

# Introduction to Cloud Computing And Its Ethical Implications – Is There a Silver Lining? (Part I of II)

BY JEREMY R. FEINBERG AND MAURA R. GROSSMAN

Understanding the legal and ethical implications of rapidly emerging technologies can be a bit like shooting at a moving target. It was barely 18 or 24 months ago that you could ask a lawyer whether he or she had a Facebook account, or “tweeted,” and you were likely to be met with a blank stare. In this short span of time, social networking sites have gone from fringe activities to mainstream tools in many lawyers’ marketing and communications arsenals. Now that Web 2.0 has become fairly common, the latest trend that some lawyers and law firms – and many of their clients – have begun to embrace, is cloud computing. In the first of this two-part series, we will provide a brief, non-technical introduction to what “cloud computing” is, explain why it is catching on, and at least identify some of the ethical issues that may arise from a lawyer’s use of this technology. In the second part of this series, we will consider a set of legal and ethical issues implicated by cloud computing, primarily when it is the lawyer’s client that makes use of this technology.

## What Is Cloud Computing? Why Is It Becoming So Popular?

Setting aside associate and support staff compensation for the moment, real estate and information technology (“IT”) costs are probably two of the most significant overhead expenditures for many law firms. Imagine, however, a law practice that did not house its own computer servers and other hardware, indeed, did not even have its own IT Department. Could such a law firm function in this day and age of ubiquitous electronic records? Sure, if it has embarked on cloud computing, a trend which essentially entails “outsourcing” some or all of the firm’s technology infrastructure, software applications, and storage needs to a third-party provider from whom the firm “leases” them, over the Internet, for a monthly fee. Cloud computing takes advantage of the convenience, scalability, and cost savings that can be achieved by sharing hardware, software, and data storage. It allows users at multiple, disparate locations to make use of a joint pool of technology resources that each alone might not be able to afford, without having to physically house or personally manage them.

Cloud computing first became possible because certain companies worldwide – among them Google and Amazon – amassed vast amounts of computer hardware and software so that they could handle the staggering consumer demands during the peak ordering season (*i.e.*, the holidays). In seeking uses for this IT infrastructure during the remainder of the year, when there was less call for the applications and servers, it occurred to these companies (and others) that they could make the excess resources available for “rent” to the public, through the Internet. (The “cloud” is the symbol used to depict the Internet in technical drawings). Law offices seeking to take advantage of the cloud could thereby secure remote access to virtually unlimited computing resources, 24 hours a day, seven days a week, on an as-needed basis, through a contract with a third-party service provider that linked them with the type(s) and amount(s) of IT resources they needed, ranging from proprietary software applications to document management systems and back-up storage.

The potential benefits for cloud users are obvious. Because of the savings in real estate costs and computer equipment, as well as on the personnel needed to manage on-site IT systems, cloud users can access the particular computing resources they need, at a particular point in time, for a fraction of the cost of owning and maintaining them. As their needs expand and contract, they can simply scale up or scale back without having to worry about details like electricity costs for operating and cooling equipment, or licensing fees and upgrades for software applications. The computing resources are conveniently available at any time, and from any place, as long as there is a working Internet connection. As a practical matter, however, use of the cloud means that a lawyer's (or law firm's) email, word processing, and document management systems – and all of the confidential client information contained on them – are no longer housed within the four walls of the lawyer's office, but rather, somewhere in cyberspace that the lawyer may not be able to readily identify at any given point in time. It is in these details that the devil may reside.

In an economy where the bottom line and around-the-clock accessibility have become increasingly important, to many organizations, cloud computing may seem like a no brainer. But before making the leap to the cloud, there are certain ethical issues that should be considered. Although a comprehensive discussion of the myriad legal issues implicated by cloud computing are beyond the scope of this article, the interested reader may wish to refer to the following series of blog entries, which provide an excellent overview of some of these issues:

<http://www.infolawgroup.com/2009/08/articles/cloud-computing-1/legal-implications-of-cloud-computing-part-one-the-basics-and-framing-the-issues/> (discussing the basics of cloud computing);

<http://www.infolawgroup.com/2009/09/articles/breach-notice/legal-implications-of-cloud-computing-part-two-privacy-and-the-cloud/> (discussing privacy considerations in cloud computing); and

<http://www.infolawgroup.com/2009/10/articles/cloud-computing-1/legal-implications-of-cloud-computing-part-three-relationships-in-the-cloud/> (discussing relationships in the cloud).

