical lawyer may know about cloud services. Many attorneys can't even describe the cloud; you would be amazed at how many think it is somehow affected by the weather. We can't blame them—definitions for the cloud are all over the place.

Generally, services provided in the cloud are provisioned by technology that is not physically located in your office; in other words, it is remote and off premises. You can certainly own the equipment yourself and house it at a data center with everything under your control, but there are many other options for cloud computing. You could purchase computing space on equipment owned or operated by someone else. Think of Amazon's Web Services, where Amazon owns the hardware and network and you purchase the computing capacity and storage. You could also purchase application access from a vendor, where it provides all the equipment, network, and storage along with the software. Think of Microsoft's Office 365, where you run Office on the vendor's hardware via an Internet connection.

Once you know what the cloud is, how do you go about selecting a provider? Are there special ethical concerns when doing so? We'll try to help your selection process by posing some questions to ask.

What is in place for physical security?

This seems like a simple question, but it's a necessary one. The first step to protecting data is making sure the equipment itself is secure. The majority of cloud providers have their equipment in a data center. The data center is physically secured at several levels. As an example, we'll describe the physical security for the data center we use. A fence surrounds the entire complex with security surveillance video cameras watching the grounds. There is a man-trap entrance system at the complex's entry point, meaning you need an access card and biometric (fingerprint reader) to pass through the first door into a small space. Once the first door closes, your access card and biometric open a second, interior door. Security guards and cameras monitor the entry—if something seems amiss, that small space turns into a man trap (sorry ladies, we didn't name it). There are additional cameras watching the watchers at the entry point. Video surveillance cameras monitor the halls and entrances to the various rooms housing the equipment. You need your access card and biometric to enter each door in the data center. This high level of physical security safeguards against unauthorized access to or removal of any equipment.

Is the provider financially stable?

This question was more important back in the dot-bomb days when everyone was talking about software as a service (SaaS). Most cloud providers are well financed, and it's been a long time since we heard of one going out of business. Nonetheless, make sure you understand the cloud provider's financial stability before signing on the dotted line.

Who owns the data?

This sounds like another simple question, but many lawyers don't know the answer. Why is data ownership important? Lawyers are required to keep client information confidential. How is that possible if you don't own the data? If the cloud provider has ownership, it can redistribute, clone, or otherwise divulge the data to anyone. Not good. Even if you own the data, does the provider have access to it? What can the vendor do with it? Typically, the terms of service explain data ownership and what the vendor is permitted to do with the data. We know many lawyers don't read the terms of service and merely check the

Generally, services provided in the cloud are provisioned by technology that is not physically located in your office.

Law Practice Solutions is a regular feature brought to you by the Practice Management Resource Center (PMRC) of the State Bar of Michigan, featuring articles on practice management for lawyers and their staff. For more resources offered by the PMRC, visit our website at http://www.michbar.org/pmrc/content.cfm or call our Helpline at (800) 341-9715 to speak with JoAnn Hathaway or Diane Ebersole, Practice Management Advisors.

> Encryption protects data from being accessed by unauthorized individuals.

box signifying they agree. Tsk, tsk—the new professional rules require you to be competent with technology.

Is the data encrypted?

Encryption protects data from being accessed by unauthorized individuals. It's another way to protect the confidentiality of client information. Data should be encrypted at two stages. The first stage is during data transmission. Typically, this is done through the use of secure socket layer (SSL) transport. If you use a web browser to access the cloud service, the URL will begin with https://. This means the data stream is encrypted and can't be read by anyone intercepting the data packets.

Data should also be encrypted while in storage at the cloud provider. This is particularly important if the data is stored on shared space that may be accessed by the cloud provider's other customers. Encrypting data at rest helps prevent unauthorized individuals from reading the information unless they can decrypt it, which brings us to the next point.

Who controls and defines the encryption key? Encrypting data doesn't do much good if an unauthorized person has access to the encryption key; in other words, why bother locking the door if you give the burglar your spare key? Getting answers to encryption questions without specifically asking the cloud provider can be difficult. A common practice is encrypting the data in transit. Encrypting data at rest is customary for storage-only services such as Dropbox and less typical for applications provided via the cloud, such as case-management applications.

Can the National Security Agency decrypt your data?

To date, we have seen no evidence that the National Security Agency can break strong encryption, though its capabilities are evolving. We remain watchful for signs that strong encryption schemes have been broken. The National Security Agency is most likely to have back doors into clouds or the tacit compliance of a provider in delivering data. We recommend avoiding large clouds such as Amazon, iCloud, and Google Drive because they are attractive targets for the government.

