The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations

A Report of the Small Law Firm Committee of the New York City Bar

Report Subcommittee:

Ashwini Jayaratnam, *Chair*
David Caplan
Tudor Capusan
Kenneth Rashbaum
William Aronin

October, 2013

The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations

A Report of the Small Law Firm Committee
of the New York City Bar

Introduction

Not so long ago, maintaining the information and research materials of a law firm required lots of space and, therefore, a great deal of cash. That function demanded endless shelf space, which was a seemingly insatiable demand as the practice grew. Client letters, case documents, memoranda and case notes multiplied faster than a colony of rabbits. The library usually needed its own room. Business development, too, required printing and publication of promotional materials. And - all this paper had to be mailed, shipped, couriered or hand delivered, adding more investment in staff and outside service costs. Further, organization of all that paper was its own nightmare, giving lawyers many sleepless nights concerned that a critical client document was misfiled or lost.

Then, in what seemed to be an answer to prayer, came the Internet Age. Suddenly, it seemed a relief to just store and transmit documents electronically. Tools like email, dedicated servers hosting multiple workstations, ECF (electronic case filing) and VPN (virtual private networking) made lawyers and their staffs capable of communicating with clients, courts and their offices from just about anywhere. Files were accessible from a person's desk, rather than down the hall in huge file rooms. Legal research through Westlaw™, Lexis™, or Fastcase™ became feasible, reducing the need for huge onsite libraries. It seemed great – but it came with the cost of new hardware-intensive technologies and steep learning curves. The expense of space was replaced with the costs of hardware and software training; IT departments replaced librarians and file clerks. For small firms, particularly, these costs were astronomical, if not utterly prohibitive. There had to be a better way, but where?

And then, this new prayer seemed to be answered; THE 'CLOUD' BURST FORTH! Even more suddenly than the explosion of Internet use, Cloud services providers appeared, eager to store all that information remotely, in the Cloud, and give lawyers (and others) the ability to access their and their clients' data from anywhere, just like before, but without the lawyers investing in IT staff, huge data storage rooms, or private networks. Providers also began offering document management, office organization and other Internet-based software platforms that purport to solve the organizational issues

with applications that are intuitive and easy for the lawyer to set up and manage.

Nirvana had arrived, especially, for small law firms. By leveraging this new technology, small law firms could afford the tools needed to grow their practices and compete on a level playing field with large law firms. Small firms or solos who previously could not afford physical storage space could now store their numerous client related documents on the Cloud, without having to worry about the cost and feasibility of hiring an IT department. More importantly, through the Cloud and wireless computing, small firms and solo attorneys could have constant access to client documents and communications whether they are travelling, in court, at a coffee shop, or at home. This increased availability to respond to their clients will give small firms an advantage that in the past they may have ceded to big firms with armies of associates and support staff.

Was it really that simple? The short answer is: Not completely. It is true that law firms cannot remain competitive if they are behind the technological curve, so adoption of Cloud-based solutions by the vast majority of U.S. lawyers, at least in part, is inevitable. But as soon as a lawyer turns over his clients' information to any third party, the attorney risks the loss of confidentiality. If the attorney leaves control of key software in another's hands, he risks losing the ability to function when timing is critical. With the Cloud becoming more ubiquitous, with clients demanding more responsiveness from their counsel, the question changes – from "whether to go to the Cloud or manage data through remote access devices (such as a laptop, tablet or smartphone)" to "*how to use these tools safely and ethically."*

Also, the issues are the same whether you access the Cloud through wired or wireless devices. The remote point must be secure and the means of transmission must be secured (e.g. encryption and administrative protocols on managing the electronic information). Your portable devices must be secured as well, Cloud or no Cloud. Data stored on smartphones, laptops, tablets and similar devices must be internally protected so that, if the device is lost or stolen, the thief or finder cannot access the information.