As for the pertinent ethical issues, we address below some of those that uniquely apply when it is the law firm that moves to the cloud. There are other issues that are implicated primarily when it is the client that chooses to do so. Those we will address in the second article in this series.

## **Ethical Issues When Law Firms Employ Cloud Computing – Is the Cloud So Different From Outsourcing?**

As a threshold matter, security and confidentiality are the predominant concerns whenever lawyers use technology to communicate and store confidential information and work-product relating to their clients. Rule 1.6 of the New York Rules of Professional Conduct (the “NY Rules”) stresses the absolute importance of safeguarding a client's confidential information, except in very limited circumstances where an exception applies. At least one local bar association committee has taken this a step further by requiring lawyers to stay abreast of developments in technology, particularly to the extent a lawyer uses technology to communicate with clients. *See* New York State Bar Association (“NYSBA”) Op. 782 (2004). In discussing the risks of transmitting documents containing metadata, the committee opined that, “a lawyer who uses technology to communicate with clients must use reasonable care with respect to such

communication, and therefore must assess the risks attendant to the use of that technology and determine if the mode of transmission is appropriate under the circumstances.” *Id.* These same concerns are present, and indeed, are likely magnified, when the lawyer stores and accesses confidential client information and work-product via the Internet.

As the language in NYSBA Opinion 782 suggests, the duty to protect confidential client information when using technology is not absolute, and is tempered by considerations of reasonableness. Indeed, if lawyers could be sanctioned solely for the inadvertent disclosure of confidential information, disciplinary committees would have their hands full keeping up with the number of lawyers to prosecute on the basis of errantly sent emails alone. The comments to the New York Rules reflect this same view. For example, Comment 16 to Rule 1.6 of the New York Rules states that a lawyer must “exercise *reasonable* care to prevent disclosure of information related to the representation by employees, associates *and others whose services are utilized in connection with the representation*” (emphasis added). *Accord* American Bar Association Model Rules of Professional Conduct (“ABA Rule”) 1.6, Comment 16. (Readers should bear in mind, however, that the New York State courts have only adopted the New York Rules and not the NYSBA’s comments. Therefore, the comments are no more than potentially persuasive authority.)

Comment 17 to New York Rule 1.6 echoes the themes set forth in NYSBA Opinion 782 in stating that, “the lawyer must take *reasonable* precautions to prevent the information from coming into the hands of unintended recipients. This duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may require special precautions.” NY Rule 1.6, Comment 17 (emphasis added). *Accord* ABA Rule 1.6, Comment 17. Elaborating further, Comment 17 also states that the “sensitivity of the information” and “the extent to which the privacy of the communication is protected by law or by a confidentiality agreement” are relevant factors in determining whether or not a lawyer should employ special precautionary measures. NY Rule 1.6, Comment 17.

As we all know, lawyers have been providing confidential client information to third-party vendors for years, with little or no adverse consequences. Before the advent of electronic discovery, it was not uncommon for lawyers to send hundreds of boxes of hard-copy documents (typically containing the confidential information of their clients) to commercial photocopying services for duplication by employees not directly under the lawyer’s (or the client’s) supervision or control. Confidentiality was secured by some combination of contractual agreement, industry practice, and general custom. Lawyers did not challenge the use of such vendors as a waiver of privilege, and disciplinary committees did not discipline lawyers for treating confidential client information in this fashion. Courts and disciplinary authorities would have had little else to do than address the flood of privilege motions and complaints that would have followed if this were not the usual custom and practice.

