Cloud Computing Services – Cloud Storage

by

Joshua H. Brand, Assistant Director
Minnesota Office of Lawyers Professional Responsibility

(As submitted to Minnesota Lawyer for publication on 1/2/12)

With the ever-increasing role that technology is playing in both our personal and professional lives, it is important to keep in mind how our ethical duties are continually evolving with the advancement and use of technology. One emerging area of relevance to attorneys is the use of cloud computing services and, in particular, cloud storage services. Distilled down to its most basic terms, cloud computing can be defined as the shared use of—and remote, universal access to—a third party's computer equipment, software, or services.[Ftn1]

Gone are the days when, if an attorney wanted to work on a client matter outside of the office, he or she had no option other than physically having that client file with them. Now, with a computer and an internet connection, an attorney is able to access client file information uploaded to third-party servers from halfway around the world. Cloud storage certainly has the potential to greatly enhance both the attorney-client relationship and attorney productivity. However, bear in mind that the use of technologies such as cloud storage will never lessen—and may, in fact, increase and make more complicated—an attorney's obligations under the Rules of Professional Conduct.

So, what issues must an attorney consider and what requirements might be imposed upon an attorney when utilizing cloud computing for the storage of client file information?

As an initial matter, an attorney must have at least a base-level comprehension of the technology and the implications of its use. While no attorney is required to know precisely how cutting-edge technology truly works or be a computer genius, the competence requirements of the Rules necessitate at least a cursory understanding of any technology used if for no other reason than to enable an attorney to effectively communicate to a client the pros and cons of its use in the representation.[Ftn2]

As the preservation of the confidentiality of client information is of paramount importance to the attorney-client relationship, an attorney must be aware of the potential risks inherent in the use of cloud storage services before uploading client data to third-party-owned and operated off-site servers.

Are such services secure? The short answer is the classic attorney response: it depends. No matter how good a third-party's security system is, it is a near-guarantee that anyone with enough time, money, and applicable expertise can find a way to bypass it. That truism applies equally to an attorney's personal computer; however, the risk of a security breach of a cloud storage server is that a client's stored information can be accessed and/or destroyed in its entirety in moments. One relatively easy and initial step an attorney can take to increase the security of client information—be it stored on- or off-site—is to keep such information password-protected.[Ftn3] While complete security is never achievable, a prudent attorney will employ reasonable precautions and thoroughly research a cloud storage vendor's security measures and track record prior to utilizing the service.[Ftn4]

Reasonable precautions may also require an attorney to read and understand a vendor's user and/or license agreement(s) prior to uploading client information to their servers. Does the vendor agreement address confidentiality? If not, is the vendor willing to sign a confidentiality agreement or otherwise bind its agents to your obligations of confidentiality to your clients? What happens to stored information in the event the vendor goes out of business or the attorney decides to terminate use of the service? If an attorney defaults on payments to a cloud storage vendor, will the attorney still be able to access and retrieve stored client information or will the vendor revoke the attorney's access to the information and effectively hold the data hostage in lieu of payment? Are a vendor's servers located in countries with less-stringent legal protections against search and seizure? Even if the servers are located domestically, to what lengths will a vendor go to fight the subpoena of information maintained on their servers? The answers to all these questions and more need to be considered prior to an attorney's utilization of cloud storage services. Despite these potential issues, most states that have issued formal opinions concerning cloud storage have determined it is permitted with proper precautions.[Ftn5]

In conclusion, the use of technologies such as cloud computing can be of great advantage to an attorney's law practice and is completely acceptable under the Rules of Professional Conduct provided an attorney first conducts the requisite due diligence necessary to safeguard the integrity of stored client information.

---

[1] Shannon Brown, *Cloud Computing 101 for Lawyers*, At Issue, 8-9, 10 (Spring 2011), http://www.pabar.org/public/yld/pubs/atissue/AtIssueSpring2011.pdf.

[2] *See generally* Rules 1.1 and 1.4, Minnesota Rules of Professional Conduct; *see also* St. B. of Ariz. Comm. on the Rules of Prof'l Conduct, Formal Op. 09-04 (2009) ("[L]awyers [must] recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.").

[3] *Cf.* St. B. Assn. of N.D. Ethics Comm., Op. 99-03 (1999) (permissible to use online data storage system provided confidential client information is protected and the password for access to stored information is restricted only to authorized persons, similar to how a law firm would control access to keys to a locked room containing a client's paper records).

[4] This may include requesting copies of the vendor's security audits and determining the specific level and type of security measures employed (i.e., firewalls, levels of encryption, intrusion-detection protection, etc.).

[5] *See, e.g.*, N.Y. St. B. Assn. Comm. on Prof'l Ethics, Op. 842 (2010) (online data storage of client information is permissible provided reasonable care is exercised to ensure that client confidentiality is protected); St. B. of Nev. Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 33 (2006) ("[A]n attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney's direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services.").