Selecting a Law Firm Cloud Provider:

Questions to Ask and Ethical/Security Concerns

by Sharon D. Nelson, Esq. and John W. Simek

It seems like everybody is talking about "the Cloud" and what new uses it provides for lawyers and law firms. All this talk got us thinking about how little the typical lawyer knows about cloud services. Many attorneys can't really even describe what "the Cloud" is. You would be amazed at how many lawyers think "the Cloud" is somehow impacted by the weather. We can't really blame them - the definitions for "the Cloud" are all over the place. Generally, services that are 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 datacenter with everything under your control. There are a lot of other options for cloud computing as well. You could purchase computing "space" on equipment owned and/or operated by someone else. Think of Amazon's Web Services, where Amazon owns the hardware and network and you purchase computing capacity and storage from them. Finally, you can purchase application access from the vendor, where they provide all the equipment, network, storage and the application software too. Think of Microsoft's Office 365, where you run Office on their hardware via an Internet connection.

Once you know what the cloud is, how do you go about selecting a provider and are there any 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 such a simple question, but a necessary one. The first step to protecting data is to make sure that the equipment itself is secure. The majority of cloud providers will have their equipment in a datacenter. The datacenter will be physically secured at several levels. As an example, we'll describe the physical security for the datacenter that we use. First, there is a fence surrounding the entire datacenter complex with security surveillance video camera watching the grounds. There is a man trap entrance system at the entry point for the datacenter. This means you use your access card and biometrics (fingerprint reader) to enter the first door into a small space. Once the first door closes, you use your access card and biometric again to open the second (interior) door. Security guards and cameras watch the man trap entry – if something seems amiss, that small space will turn into a man trap (sorry ladies, we didn't name it). There are even cameras watching the watchers at the entry point. Video surveillance cameras monitor the halls and entrances to the various rooms that house the equipment. You need your access card and biometric to enter each door in the datacenter. This

high level of physical security is a safeguard against unauthorized access or removal of any equipment that isn't logged.

What is the Financial Stability of the Provider?

This question was a lot more important back in the dot bomb days, where everyone was talking about SaaS (Software as a Service). Most cloud providers are well financed and we haven't heard of any going out of business for a long time. Nonetheless, make sure you understand the financial stability of the cloud provider before you sign on the dotted line.

Who Owns the Data?

This sounds like such a simple question, but many lawyers don't know the answer. Why is data ownership important? Lawyers are required to keep their client's information confidential. How are you supposed to do that if you don't own the data? If the cloud provider has ownership, they can redistribute, clone or otherwise divulge the data to anyone. Not a good thing. Even if you own the data, does the provider have access to it and what are they allowed to do with the data? Typically, you'll get the answer to data ownership and what the vendor is permitted to do with the data from the terms of service. We know most lawyers don't read the Terms of Service (TOS) document and merely check the box signifying that they agree. Tsk, tsk – remember that the new professional rules require you to be competent with your technology.

Is the Data Encrypted?

Encryption will protect the data from being accessed by unauthorized individuals. It's another way to protect the confidentiality of the client's information. There are two areas where the data should be encrypted. The first is when the data is transmitted. Typically, this is done through the use of SSL (Secure Socket Layer) transport. If you are using a web browser to access the cloud service, the URL will begin with https://. This means that the data stream is encrypted and will not be readable by anyone intercepting the data packets.

The second area where the data should be encrypted is while it is stored at the cloud provider. This is particularly important if the data is stored on shared storage space that may be accessed by a different customer of the cloud provider. Encrypting the data at rest will help prevent unauthorized individuals from reading the information unless they can decrypt it, which brings us to the last point.

Who controls and defines the encryption key? Encrypting the 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? It may be difficult to determine the answers to the encryption questions without specifically asking the cloud provider. It is common practice to encrypt the data in transit. Encrypting the data at rest is common for those services that are

strictly storage services such as Dropbox and less common for applications provided via the Cloud such as case management applications.

Can the National Security Agency (NSA) decrypt your data?

To date, we have seen no evidence that the NSA can break strong encryption though there is no doubt that its capabilities are evolving – we remain watchful for signs that any of the strong encyption schemes have been broken, but have seen none yet. The NSA is most likely to have back doors into clouds or to have the tacit compliance of a provider in providing data. We would avoid large clouds such as Amazon, the 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 installed at a datacenter, you know the answer to this question. The end goal here is to have your data stored in the United States, where the laws are well known. Should you need to address something with the data or performance of the service provider, most lawyers know how to navigate through the court system and what legal options are available. Not so true if the data resides in a foreign country. Privacy laws and cross border issues can be very complicated when dealing with foreign countries. France is particularly tough when it comes to data privacy. We recommend that the data be stored in the United States, the new concerns about the NSA notwithstanding.

Who Can Access the Data?

This is similar to the encryption question. If you control the encryption key, this question is less important. However, if you don't, under what circumstances with the vendor give your data over to law enforcement or the government? Will the vendor decrypt your data (assuming they have a master encryption key) and turn it over to law enforcement? Will they even notify you that they are doing so? Look for terms in the TOS where the vendor will give you notice prior to turning the 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 get no notice. This makes yet another argument for encrypting the data and holding the master decryption key yourself. All the cloud provider can give the government is encrypted data, which is fundamentally garbage data without the decryption key so long as the encryption is strong.

What about Data Breaches?

Who has responsibility in the event there is a data breach? Who makes and pays for all the data breach notifications? Will the provider pay for identity theft monitoring if needed? Who is liable? Hopefully, you will never experience a data breach, but you should be aware of what to do should it occur. We would certainly suggest that the cloud provider be liable in the event there is 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” rack space in a datacenter.

How is the Data Stored?

We know that it is stored electronically, but is it held separately from other customers? The reason for this question is to avoid a situation like Megaupload. If your data is stored on equipment along with other customers, make sure there is another copy somewhere else. In the Megaupload case, its assets were confiscated as part of the action of the United States Department of Justice for allegedly operating as a company supporting copyright infringement. Many businesses which had nothing to do with the alleged illegal activities of Megaupload went bankrupt. The problem was that their data was held on the same equipment as the supposed bad guys and they had no access to it. The lesson here is to make sure your data is segregated or another copy exists on redundant equipment in another location. We prefer that data not be commingled at all, but that isn’t always an option.

Is There a Service Level Agreement (SLA)?

Does the cloud provider provide any guarantee of uptime and access to the data? Generally, a datacenter has the capability to provide 99.999% (called “the five nines”) of uptime. They have backup generators to provide electricity in the event of a power outage. In addition, they have multiple carriers and connections to the Internet for connectivity.

Are Updates Automatic?

Many folks are absolutely religious when talking 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 correct vulnerabilities. However, sometimes updates can be a bad thing, especially if you have installed a core application that is critical to your firm’s operation. The update may break 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 any updates. This is obviously less of a concern if you merely use the application services provided by the vendor.

Is There an Exit Strategy?

What do you do if you want to leave your cloud provider? Assuming that the data is yours (and it should be), how do you get the data out of the system? What format will the data be in? Is there a charge to get your own data? If you have to pay to get your own data, 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 data backup mechanism.

So many questions? Yes, and we could spin this article out further if space would allow. If you are overwhelmed by trying to cope with cloud provider selection, there are plenty of reputable

legal IT consultants who can help you. And that's the true point of 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. But the questions we've enumerated here will give you a pretty good condensed guide if you are fairly tech savvy and want to undertake the selection process yourself.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com