More recently, lawyers have ethically employed outside vendors for even more complex tasks, ranging from collecting and searching electronic evidence, to performing basic document review and preparing legal research memoranda or pleadings. The latter tasks are sometimes even outsourced overseas, to other countries, where the cost of performing these services is even cheaper than it is in the U.S. Ethics committees reviewing these practices have largely approved of them. In 2006, the New York City Bar Association (“NYCBA”) issued Opinion 2006-3, in which it established a five-step “checklist” for lawyers seeking to outsource legal activities overseas. To pass ethical muster, the lawyer engaging in such

outsourcing must (i) ensure that the client's confidences and secrets are preserved; (ii) supervise the non-lawyer to ensure that the non-lawyer's work contributes to the lawyer's competent representation of the client; (iii) take precautions to avoid conflicts of interest; (iv) bill appropriately for such activities; and (v) obtain the client's advance consent whenever confidential information is to be disclosed. *See* NYCBA Op. 2006-3 (2006).

Two years later, the American Bar Association largely followed suit with Formal Opinion 08-451 (2008). Although not addressing the duty of the outsourcing lawyer to perform conflicts checks, the ABA Opinion stated, "[t]here is nothing unethical about a lawyer outsourcing legal and nonlegal services provided the outsourcing lawyer renders legal services to the client with the 'legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation' as required by Rule 1.1 [of the ABA Model Rules]." ABA Formal Op. 08-451 (2008). Similarly, the bar association ethics committees of the other states have also weighed in approvingly on this issue. *See, e.g.*, Prof'l Ethics of the Fla. Bar, Ethics Op. 07-02 (2008); North Carolina 2007 Formal Ethics Op. 12 (2008); San Diego County Bar Ass'n 2007-1 (2007). Recently, the Professional Responsibility Committee of the New York City Bar Association released a detailed report addressing best practices and approaches for lawyers seeking to outsource legal and nonlegal work. The committee's report is available at:

<http://www.nycbar.org/pdf/report/uploads/20071813ReportontheOutsourcingofLegalServicesOverseas.pdf> (the "NYCBA Outsourcing Report").

If cloud computing is merely a form of outsourcing, are the ethical issues related to cloud computing really any different for law firms? If a lawyer follows the guidance on outsourcing from the New York City Bar and the ABA, among others, will everything be fine? Although the outsourcing opinions establish a useful backdrop, they do not in and of themselves resolve these questions because cloud computing raises many issues that are separate and distinct from "plain vanilla" outsourcing. For starters, how exactly is the lawyer to protect the confidential information of a client, when the lawyer has no idea what server it is stored on; the state (or country) in which the server is located; when and where the data might be moved; what is commingled with the client's data on the same server; who exactly owns the server the data is stored on (since many cloud providers sub-contract out the storage or other components of their process); and whether the cloud entity or entities will be solvent tomorrow?

A related issue is whether and how the lawyer can reasonably "supervise" the technical operations of many interconnected computer systems, entities, and personnel that may span the globe and constantly be shifting? And finally, can a lawyer effectively obtain the informed consent of a client who essentially must be told that every piece of confidential information they share with the lawyer will be placed on the Internet, and may thus be less than totally secure?

There are no easy answers to these questions, and the standard "Terms of Service" agreement with a cloud provider rarely addresses all these issues, so the ethical attorney must do appropriate due diligence and either learn (or associate themselves with someone who understands) the nuances of the cloud services they are seeking to employ.

Unfortunately, there is very little guidance out there for the interested attorney. No ethics committee opinion or court decision that we are aware of has grappled with these issues, at least as of yet. (We understand, however, from blog postings that North Carolina is now considering such an opinion. *See, e.g.,*

<http://www.myshingle.com/2010/04/articles/tech-web/north-carolina-wants-your-comments-on-cloud-based-practice-management-tools/>

One recent ethics opinion issued by the Arizona State Bar Committee on the Rules of Professional Conduct has at least opined on a factual situation that is similar in nature. In an opinion issued on Dec. 9, 2009, that committee analyzed whether a law firm ethically could make use of an online file storage and retrieval system that enabled both the client and firm to access confidential files over the Internet. Concluding that a reasonableness standard applied in connection with this activity, the opinion focused on the nature of the precautions taken to safeguard the security and confidentiality of the information. *See State Bar of Arizona Ethics Op. 09-04 (2009)*. (Notably, the opinion did not address the issues of supervision, client consent, or other issues flagged by ethics committees that have addressed typical outsourcing arrangements.)