Enthusiasm for technology in the legal profession, therefore, needs to be tempered by sober reflection on the legal, regulatory and ethical risks that are raised by the complexities of managing electronic information. Of course, one might say that Cloud service providers are the same kind of third parties as the cleaning crews, external copy centers, and delivery services that have long been exposed to confidential client information. That is true, to a point. But putting data in the Cloud adds a whole new universe of parties with access, and the Cloud providers exercise far greater control than any of those other outsiders. The fact remains that, whether confidential and privileged information remains on-site within the firm, resides on the servers of a third-party Cloud provider, or rests in the drives of smartphones, tablet PCs or laptops, attorneys must know the rules and potential disclosure risks, and exercise reasonable care when choosing computing technologies and service providers.

This paper will explore the landscape of what is reasonable care. It will analyze required safeguards for client and firm electronic information in the context of law firm

practicalities, and the business case for moving to the Cloud and using portable devices. It will also outline ways in which lawyers should carefully evaluate all service providers to ensure that they employ sufficient procedures to protect clients' confidences and electronic information and how best to employ appropriate precautions when using portable media. Finally, the paper will propose practical ways to mitigate risk as information technology advances. It will offer ways in which lawyers can, and must, become educated regarding the technologies, and it will outline procedures required when contracting with Cloud providers and utilizing portable devices in order to safeguard client and firm data, thereby minimizing ethical and malpractice risks.

I. What is "the Cloud?"

The term "Cloud Computing" means different things to different people but, in the most basic of terms, "Cloud Computing" refers to the on-demand access to remote computing services over the Internet, such as productivity applications (e.g., Google Docs and Microsoft Office 360), online document and practice management software, and remote data storage and retrieval, available from anywhere one has an Internet connection.

A more technical definition of Cloud Computing is:

> . . . (A) model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.[1]

Many people use Cloud computing every day, perhaps without even realizing it. Examples include web-hosted email (such as Gmail, Verizon and AOL) and social media sites. For Cloud-hosted email, the email application and the actual messages are largely housed on servers far away from the user. When the user logs in *via* a web browser or PDA app, email is displayed on the local device but the user-issued commands (e.g., send, reply, or forward) are largely being processed far away, on one server or several.

The Cloud comprises three distinct models:

Software as a Service (SaaS) – In this model, the Cloud services provider offers access to a software application, such as Microsoft 360, to customers *via* an Internet connection such as a web browser.[2] This is the model that will be used most frequently by small law

---

[1] Peter Mell and Tim Grance, The NIST Definition of Cloud Computing (Draft) (Jan. 2011)(NIST Definition), at 2, available at http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_Cloud-definition.pdf. The National Institute of Standards and Technology (NIST), is the federal technology agency that works with industry to develop and apply technology, measurements, and standards. *Id.*

[2] NIST Definition, *supra* n 2, at 2. The article also notes access to the infrastructure is limited to user specific application configuration settings.

firms. The Cloud provider manages the underlying infrastructure through which the application is accessed (e.g., servers, storage, operating systems, etc.). Online backup services also fall into this category. Within the category of SAAS is Storage as a Service, which offers remote access to user-content (data that the user uploads to the service via the Internet). While users create and edit content using their own applications, software may be installed on the user's computer for easy upload to a Cloud-based repository, or for the purposes of enabling automatic data backup from the user's computer to the online storage service. Some services integrate the ability to share files and folders with multiple users. Many of these services use modern encryption methods for file transfer and storage. Popular examples of Storage as a Service providers include Google Drive, Dropbox, Rackspace, Carbonite, and Amazon Cloud Drive. Cloud storage allows the user to save data to a storage system that is remote and maintained by a third party. Examples of Cloud storage solutions are BitCasa, Dropbox, Google Drive, and SugarSync. Users create accounts and can upload or modify files anywhere there is an Internet connection. In addition to providing round-the-clock access from any Internet-connected computer (including mobile devices), harnessing the Cloud in this way eliminates the need to carry physical storage devices and the need to procure and maintain large amounts of storage. These services present the potential to increase productivity through collaboration, by enabling groups of users access to a single document in real time (sometimes contemporaneously) Some collaboration tools in these and other storage applications comprise additional capability, including authorization for users to make comments, see edits, and create multiple versions.

