

Ethics up in the Clouds

By Travis Pickens

Cloud computing may as easily be called “Internet” computing. The idea is that all your law practice data and software platforms and services are operated, maintained and stored offsite by a vendor up in the “cloud,” and you are allowed to access it from any location through the Internet. Also generally known as SaaS (software as a service), it has been defined as:

[S]oftware that’s developed and hosted by the SaaS vendor and which the end user customer accesses over the Internet. Unlike traditional packaged applications that users install on their computers or servers, a SaaS vendor owns the software and runs it on computers in its data center. The customer does not own the software but effectively rents it, usually for a monthly fee.¹

The outside vendor provides ongoing technical operation, maintenance and support for the software provided to the lawyer, and it all takes place outside of your office. Sometimes the related concepts of IaaS (infrastructure as a service) and PaaS (platform as a service) are used in discussions of cloud computing, but the grand idea of all these concepts and how they interrelate to form the cloud computing methodology is that the lawyer is not storing information on his or her own computer and server, nor maintaining it. Someone else is, and the lawyer is simply accessing all of it through the Internet. Online services now available to attorneys include law practice management systems, document management and storage platforms, document and information exchange services, e-mail networks, digital dictation services and billing/timekeeping services.²

Cloud computing options offer extraordinary flexibility to the practice of law. Imagine being able to practice from any location that is Internet accessible, anywhere in the world, whenever you want. Then, imagine no loss of time or function; all of your files are accessible, and all of your client documents are available. You can work, manage and even bill your time as if you had driven to your office.

The software programs you use are continually, seamlessly updated by the vendor. There are no new patches or updates to install in your office, no incompatibility issues, and no scheduling hassles or surprise costs with the IT department or contractor. You typically pay a set monthly subscription fee.

This is what cloud computing proposes to bring to the table for consideration. There is no reasonable question that cloud computing in

some form has a place, if not now then shortly, in the practice of law. The key concern however for us, now and in the future, is how do we ethically use it?

Cloud computing raises ethical issues in at least the following areas of ethics:

- maintaining confidentiality of client information³
- safekeeping client property⁴
- competence⁵
- diligence⁶
- expediting litigation⁷
- communication⁸
- supervisory responsibilities⁹

All these ethical issues must be carefully considered.

SEVERE WEATHER

Confidentiality and Safekeeping Property

The most fundamental precepts of the attorney-client relationship are confidentiality and safekeeping of client property and information.¹⁰ What happens when an outside vendor/third party enters the equation, at a remote location — maybe in another country, with virtually all of your client information stored on their equipment?

Trusting third parties outside the law office with client information is not a novel idea and has passed ethical scrutiny, *e.g.*, the U.S. Postal Service, experts, court reporters, graphic artists and independent IT consultants, so the fact that third parties are involved is not in itself an insurmountable barrier. But cloud computing ramps up the involvement of third parties to an entirely new level. Almost all of the lawyer's data and files that mattered to his or her practice would be stored and maintained by someone else, somewhere else.

To varying degrees, ethics opinions from a handful of other states indicate that cloud computing systems, in some form, may be utilized, but at least at this point, there is not an Oklahoma Supreme Court decision or an opinion from the Oklahoma Legal Ethics Advisory Panel.

In December 2009, the Arizona State Bar Committee on the Rules of Professional Conduct issued an opinion which held that with reasonable precautions to safeguard security and confidentiality, firms may use an online file storage and retrieval system that enables

clients to access their files over the Internet.¹¹ The committee had previously determined that electronic storage of client files is permissible as long as lawyers and law firms "take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence."¹² The Arizona committee also said "[i]n satisfying the duty to take reasonable security precautions, lawyers should consider firewalls, password protection schemes, encryption, anti-virus measures, etc."¹³ This opinion followed opinions issued by the ethics committees of the states of New Jersey¹⁴ and Nevada.¹⁵ Generally, these states' opinions permitted use of an outside server provider to store client files in digital format, provided the attorney exercised reasonable care. The Arizona committee approved a system in which documents would be converted to a password-protected PDF format and stored in folders with unique, randomly generated alphanumeric names and passwords.

The Ethics Committee of the North Carolina State Bar issued a "proposed" ethics opinion that states a law firm may contract with a vendor of software as a service for apparently a multitude of purposes, provided the risks that confidential client information may be disclosed or lost are effectively minimized.¹⁶ The committee reasoned that a lawyer must take reasonable precautions, but it noted that no particular mode of use (*i.e.*, computing use) is dictated by the Rules of Professional Conduct. The opinion has not been adopted and the issue has been directed to a subcommittee for further study.

More recently, the New York State Bar Association Committee on Professional Ethics has issued Opinion No. 842 on Sept. 10, 2010, holding lawyers may store clients' confidential information online with a third-party provider so long as they take reasonable care to vet and monitor the provider's security measures and stay abreast of technological advances and the changing law of privilege.

