

Cloud Computing and Virtual Law Practice Issues

By Kim Brand

The Internet has changed everything, or so it would seem. The availability of high speed Internet access, scalable computing infrastructure and low cost data storage have made it possible for lawyers to utilize IT services delivered ‘virtually’ rather than purchase equipment and software and have it installed ‘physically’ in their offices. The fashionable term for this arrangement is ‘Cloud Computing.’ So named because the services delivered, and the data managed, are ‘out there’ somewhere on the Internet. If you haven’t noticed the proliferation of these services, you haven’t been paying attention.

Cloud services have literally revolutionized the computing industry and are poised to change the way lawyers practice law. In a future dominated by this Software as a Service (SaaS) model, your PC (or a mobile device like a laptop or iPad) will simply be a means to get you onto the web. Your workplace will be your browser and your location will be irrelevant.

I was recently asked by the Indiana State Bar to participate on a panel that discussed this new computing paradigm. As a non-lawyer, my focus was limited to technical issues related to data safety and security, connectivity and productivity. To be sure, the state of the art is changing almost daily. My brief remarks, and this short article, are intended to simply present some issues that the practitioner should consider *in addition to* the utility of the particular service he or she may be considering to employ.

1. Service Level Agreements (SLAs): What are they? Why would you want one?
2. Passwords: Global access makes strong passwords more important.
3. Getting out: What happens if you want to change providers and get your data back?
4. Internet Service: Why you should rethink Internet access for Cloud based applications.

SLAs

A Service Level Agreement is the contract you execute with a web services provider that defines what they do for you, how they protect your data and what happens if something goes wrong. Many providers use Amazon's Elastic Compute Cloud (EC2) service, which defines a service up-time commitment of 99.95%, (leaving only 4 hrs 22 minutes per year of downtime,) and a refund policy: a 10% service 'credit'. They specifically disclaim any other liability if access to their service or your content is interrupted.

The Google Apps SLA includes this term concerning disclosure of Confidential Information:

Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

ATT's popular High Speed Internet Business Edition SLA guarantees 99.99% uptime for their *backbone*, but only that your DSL service will be repaired within 24 hrs if your service goes down - and a 1 day credit for the service (about \$2 to \$3) if they don't get you working by then.

Rackspace is a popular Cloud Services wholesaler to many application providers. They guarantee 100% uptime - or you get a 5% credit on your monthly bill for every 30 minutes their servers are unavailable. After 10 hrs you could presumably get a 100% credit.

My own experience with hundreds of customers is that, for each, their Internet goes down a few times a year. The fix is usually to reboot a piece of equipment – but sometimes the outage lasts much longer. And I've noticed that bandwidth providers aren't as helpful for \$60/mo as they once were when their fees were over \$1000/mo. Your mileage, as they say, may vary.

It is important to know that SLAs apply to all the parts of your Cloud Service experience. Your Internet provider has one, the application hosting service has one and your application developer may have another. This creates an SLA 'Stack' which, like stacking errors in the real world, produce an overall less reliable experience than if taken separately. The strength of the chain being that of its weakest link.

Passwords

Cloud based applications are so named because they are 'out there' - like clouds. They are accessible from nearly everywhere you have an Internet connection. That is an empowering notion. Work can be done from anywhere at anytime. But that also results in access to potentially private materials from everywhere by anyone.

There are two basic threats to security: skill and time. If someone has sufficient skill they can probably hack into your system. If even an unskilled person is given enough time, they can probably hack into it too. The benefit of protecting private information inside your office and limiting access using doors and locks is that you make it difficult to get access to your stuff by people you don't know.

Putting information in the cloud assures access from anywhere but increases that chances that smart people with time on their hands may try to steal your data. Your Cloud Services vendor should assure the security of their systems. But your main defense is your password.

At minimum, password policies need to be reviewed. Using your first name to login to your on-premise server may be OK, but it is irresponsible if you are using a Cloud based service - literally anyone can guess your first name! A recent breach of a popular website allowed some post-hack forensic analysis of the passwords people commonly used. The most popular password: 123456. Number two: password.

People have a hard time remembering complicated passwords. They don't like to change them often. But those are the two basic requirements in the world of globally accessible applications and data.