- **Platform as a Service (PaaS)** – Here, the Cloud user chooses the application(s) to which she has access, and can often configure and customize it. The user, then, has more control over the application than in a SaaS model, though the Cloud provider retains management of the underlying infrastructure.

- **Infrastructure as a Service (IaaS)** – In this last model, the Cloud user has control not only over the applications available to it, but also the capability to modify and manage essential computing resources (processing, storage, networks, etc.). The user also has the ability to control things such as operating systems, storage, and select networking components or host firewalls.[3] This model provides the most flexibility of all of the service models.

Generally speaking, nearly all of the services offered to small law firms and solo practitioners will be SaaS services. Few small law firm attorneys are going to have the time, interest and expertise to design their own software applications or network structures.

Cloud services are deployed in three variations, and each has a different level of security and confidentiality:

---

[3] It is rather like renting as opposed to purchasing infrastructure – this may be the most pragmatic way to get necessary infrastructure for startup companies, etc., that either cannot or do not want to make a huge capital investment.

- **The Public Cloud**– access is available to the general public. In this form, a provider will host data of many users and user groups, with access to each user's data segregated and secured by unique passwords or other identifiers.

- **The Private Cloud** – access is available to and the infrastructure is used solely by a specific organization, which allows exclusive access, pooling of resources and/or eliminating resources as needed. The private Cloud may be hosted by a third-party, but it will be legitimately accessible only by the authorized members of a distinct group (e.g., employees or, perhaps, clients or authorized third-parties).

- **The Hybrid Cloud** –a combination of a public and private Cloud. For example, an organization might utilize a public Cloud for its email and a private Cloud for its more sensitive documents or databases. It may provide for a Cloud with many tenants but with virtualized servers, partitions of the server set off from other users by firewalls, so that no one but the authorized users may gain access.

II. The Cloud and the Law: What Are the Challenges?

An array of Cloud services are available to small law firms. They include availability of software from the Cloud (i.e., GoogleDocs and Microsoft 360), storage and file sharing (such as Carbonite and DropBox,), billing services (such as Rocket), and on-line client relationship management (CRM) applications, which often comprise client contact information, identities of matters pending for those clients, and descriptions of tasks performed if there is billing capability in the application. Some of the benefits offered by these services have already been discussed: remote access, lower hardware costs, and ease of organization.

Yet, the Cloud may not be the answer for all law firms, or all law firm and client documents and data. Before considering a move of some or all of the firm's information to the Cloud, the firm should consider whether it has the capability to manage its information in that environment. Use of the Cloud requires a level of knowledge of and familiarity with mechanics of the providers' systems, and it requires internal organization and discipline within the firm.[4] A law firm considering migration of its information to the Cloud must be prepared to develop and follow internal information policies and procedures for handling client and firm data, and then evaluate the extent to which a particular Cloud service and deployment model, as well as the specific Cloud provider, can help implement those policies. Two key risks/requirements must be investigated before engaging any Cloud provider:[5]

---

[4] See, for example, Comment 8 to Rule 1.1 of the newly amended ABA Model Rules of Professional Conduct, which requires lawyers to "keep abreast" of the "benefits and risks associated with relevant technology" in order to meet their duty to remain competent to represent clients.

[5] Also see another discussion of risk factors in Section III.B below.

1. How secure will be the data hosted with the Cloud provider? Will privilege and confidentiality be maintained in the Cloud provider's servers as well as in transmission to and from those servers?

    a. Security and confidentiality of client information are paramount concerns for attorneys, and they are intertwined. These concerns can be divided into external and internal security issues. Preserving external security requires the provider to implement strong measures to prevent attacks from outside the provider's organization (using, for example, sufficiently robust encryption and other safeguards to prevent unauthorized access to the data).[6] Maintaining internal security requires preparation and implementation, through documented training and compliance monitoring, of policies and procedures for managing electronic information. Does the law firm have a firm understanding of how external and internal security are maintained by a Cloud provider? These questions should be answered affirmatively before the first byte of data is sent to a Cloud provider.