Cloud computing does introduce a heightened risk, at least in theory, in the sense that it outsources all, or nearly all, of a lawyer's data to an off-site location. Thus, the information is perhaps more vulnerable to hackers, snoops and governmental investigations.

But rock-solid certainty is not required. Significantly, in the few ethics opinions that have addressed it, the consensus appears to be that

the law firm is not required to *guarantee* that the system will be *invulnerable* to unauthorized access. In fact, one way to consider the integrity of cloud computing security is to contrast it to what is commonly done now. It is not a particularly compelling argument to say that an office with a light wooden or glass door in an executive suite, with a simple door handle lock, completely accessible by all office personnel, cleaning crews and the landlord, is the vanguard of security. An argument can be made that cloud computing is *more* secure than traditional methods precisely because it is off-site in what is almost certainly a more secure facility with redundant backups and superior electronic protection.

It makes sense that you seek and obtain your clients' "informed consent" to a cloud computing arrangement if you choose to use it. Should cloud computing become an attractive option for your law practice, provisions regarding the use of cloud computing should be included in your fee agreements.¹⁷

One aspect of cloud computing your clients will likely appreciate is the ability to go, through their own passwords, directly to their file in the cloud and retrieve copies or new documents posted by your firm, all without a call or e-mail to your office.

Competence, Diligence and Expediting Litigation

Comment to Rule 1.6 of the Oklahoma Rules of Professional Conduct states:

A lawyer must act *competently* to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.¹⁸ (emphasis added)

Ethics committees have emphasized that law firms without the requisite expertise should consult with their own IT professionals in evaluating these decisions and arrangements. Many lawyers shy away from technical expertise and need independent advice not only to understand the technical terms of the underlying deal, but to fully investigate the

privacy and use concerns raised in evaluations for purposes of compliance with the Rules of Professional Conduct.

One perspective that is sometimes lost in these discussions is the impact of technology in *remaining* competent to practice. Comment [6] of Rule 1.1 of the Oklahoma Rules of Professional Conduct states:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law *and its practice*, ...¹⁹

This language ("and its practice") was likely written to address substantive law and procedural matters, but there may be a day when competence in the current technology is a factor in assessing disciplinary matters. For example, the Canadian Bar Association's rule on attorney competence includes the following comment:

4. Competence involves more than an understanding of legal principles; it involves an adequate knowledge of the practice and procedures by which those principles can be effectively applied. To accomplish this, the lawyer should keep abreast of developments in all areas in which the lawyer practises. The lawyer should also develop and maintain a facility with advances in technology in areas in which the lawyer practises to maintain a level of competence that meets the standard reasonably expected of lawyers in similar practice circumstances.²⁰

“When you place this amount of information in the hands of an outside provider, you introduce a different type of risk.”

The ABA's Commission on Ethics 20/20, appointed in 2009, is now reviewing the impact of advances in technology on the Model Rules of Professional Conduct and how they should be adapted to reflect those advances. A law office need not be a studio of technological wizardry, but it should not be mistaken for a Luddite village. Clients now expect a certain level of technological savvy. Perhaps your practice is one that can still manage using hard-copy letters, three-ring notebooks and brown expansion folders in gray metal file cabinets, but the sun is setting on this charming but moribund style of practice. If the mode of practice completely forsakes technological

progress, there may well be a day in the future when that practice becomes “incompetent,” at least presumptively.

Related to competence are the duties of diligence and expediting litigation.²¹ These requirements clearly present the “availability” component of computer security. If the information is not available, the lawyer can be neither diligent nor expedite litigation. Any cloud system utilized must be evaluated in terms of remaining constantly available and providing adequate and timely backup. These should of course be areas of careful inquiry of a vendor (and contractual responsibility).

Communication and Supervisory Responsibilities

A lawyer must keep a client reasonably informed about matters being handled by the lawyer.²² This obligation imposes a duty to communicate with a client in order to: 1) avoid causing inconvenience and unnecessary expense to the client; 2) keep a client informed about the status of a matter entrusted to the lawyer; and 3) enable the lawyer to respond to a client’s requests for information.

The information must be available to the client. When you place this amount of information in the hands of an outside provider, you introduce a different type of risk. Whether it will be on balance, a more significant risk remains to be seen. There are risks with every level of technology. Presently, office computer hard drives crash, software malfunctions and computers get stolen. It is clear that lawyers may not wholly delegate security concerns. The firm will be held responsible for overseeing how the sensitive data is being collected and stored.

Finally, and equally important, lawyers have responsibilities for non-lawyer assistants.²³ The managing lawyer must put measures in place that ensure the assistants’ conduct will be compatible with the responsibilities of the Oklahoma Rules of Professional Conduct. The prudent attorney will be careful to contractually require vendors with whom they deal for cloud computing to have protocols that meet these standards.

OKLAHOMA FORECAST

At the time of this article, there is no indication that Oklahoma will approach this issue much differently than the states that have already weighed in. But, it remains to be seen.