Where is the data physically stored?

Why is this an important question? If your equipment is at a data center, you know the answer. The goal is to have your data stored in the United States, where the laws are well known. If you need to address an issue concerning the data or the performance of the service provider, most lawyers know the available legal options and how to navigate the court system. That's not as true if the data resides in a foreign country. Privacy laws and cross-border issues can be very complicated. France is particularly tough when it comes to data privacy. We recommend storing data in the United States, despite concerns about the National Security Agency.

Who can access the data?

This is similar to the encryption question. If you control the encryption key, this question is less important. If you don't control the key, under which circumstances will the vendor give your data to law enforcement or the government? Assuming the vendor has a master encryption key, will the vendor decrypt your data and turn it over to law enforcement and, if so, will it notify you? Look for provisions in the terms of service where the vendor states it will give you notice before turning data over to law enforcement. This gives you an opportunity to file a motion to quash. If the law-enforcement request comes in under the USA Patriot Act, you're toast. The government will get your data and you will not receive notice. This is another argument for encrypting data and holding the master decryption key yourself. The cloud provider can only give the government encrypted data, which is fundamentally useless without the decryption key as long as the encryption is strong.

What about data breaches?

Who has responsibility in the event of a data breach? Who makes and pays for the breach notifications? Will the provider pay for identity-theft monitoring, if necessary? Who is liable? Hopefully, you will never experience a data breach, but you should know what to do if one occurs. We suggest that the cloud provider be liable in the event of a data breach since it controls the environment. Most cloud providers try to disclaim liability. You will almost certainly be the responsible party if it is your equipment and you are only renting space in a data center.

How is the data stored?

We know the data is stored electronically, but is it held separately from other customers' data? The reason for this question is to avoid a situation like Megaupload. If your data is stored on equipment along with other customers' data, keep a copy of your data somewhere else. In the Megaupload case, the company's assets were confiscated as part of a Department of Justice investigation into allegations of copyright infringement. Many businesses that had nothing to do with Megaupload's alleged illegal activities went bankrupt because their data was held on the same equipment as the suspected criminals and they couldn't access it. The lesson here is to make sure your data is segregated or a copy exists in another location. We prefer that data not be commingled, but that isn't always an option.

Is there a service-level agreement?

Does the cloud provider provide any guarantee of uptime and access to the data? Generally, a data center has the capability to

provide 99.999 percent of uptime. It should have backup generators to provide electricity in the event of a power outage and multiple carriers and connections to the Internet to ensure connectivity.

Are updates automatic?

Many folks rave about the cloud and how they no longer have to worry about availability or upgrades. Automatic updates can be a good thing, especially if they are security patches to fix vulnerabilities. However, updates can sometimes be a bad thing, especially if you have installed a core application that is critical to your firm's operation. An update may damage your application. Will the cloud provider allow you to approve the installation of an update or upgrade? You may need time to test your applications to make sure there are no problems with the updates. This is obviously less of a concern if you use the application services provided by the vendor.

Is there an exit strategy?

What should you do if you want to leave your cloud provider? Assuming the data is yours (and it should be), how do you retrieve it? In which format will the data be? Will you have to pay to get your data and, if so, how much? Are you being held hostage by onerous terms? The ability to extract your data in some usable form can also serve as a backup mechanism.

So many questions, yet we could spin this article out further if space permitted. If you are overwhelmed by the process of selecting a cloud provider, plenty of reputable legal IT consultants can help. And that's the main point concerning the change to Rule 1.1 of the Rules of Professional Conduct: if you are not competent to handle technology decisions yourself, find someone who is. The questions we've posed here can guide you if you are fairly tech savvy and want to undertake the selection process on your own. ■

Sharon D. Nelson, Esq., is the president of Sensei Enterprises, Inc., a digital forensics, information security, and information technology firm in Fairfax, Virginia. She is a frequent author (11 books published by the ABA and hundreds of articles) and speaker/podcaster on legal technology, information security, and electronic evidence topics. She is also the 2013–2014 president of the Virginia State Bar.

John W. Simek is the vice president of Sensei Enterprises, Inc. He has a national reputation as a digital forensics technologist and has testified as an expert witness throughout the United States. He holds numerous technology and digital forensics certifications. He is a coauthor of 10 books and hundreds of articles, and speaks frequently on legal technology, information security, and electronic evidence.