    b. The Cloud can pose new security and confidentiality risks, but it can also enhance safeguards for client and firm data. Moving data over the Internet and storing it with an outside organization with many employees who may have access, or that may be an attractive target for hackers, creates risks of security breaches. On the other hand, most reputable Cloud providers are experts in security and technology, unlike lawyers. Security is a critical aspect of their business models and a core competency of Cloud providers. They can employ security processes and protocols that may be beyond the means of most law firms. Hence the task for individual lawyers and firms, and for those who set the rules for our professional conduct, is to set policies and to act in ways that balance these intertwined factors.

    c. In addition, the more sophisticated Cloud providers may replicate data across multiple servers; storing files in multiple locations or even dividing (replicating) files among several servers in different locations. The low likelihood that all of a provider's servers will fail at the same time or that an unauthorized user could gather all of the pieces of the file without detection may significantly reduce the risk of a data breach.
    Yet, this replication across the servers (and perhaps jurisdictions) can also create potential security and legal risks. More pieces of files in more locations means the pieces may frequently be in transit, through servers where security may be less robust, and over which the Cloud provider may have less control. In addition, data traveling through

[6] These security requirements are, in some cases, mandatory. Firms representing entities covered by HIPAA, for example, must follow certain precepts in the HIPAA Security Rule. Similarly, Payment Card Interchange (PCI") data require strict protections.

certain jurisdictions may come under the control of those jurisdictions' privacy provisions, laws or other regulations regarding security of protected data. Some of these jurisdictions, though, may have laws that protect data more stringently than laws in the U.S. The firm thinking of a particular Cloud provider should carefully balance all these considerations.

d. The onset of Cloud computing does not drastically change the principles governing law firms' risk assessment from those governing paper-based information hosted with a third party, but it does add a degree of complexity. The degree of data control turned over to a Cloud provider and the ubiquity and potential transparency of the Internet create new issues in application of traditional principles. These are yet to be significantly addressed in the courts and legislatures. Nevertheless, current law still provides some guidance for assessment and resolution of legal issues related to Cloud computing. There is a considerable body of law, for example, regarding interactions between a principal and a third party with possession or control over its data (most of which stems from the paper days), as well as potential liability when that third party somehow harms the principal by losing or mishandling that information. Similarly, as discussed in Section III of this Report, there is a plethora of state bar ethical opinions regarding the obligations of law firms with regard to client information in the custody of third parties. In fact, given the lack of reported cases on issues of loss of data in the Cloud and breaches of confidentiality, the state bar opinions are arguably the *only* source of legal guidance in the area, and those opinions have differing standards for use of Cloud services.

e. Ultimately, it is incumbent on the firm considering use of Cloud services to carefully evaluate the security regimens, risks and protections available to it and the commitments of the provider in light of existing legal standards.

2. Can the firm access its data as needed?

Leaving critical data in the hands of a third-party can be a recipe for professional anxiety from ethical, legal and business perspectives. Perhaps the most stomach-churning is the fear of inability to access the when needed at a critical time. When the firm stores information in a remote location, it runs the risk that it may be unable to access data from that location. To successfully access the file, you must (1) have a reliable Internet connection, (2) the remote location (the Cloud) must be up and running, (3) the file must have been properly transmitted to and stored with the Cloud provider. Some of the enumerated concerns are separately mentioned below. These risks are real, and they include:

a. **Internet connection failure**. Access to Cloud services is always through the Internet. There are multiple links in any Internet path between law firm and provider. Also, when one uses wireless devices to access the Cloud, limited coverage areas, signal strength and bandwidth can become a limitation on the ability to access data and files. A failure of any of these connections at a key moment can lead be a major problem, or even a disaster.

b. **Server maintenance or failure**. When the provider's servers are down due to failure or maintenance, the firm cannot access the documents stored in that location. Just like a personal computer or a firm's on-premise servers, these machines can fail or they undergo maintenance, during which time those machines may be disabled. This risk can be mitigated by replication across multiple servers, or backup on the firm's computers, but it is still a factor that must be addressed.

c. **Provider business failure**. Like any other business, Cloud service providers can be bought, sold, or liquidated in bankruptcy. In case of bankruptcy, the Cloud provider may stop maintaining the servers, or secured creditors may claim those servers without considering preservation of data for its owners. This would put the firm in the difficult situation of trying to recover its data from a Cloud provider that does not have any more resources to spend on client services.