What are the “best practices” that a law firm should follow when evaluating cloud computing and an appropriate vendor? First of all, many questions should be asked. As gleaned from the articles and opinions on cloud computing (*see* Endnotes), the questions should include at least the following areas:

- The track record and financial stability of vendor
- Your own understanding of the vendor agreement. Do you truly understand it in all of its technical complexity? Should an independent IT consultant be retained for the analysis of security, backup and negotiation of terms?
- Confidentiality generally, as it is addressed by the vendor agreement and regarding its employees (and employees that may leave the vendor’s employment)
- The specific physical and electronic safeguards and security, preserving confidentiality of stored data, including the specific types of encryption and passwords used
- The vendor’s history with security audits
- The host country and related search and seizure laws
- The persons with access to the data
- The ownership of the data — vendor or lawyer?
- The protocols and access to information once the use of the product is terminated, or if the vendor goes out of business
- The compatibility of vendor’s software with similar vendors
- The ability of the lawyer to retrieve data from the server to use or back up
- How frequently are backups performed?
- Is information backed up to more than one server?
- The safeguards against natural disasters
- Whether there is direct access to the data by clients, and related confidentiality risks
- The lawyer’s own backup in case something goes wrong
- Will the vendor contractually agree to protocols compatible with the requirements of the Oklahoma Rules of Professional Conduct?
- What happens when there are “temporary” power outages?
- How are the risks allocated?
- Indemnification and insurance considerations

In addition to these questions, prudent practitioners considering cloud computing should:

- Seek and/or rely upon a written ethics opinion from the Oklahoma Legal Ethics Advisory Panel prior to wholesale, unqualified transition to and investment in the “cloud.”
- Use programs recommended by law-related technology experts, such as the OBA’s Management Assistance Program Director Jim Calloway, or those “certified” or endorsed by bar associations, law-related organizations and groups.
- Carefully document your due diligence in evaluating cloud computing products.
- Consider a “hybrid” approach to computing, slowly and carefully incorporating cloud computing as it evolves as a technology. It may be the best computing system for you is a bit of both.
- Disclose your use of cloud computing in your written fee agreement with your clients and get their informed consent.

CONCLUSION

Barring unforeseen challenges, cloud computing should be welcomed as a valuable technological advance that will provide an entirely new level of freedom and convenience for the lawyer and the client. However, it must not be wholly embraced without deliberate analysis, discussion, testing and time to evaluate its complexities in the field.

It may be the future, but we will get there one day at a time.

1. www.cio.com/article/109704/Software_as_a_Service_SaaS_Definition_and_Solutions; Levinson, Meridith.

2. “Cloud Computing for Lawyers: An introduction,” Nicole Black, Feb. 2, 2010 <http://blog.firmex.com/cloud-computing-for-lawyers-an-introduction>.
3. ORPC 1.6.
4. ORPC 1.15.
5. ORPC 1.1.
6. ORPC 1.3.
7. ORPC 3.2.
8. ORPC 1.4.
9. ORPC 5.3.
10. ORPC 1.6 and 1.15.
11. Arizona State Bar Comm. On the Rules of Professional Conduct, Op. 09-04; www.myazbar.org/ethics/rules.cfm.
12. Arizona State Bar Comm. On the Rules of Professional Conduct, Op. 05-04; www.myazbar.org/ethics/rules.cfm.
13. Arizona State Bar Comm. On the Rules of Professional Conduct, Op. 05-04.
14. N.J. Supreme Court Advisory Comm. On Prof’l Ethics, Op. 701 (2006).
15. Nev. State Bar Standing Comm. on Ethics & Prof’l Responsibility, Formal Op. 33 (2006).
16. Ethics Committee of North Carolina State Bar proposed 2010 FEO 7, April 15, 2010; <http://socialmedialawstudent.com/featured/north-carolina-publishes-proposed-ethics-opinion-on-cloud-computing/>.
17. ORPC 1.0 (e) & (n).
18. Ethics Committee of North Carolina State Bar proposed 2010 FEO 7.
19. ORPC 1.1 Comment [6].
20. Canadian Bar Association Rules of Professional Conduct, “Competence and Quality of Service,” Comment [4].
21. ORPC 1.3 and 3.2.
22. ORPC 1.4.
23. ORPC 5.3.

ABOUT THE AUTHOR



Travis Pickens serves as OBA Ethics Counsel. He is responsible for addressing ethics questions from OBA members, working with the Legal Ethics Advisory Panel, monitoring diversion program participants, teaching classes and writing articles. A former litigator in private practice, he has served as co-chair of the Work/Life Balance Committee and as vice-chair of the Lawyers Helping Lawyers Assistance Program Committee.



Informed.

We have the knowledge and experience to effectively and efficiently handle difficult and intricate immigration cases.

For more information contact
Amir M. Farzaneh at 405.528.2222.

Hall, Estill, Hardwick, Gable, Golden & Nelson
A Professional Corporation

Tulsa, OK Oklahoma City, OK Northwest Arkansas Washington, D.C. www.hallestill.com

HALL
ESTILL
ATTORNEYS AT LAW