The opinion mirrored much of the above reasoning of NYSBA Opinion 782 and the comments to the ABA and New York Rules. It recognized that the duty to take reasonable precautions does not mean that a lawyer must guarantee absolute protection against any and all unauthorized access, but rather, that the lawyer must use sound professional judgment to determine the types and level of precautions that are appropriate to protect against foreseeable attempts at unauthorized access. The opinion cautioned that lawyers must be mindful of the limitations on their knowledge concerning computer security and to consult with experts when necessary. Finally, the committee noted that because technology is ever-evolving, “whether a particular system provides reasonable protective measures must be ‘informed by the technology reasonably available at the time to secure data against unintentional disclosure.’ As technology advances occur, lawyers should periodically review security measures in place to ensure that they adequately protect the security and confidentiality of the clients’ documents and information.” *State Bar of Arizona Ethics Op. 09-04*.

To the extent that this ethics opinion establishes a continuing duty for lawyers to re-examine the security features and related protections afforded by the technologies they are using to handle confidential client information, it contains sound advice for lawyers who are considering a move to the cloud. There may be practical limits on how much a lawyer can learn about where its clients’ data will be located or moved, what it will be commingled with, and what its cloud service provider is doing to keep the data safe and secure. But before moving confidential information to the cloud, the lawyer should endeavor to learn as much as possible about the protections that will be afforded to that data and seek ongoing information from the cloud provider to make sure that the protections are reasonable and appropriate in light of changes and developments in technology.

The bottom line is this: there is nothing in the ethical rules that appears to prohibit a law firm’s move to the cloud when appropriate due diligence and precautions are undertaken. Not every lawyer, however, will have the technical competence to do that, and lawyers seeking to move to the cloud should associate with knowledgeable Internet technology experts when necessary. If the lawyer is unable to obtain sufficient information from the cloud provider to resolve concerns about information privacy and

security, and to understand the inner workings of the particular provider, it may be prudent to refrain from moving to the cloud, or to go elsewhere, where the cloud services are more transparent. Although supervision and oversight of third-party cloud providers may prove challenging, it behooves the lawyer to at least understand the provider's processes and to ensure that they are compatible with the lawyer's professional obligations. As one outsourcing ethics opinion stated, "[i]f physical separation, language barriers, differences in time zones, or inadequate communication channels do not allow a reasonable and adequate level of supervision to be maintained over the foreign assistant's work, the lawyer should not retain the foreign assistant to provide services." North Carolina Formal Ethics Op. 12 (2008).

In its recent report, the New York City Bar elaborated that the outsourcing law firm:

should establish practices and procedures for the supervision of offshore legal support that are sufficiently adaptable to the specific offshore entity and compensate for physical separation, time zone differences, and any differences in legal systems and legal education and training. This requires the law firm to become sufficiently familiar with the professional training of foreign professionals, attend to training the foreign professionals in relevant legal and ethical rules, and establish regular communications practices to ensure that the foreign professional has reasonable access to supervising lawyers in the local law firm.

NYCBA Outsourcing Report at pp. 5-6.

Because of the nature of cloud computing, "supervision" takes on a very different meaning in this context, as compared to the typical outsourcing situation. Many of the more important questions can and should be addressed in the contract with the provider. In Part Two of this series, where we address issues primarily related to a client's use of cloud computing technologies, we will focus on some of the challenges that should be addressed through contracting. For now it may be sufficient to say that in order to discharge the supervisory obligation, the ethical lawyer needs to think ahead, to fully understand the terms of the agreement, and to maintain an ongoing and open line of communication with the cloud provider.

A reader reaching this point might fairly complain that this article has raised as many questions as 6 as answered. With that, the authors cannot quibble. The application of the outsourcing analogy to cloud computing is decidedly imperfect, and cloud computing is very much uncharted territory. The ethical issues we have identified, and others, may well need to percolate further before they are more susceptible to definitive resolution.

---

*Jeremy R. Feinberg is the Statewide Special Counsel for Ethics for the New York Unified Court System. Maura R. Grossman is Counsel at Wachtell Lipton Rosen & Katz in New York. The views expressed in this article are solely those of the authors, and do not necessarily reflect the views of their respective employers and/or clients.*