These risks, of course, must be mitigated, and there are ways to do so. Relationships between law firms and Cloud services providers are governed by a contract known as the Service Level Agreement (SLA). The small law firm would be well-advised to seek providers whose SLA provisions give the firm comfort that its data will be accessible, either through the service provider's primary servers, or back-up servers, the purchase of which is a critical component of a firm's management. Navigating through these concerns requires an understanding of the available services and how they work, and of the available legal guidance, and suggestions for navigating these waters are set forth in "Suggested Practices" section of this paper. As mentioned above, at the present state of the law, the only readily available legal guidance is the ethical pronouncements of several state bar associations, which are discussed below.

III. The Ethical Risks and Obligations of Using Cloud Services

The issue of whether lawyers are ethically permitted to use cloud services is – to some extent – a ship that has already sailed. As a practical matter, most lawyers already use cloud services on a daily basis. Small law firms and sole practitioners commonly use cloud-based email platforms, such as Hotmail and Gmail, for professional purposes. Even in law firms that have dedicated email servers and systems, individual lawyers frequently email client confidential materials to their personal cloud-based email accounts when they need to work remotely.[1] Alternatively, they access their office desktops through remote applications, such as Citrix. In addition, many clients use cloud-based email accounts to communicate with and send information to their lawyers. Likewise, the use of free Internet-based word processing and calendaring systems, such as Google Docs and Google Calendar, is becoming more prevalent among lawyers and clients alike. Law firms are also starting to use services such as Dropbox or file transfer protocol (FTP) sites to share information with clients or colleagues. As a result, enormous amounts of confidential information are routinely being stored and shuttled around the cloud by lawyers who may not even realize they are using the "cloud. " The challenge for legal ethicists is not to put the genie back in the bottle, but to provide guidelines to lawyers on how to minimize the ethical risks of using the cloud.[2] The first step is to identify what those ethical risks are.

A. The Risks of Using Cloud Services

While cloud computing services offer a wide range of economic and technological advantages, they carry with them a host potential disadvantages. These, in turn, create ethical risks that lawyers must consider and manage before leaping into the cloud. Some of the disadvantages of using the cloud to communicate and store information include:[3]

- **Unauthorized Disclosure of Data Resulting From Security Breaches:** data stored in the cloud with third-party service providers may be more vulnerable to inadvertent or intentional data breaches.[4] This risk is

[1] There are other ethical implications of using email – as distinct from cloud computing – that are beyond the scope of this report. *See* N.H. Op. 2012-13/4 (2012) (noting that using email "presents unique risks and challenges which must be addressed and mitigated separately" from the risks associated with cloud computing). In addition to confidentiality, these ethical risks include "authenticity, integrity misdirection or forwarding, permanence . . . and malware." *Id.* (quoting Penn. Op. 2011-200 (2011)).

[2] Lawyers practicing in 2013 might be surprised to learn that, not long ago, ethics committees were debating the ethics of using cell phones and email. *See, e.g.*, ABA Formal Op. 99-413 (1999) (permitting use of unencrypted email); N.Y. State Bar Ass'n (NYSBA) Op. 709 (1998) (ethics of using email to send confidential information); N.Y. City Bar Ass'n (NYCBA) Op. 1994-11 (1994) (ethics of using "cellular and cordless telephones").

