KIRK TO ENTERPRISE … BEAM ME UP SCOTTIE!

Ellen Freedman, CLM

One of the most frequent questions I am asked nowadays is about cloud computing. Many solo and small firm attorneys continue to experience a profit-squeeze. New grads unable to secure positions at firms are being forced to strike on their own. They are joined by a continuing trickle of large-firm attorneys cast adrift in efforts to shore up bottom lines. And ironically, by continued defections of the up-and-coming rainmakers these firms are desperately trying to hold onto; who are realizing that they can retain more of what they bring in by moving to a lower-overhead environment. All of these lawyers have the same objective; identifying low cost alternatives to enable them to fully utilize today's dizzying array of technology. And to do it without a constant distraction from billable work for clients in order to deal with technology issues.

The most pressing question, even before the who, what, and how of best utilizing technology through the cloud, is ***can I***? Understanding the ethical issues, and the lawyer's obligations, is the overriding concern. The cloud is scary. And largely misunderstood. Equally unclear are the lawyer's obligations and how they may be met in a simple to understand, pragmatic, best-practices way. My goal for this article will be to clarify these issues for the reader.

Using the cloud isn't anything new. Even if you don't realize it, you've been using it for years. For example, when you do research on LexisNexis, Westlaw, or InCite, you're conducting legal research in the cloud. Many of you use internet-based email platforms, like Gmail, AOL, Hotmail or Yahoo mail. If you do, your client communications are stored in the cloud. Increasingly, lawyers are using Hosted Exchange Server for their Outlook email, in order to gain functionality and synchronization with mobile devices. Again, email in the cloud. Cloud computing doesn't mean just one thing. It is a term which can apply to several meanings. For most of you it is sufficient to know that it generally means accessing information and/or running apps — programs — across the internet, on-demand, from anywhere you can get an internet connection, without the need to store the information or software locally. A more specific name used might be SaaS (software as a service) which indicates utilizing software through the internet, such as time & billing, case management, or e-discovery documents; or Cloud Hosting, which is a means of storing your data on a remote file server owned by a third party and accessing it through the internet.

Ask any attorney what their greatest fear is regarding venturing into the cloud, and concern over security is always the first response. Security risks surround a lack of direct control over who might have access to confidential client data, as well as the possibility that the data might not be available at all times. The reality is that even with a "traditional" computing environment, the same risks exist.

There is no absolute data security; it just doesn't exist in the real world. Third parties have always had access to confidential client data; contract employees, temporary employees, cleaning services, building and maintenance personnel, and even outside IT support personnel. And we're not talking just about digital data, we're also talking about confidential client data in paper form in document storage facilities, in physical files throughout the office, and sitting on desks, credenzas, and in many offices, in piles on the floor.

There is absolutely no system which is guaranteed to have your data available at all times. Having your data stored locally does not eliminate the possibility of a critical system outage which makes that data unavailable. It does not eliminate the possibility of data loss from a security breach, a virus, or a natural disaster. There are many lawyers who can attest that an office fire or flood can destroy both electronic and physical files in one fell swoop. And as we are now all too aware following the Gulf Coast disaster caused by Hurricane Irene, and the local disaster of Hurricane Sandy, having a backup taken home at night may not be enough to ensure recovery. In point of fact, with written guarantees of 99.999% uptime from cloud SaaS and hosting vendors; with security measures far beyond what any firm — other than one global in nature — can afford to deploy; and with hardware and power redundancies which make mother nature's efforts to create failure futile, you are safer in the cloud.

The advantages of cloud computing are many. First, you can access your data from anywhere you can get an internet connection, on a variety of devices. There is minimal capital investment needed. It is a pay-as-you-go model, with minimal installation headaches and costs. It is a scalable solution that can upsize or downsize as your needs change. There is little if any maintenance required by the firm; the vendor does fixes, upgrades, backup and even training in many cases.
Depending on the vendor and product, unlimited end-user support may also be included.

Cloud computing has some disadvantages as well. Not all software features may be available through a browser. There is usually less ability to customize, and less choices available to integrate with other software packages. Sometimes there is slower performance, depending on the internet connection. Of course, if you stop paying, it stops working, or you lose access to your data. In the long-term cloud

computing can be more expensive, because unlike a traditional business lease, where payments eventually end, your cloud computing expenses continue month after month. However, there is debate about this point, because the computation of "total cost of ownership" used to arrive at this conclusion rarely takes into account the savings in billable hours and staff time managing a traditional in-house system.

The true Achilles heel of cloud computing is the fact that the lawyer is depending on a third party — the vendor — to fulfill the professional obligations concerning security, confidentiality, and other ethical requirements. Hence the need to do ones due diligence.

We are fortunate in PA to have Formal Opinion 2011-200 [Ethical Obligations for Attorneys Using Cloud Computing / Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property]. It clearly spells out exactly what an attorney must consider and do to meet the requirements of Rule 1.0 (Terminology), Rule 1.1 (Competence), Rule 1.4 (Communication), Rule 1.6 (Confidentiality of Information), Rule 1.15 (Safekeeping Property), and Rule 5.3 (Responsibilities Regarding Non-lawyer Assistants) when venturing into the cloud.

In response to the question, "May an attorney ethically store confidential client material in 'the cloud'? " the short answer is:

> *Yes. An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.*

Lawyers are correct in being concerned about the security and confidentiality of data stored in the cloud. However, as long as you make informed decisions about the selection of a vendor you can eliminate or minimize the risks.

You need to know what security measures the vendor has in place. You need to know what protections they employ to prevent loss of your data, and ensure reliable access. You need to know the exact physical locations where your data will be stored in order to ensure that those jurisdictions do not have laws or rules that would permit a breach of confidentiality. You have to carefully review the Service Level Agreement — the thing most people click AGREE to without actually reading — to make sure you remain the owner of your data, and that this will not change if the vendor becomes insolvent, or because you are not paying disputed charges. You need it to confirm that the vendor understands, embraces, and is obligated to conform to the professional responsibilities required of lawyers, including

specific agreement to comply with ethical guidelines.

Page 8 – 11 of Opinion 2011-200 lists the essential requirements necessary to meet the standard of reasonable care for cloud computing. You will note that most are the same safeguards which would be applied to firm employees and vendors supporting a traditional in-house computer system. Start your journey with a review of this Opinion, available to members on the PBA web site, followed by a call or email to me. I can provide you with a detailed list of the questions you need to ask a prospective vendor, and what you need to verify, in order to ensure you have met your duty of due diligence. This comprehensive list was created as a joint effort of Practice Management Advisors like myself in the U.S. and Canadian territories. I can also assist you in thinking through other practical considerations, such as data migration to and, if necessary, from the vendor's system. As well as what might serve you best in-house versus out-sourced in the cloud, and how to tie them together.

There's really no reason you can't take advantage of the myriad of technological tools readily available and affordable in the cloud. What holds most of you back is fear that your lack of knowledge will create an ethical disaster. But it's not that difficult to make solid decisions which satisfy your ethical requirements. You just have to know what questions to ask, and what the acceptable answers are.

A version of this article originally appeared in the Spring 2013 issue of the PBA Solo/Small Firm Section Newsletter.