# Is Cloud Computing Inevitable for Lawyers?

by Sharon D. Nelson and John W. Simek



Not a single day goes by when you don't hear something about cloud computing. It could be some new feature or service offering or even a data breach. So what's all the hype? Are you destined to be using some type of cloud service in your practice, assuming you aren't already? It's even likely that you are already using the cloud and don't realize it. If you use Gmail or other web-based providers, you are using the cloud. Let's take a look at whether cloud computing is right for your practice and suggest some questions you should be asking of any cloud service.

## What is the Cloud?

Before we jump into the pros and cons of cloud computing, let's try to establish a basic understanding of what the cloud really is. Essentially cloud computing is where your data is not on your premises and you access it via a network, typically the Internet. The cloud services could include such things as a case management application, document management or file storage. Products like Office 365 and Google Apps are also cloud services. We could get further in the weeds and talk about the differences between private, public and hybrid clouds, but our basic definition will do for now.

## Application Provisioning

When deciding on whether to utilize cloud services, there are basically two choices. You can purchase a software/hardware solution that you physically control or "buy" the function from a cloud provider. Let's talk about data you have in your office. When you purchase software licenses, you may be required to also purchase maintenance. Someone will have to install and configure the software and maintain it (apply patches, updates, etc.) for as long as you use the software. The investment in the software is normally a one-time purchase with additional costs (e.g. maintenance, upgrades, etc.) going forward. In contrast, cloud services are delivered through a subscription model. You pay as you go. There may be minimal contract commitments (e.g. 12 months usage) or it may be month to month with no commitment.

Which model is best for you? That depends. Make sure you are honest about assembling all the costs for either scenario. The price of purchased software has a higher initial cost, but the expense rapidly tapers off the longer you use the software. However, subscription cloud services are a constant expense throughout the lifetime of the software usage. That could be a good thing since it is fairly easy to budget a constant expense. Be sure to total all the costs across whatever period you are analyzing. Typically, project costs are estimated over a 3 or 5 year period. Don't' forget to account for hardware expense for any in-house application hosting. The good news is that you can spread out the hardware cost across multiple applications if they are all running on a single server.

## Mobile Devices

We have become an extremely mobile society. Remote access to our data and applications is a fundamental business requirement for almost every firm. We have a strong desire to use our mobile devices for this remote access. Since cloud computing is typically provisioned via a web browser, all you need is an Internet connection. Smartphones are equipped with browsers and purchasing a data plan will get you on the Internet. You could even use the device's Wi-Fi capability if you don't want to pay for a data plan, but that would limit your usage of the cloud. Some cloud providers provide mobile apps specific to their particular service. In those cases, make sure that the app is supported on your specific device.

There are alternatives for remote access to on premise solutions, but they tend to be more complicated and costly to implement. Cloud computing definitely wins the remote access battle here, especially when using mobile devices.

Why is mobile device usage so desirable? Since most of us have a smartphone with us darn near every minute of the day, we can capture time for billing purposes; check our calendar for deadlines and tasks, look up documents for a particular case and much more. Be sure you check the court rules though. Some courts still forbid bringing electronics into the courthouse, even for attorneys.

## Collaboration and File Sharing

This is where cloud computing is a great alternative. You can have a client portal, where the client can access only their information and collaborate with their counsel. We've also seen situations in which attorneys from other firms use a portal to work on a case when they are co-counsel. These portals are extremely easy to provision in the cloud. It is much harder to implement this type of file sharing and collaboration when the application and data reside on your firm's network. You may have to create a user ID for the clients or co-counsel that can authenticate to your network. This means that you have to lock down access carefully since you wouldn't want them accessing other data or systems within your firm.

When attorneys want to try cloud computing, they usually start with one of the file sharing or file storage services. Box.net and SpiderOak are two secure file sharing services. Many attorneys also use Dropbox to share files, but that's not a very secure way to exchange data. When attorneys begin with cloud file sharing services, they begin to gain confidence in what cloud computing can provide.

## Where's the Data?

This is an easy question if you have a server that stores your documents and other client information. However, it is not such an easy answer if you are in the cloud. The key point is that you should know where your data resides if it is in the cloud. Data that is stored outside of the US borders isn't necessarily subject to U.S. laws. You should make sure the cloud provider is storing the data in the United States and hopefully at multiple locations. Though Europe may have stronger privacy laws, you are probably not an expert in them and don't want to deal with cross-border issues.

## Is it Your Data?

The secondary question is concerned with data ownership. Don't assume that you maintain ownership of the data simply because you're the one that put it in the cloud to begin with. Read the Terms of Service to see if you retain ownership of your data. The TOS will also tell you what the cloud provider can do with your data even if you maintain ownership. As an example, they may be allowed to access the data in order to deliver targeted ads to you. They may also deliver the data to third party providers. Obviously, if client confidential data is being sent to the cloud provider, it is imperative that you understand who can access what data and what they can do with it.