Products and services are becoming available to make password management safer and easier. The Yubi Key is a \$25 USB device that generates a complex one-time-use password. It can be used alone or with another password to create a two-factor authentication scheme recommended by most security experts: something you *know* and something you *have*. (Biometric authentication adds a third: something you *'are,'* to the list: your fingerprint, distribution of blood vessels in your retina, etc.) I predict we'll see more of these hardware 'tokens' in use for Cloud Services in the future.

LastPass is a Cloud Based password storage vault where, with one password, you can unlock a web-based file holding all your other passwords. Sounds like a great idea - except - LastPass was apparently hacked in May 2011 forcing the company to recommend that its users change their administrative password to prevent all their other passwords from being compromised. They promised greater vigilance in the future. There seems to be no foolproof system yet that combines 'simple' and 'safe' when it comes to Cloud Security.

Here is the bottom line: the most secure - 256 bit encrypted - biometrically protected - 24/7 guarded - multiple firewall defended - data center in the world is impotent if your password is password!

Getting Out

I once used a wonderful Client Relationship Management (CRM) system. It integrated telephone calls, contact history, calendar, to-do list and other productivity aids. I was in love!

Then the service went bankrupt. Happily, they gave me plenty of time to rescue my data from their servers. (Several recent Cloud Service failures didn't end so well.) I retrieved my data into multiple Excel spreadsheets but the application that stitched all that data together into a fabric of information was lost – and so was the productivity their software promised.

Be careful to learn what your cloud application vendor's policy is on getting your data out of their 'old' cloud and into your 'new' cloud - or onto your PC if they go away or a better service comes along. It is certain that there will be much shifting and shaking in the

world of cloud services; as usual there will be a few winners and many losers. Protect your information and your productivity by assuring that what goes up can come down.

Internet Service

In a typical office connected to local resources like PCs, servers, printers, scanners, copiers, etc. using a local network there are many points of failure. If one piece of equipment fails there are others that may still be used. While a single point of failure may disable the network, individual PCs usually still work.

If you depend on Cloud Services to work, your Internet connection is a single point of failure which can dramatically affect your productivity – even if it simply slows down.

Consider these factors when moving to the Cloud:

- The dependability and speed of your local Internet service
- The dependability of the Internet service and equipment at the location where the provider's servers are located
- Performance of those networks: speed, access, security, backups, etc.

Most Cloud Service vendors have taken care to build redundancy into the means by which their applications and services are delivered - and that includes redundant connections to the Internet, fail-safe power protection, expensive server replication and fail-over technologies and 24/7 monitoring. After all, if something breaks at the vendor, potentially thousands of users could be affected.

But most attorneys' offices don't have such redundancy - in particular, redundant access to the Internet is a rare luxury. We have seen several instances where Internet access has been unavailable for days with an equipment or service outage which leads to real suffering by affected clients.

With Internet service becoming a vital part of the production of work product, the speed of the Internet takes on additional significance. Faster/cheaper Internet service is becoming available in many areas. But upgrades in some business locations have lagged behind residential deployment delivered over home cable TV service. A single 'T1' (still \$300+/mo) is no longer the 'gold standard' for Internet access.

The bottom line is that before committing your firm to a cloud-centric application environment you should make sure you know your 'backup' options for alternate Internet access; or, create a plan for doing without those services for periods of time should the Internet be interrupted at your office. Also, take advantage of trial periods to 'feel' the performance of web based applications over several days' use. In a business where time is money, staring at the screen watching an hour glass spin is no way to spend your time.

For the original version of this article, including links to many additional resources, visit <http://bit.ly/inbar-cloud-tech>

Kim Brand is President of Computer Experts, Inc. Kim has spent over 30 years in the technology industry; from software developer to IT consulting to leader of his Indianapolis based IT service company: Computer Experts, Inc. He is the inventor of 'FileSafe,' a small business file server in use by many law firms and other small businesses across Indiana. www.FileSafeServer.com. Kim is the author of two books, several published articles, whitepapers and speaks regularly on technology subjects ranging from data safety to email management. Audiences regularly praise his translation of 'Geek Speak' into understandable English. He is on the board of the International Legal Technical Standards Organization (ILTSO) and was a principal contributor to the 'Local Networks' standards introduced in April of 2011.

©2011 Kim Brand. All rights reserved.