## Security Issues

When you participate in cloud computing, you're likely using computers that reside in a highly secure data center. The data centers have all kinds of security measures in place, starting with physical security. They are nondescript in appearance with high fences, video surveillance cameras, biometric access, man traps, etc. Suffice it to say that you will have a really tough time getting physical access to the computers in the data center if you don't belong there. This security is much greater than that normally available at law firms.

Besides the physical security, cloud providers are constantly updating operating systems, patching computers and making sure the firewalls are secure. In other words, the security of a cloud system tends to be a lot better than that of most law firms. That doesn't mean that a cloud solution is the best option for you. The allure of a mega-secure environment may not outweigh handing over confidential data to another party. In fact, maintaining control of the data (physical and logical access) can be more attractive than handing the data off to a cloud provider, where you really don't know what happens with your information.

You can mitigate the security risk of handing over data by encrypting it before you transmit it to the cloud provider. However, aside from cloud storage providers, encrypting data prior to transfer for other cloud computing vendors (e.g. case management, document assembly, document management, billing, etc.) will normally render the service unusable. A conundrum, yes?

## Flexibility

Licensing costs are a prime concern when implementing an on premises solution. It is less of a concern for cloud solutions. Cloud computing is very "elastic." That means that you can add and subtract users with very little financial impact. In contrast, systems that you own tend to only move in one direction…up. You may hire new associates and have to increase your license count. If the associate leaves in 4 months, you can't normally just reduce the cost. You have paid for the license and there is no "refund" if you return one license. Certainly cloud computing can be more financially attractive, especially if there is a lot of churn at your firm and the number of users is volatile in a short period of time. When comparing cloud solutions to firm owned solutions, make sure you anticipate the licensing costs for the number of users. If your user base is fairly constant, licensing costs over the long term will typically be less than paying for the flexibility of cloud solutions.

We may not have much of a choice for some critical business applications. As an example, Microsoft is pushing the subscription model really hard with its Office 365 offering. The pricing is very attractive and a great solution for many attorneys. However, if you only upgrade your Office software every other version upgrade, purchasing a traditional license will probably be cheaper. But what if Microsoft no longer delivers retail licensing and only has Office 365 subscriptions for sale? In that case, we'll all be forced to use the cloud to utilize a key office productivity software package.

## Disaster Recovery

A great use of cloud services is for the storage of backup data and recovery in the event of a disaster. However, some commentators are questioning whether the use of cloud computing means that law firms don't need to have a disaster recovery plan. After all, the cloud providers will have redundant data centers, redundant power, redundant power supply, redundant communications and pretty much redundant everything. This means that the end-user has effectively shifted the responsibility or data and application access to the cloud vendor. In consideration for your subscription payment, they make sure you can always get to your data and application. You will need to make sure you have alternatives for Internet access from your own devices (cellular data, multiple broadband providers, Wi-Fi hotspot, etc.), but that is far less burden than designing high-availability for in-house applications. Despite the significant redundancies of the cloud provider, we still believe you should maintain control of your data at least with a copy in your physical possession.

## Final Words

Cloud computing isn't for every firm. Virtual law practices will be more dependent on cloud services than other practices. One of the key decision points is how to protect the confidentiality of the data. A lot of law firms will opt to keep the data within their own walls and control. Others will readily give the data to a cloud provider, encrypting it before transmission. Others will just trust the security and proper operation of the cloud vendor. No matter which approach you take, cloud computing is here to stay. Just using the cloud for remote data backup (encrypting with a user controlled key) is a first step for most law firms. Solo and small firms will be heavier users of the cloud since they can get a larger "suite" of services for lower cost. Just make sure you do your due diligence since you are shifting the security responsibility to someone you have little control over.

To answer the question asked by the title of this article, we are seeing more and more law firms turn to the cloud for a variety of reasons. There are financial pros and cons which are poorly understand and which often go unmeasured. There is a continuing failure to properly investigate the security of the cloud. We really haven't seen a law firm get seriously burned by using the cloud, but we probably will. If you are allowing your data to be commingled with that of others, you are asking for trouble – if the government seizes servers with commingled data, you may be in quite a pickle. Easy answer there – don't allow your data to be commingled.

So is adoption of cloud services inevitable? Not yet. There are firms which resist the cloud on ethical grounds – and they have some valid concerns. But the truth is that cloud security is often better than

what law firms themselves can provide – one very good reason to consider cloud computing. As we know from recent transparency reports, many cloud providers turn data over law enforcement, some without giving you prior notice and a chance to file a Motion to Quash. Forgive us if we say any prediction for the future of law firm cloud usage will necessary be "cloudy." There are many rushing to the cloud, but there are also those who have their feet firmly planted in the "we'll control our data in-house" camp. There's not a "right" or "wrong" answer, but we don't see ALL law firms using cloud providers anytime soon.

*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*