[3] This list is derived, in part, from a list compiled by the ABA Ethics 20/20 Commissions Working Group on the Implications of New Technologies, as well as other sources. For a more in-depth discussion of the risks faced by attorneys using the cloud, see Trope and Hughes*, Contemporary Issues in Cyberlaw: Red Skies in The Morning - Professional Ethics at the Dawn of Cloud Computing*, 38 Wm. Mitchell L. Rev. 111 (2011).

[4] What happened to the Virginia law firm of Puckett & Faraj is a chilling example of this first risk. The two-attorney law firm stored client communications and documents with Google, and that information

compounded if the service provider fails to use appropriate levels of data encryption or employ other best practices for data security. In addition, venders may have inadequate procedures for complying with state and federal laws governing data privacy or notifying customers of security breaches.

- **Other Types of Unauthorized Disclosure:** data breaches are not the only causes of unauthorized disclosure of data. Data may also be disclosed if the service provider has inadequate procedures for responding to (or, when appropriate and permissible, resisting) subpoenas, court orders, or other process seeking production of information;

- **Ownership and Licensing Issues:** vendor contracts may contain unclear or inappropriate provisions about who owns or has the right to use information stored with the cloud service;

- **Temporary Loss of Access to Data:** lawyers may temporarily lose access to information in the cloud for a variety of reasons. The server where the data is stored may experience interruptions in service, Internet connections may be lost, or disputes over payment may lead to temporary denial of access;

- **Permanent Loss of Data:** worse, lawyers may permanently lose access to their data. It is unlikely, though possible, that a cloud provider may fail to adequately back up its data, but permanent data loss is possible if the provider goes out of business;

- **Geographical Risks:** in most cases, lawyers have no control over (or even knowledge of) the geographical location of the servers that store their data. Some of those servers may be located in countries with different legal protections for electronically stored information than in the United States;

- **Problems at Termination:** service providers may have inadequate procedures for preserving, delivering, or deleting data at the end of a service contract. In addition, as noted above, disputes over payment or other contract terms may delay access to data.

---

was compromised when an external attack penetrated the confidential information through theft of the firm's Google passwords. The hacker entity "Anonymous" gained access to 3 gigabytes of emails, amounting to several years of confidential client information, some of which pertained to a pending trial.
http://www.abajournal.com/news/article/unaware_that_anonymous_hacking_group_existed_until_friday_law_firm_partner/

Each of these risks must be assessed in the context of the particular attorney-client relationship, taking into account the nature of the representation, the type of confidential information being handled by the lawyer, and the reasonable expectations of the client with regard to the handling of that information.[5] Thus, the reasonableness of a lawyer's actions in safeguarding confidential information may change, depending on a variety of factors.[6] For example, a law firm that represents institutional clients that are subject to federal privacy regulations, such as HIPAA, GLBA or FCRA, will likely have heightened duties concerning the online storage of client data. Likewise, a law firm that is handling a high profile corporate merger or litigation may need to take additional precautions to protect confidential information online.[7] As discussed further below, ethics opinions have generally concluded that client consent is not necessarily required to use cloud computing. Nevertheless, in many instances, consistent with the ethical standards discussed in Section B, obtaining client consent – or at least giving the client advance notice – may be advisable and appropriate.

B. The Ethical Standards Applicable to Cloud Computing

In light of the risks described above, cloud computing implicates a wide range of ethical obligations. The predominant concern is data security, which implicates a lawyer's ethical duty to safeguard confidential information belonging to clients.[8] Yet, lawyers who use cloud services must also be aware of – and comply with – numerous other ethics obligations. These include:

- The duty to "provide **competent representation** to a client," pursuant to RPC 1.1, which includes the duty to understand the cloud technology and services being used, the duty to obtain client consent – where appropriate – to the use of cloud services, and the duty to counsel the client on their own use of cloud services in connection with the representation;

- The duty to **communicate** with the client about the representation, pursuant to RPC 1.4, which includes the obligations to "promptly" inform the client of "material developments" in the matter, "reasonably consult with the client about the means by which the client's objectives are to be accomplished," and "keep the client reasonably informed about the status of the matter."

---

[5] *See, e.g.*, Cal. Op. 2010-179 (2010) (changing expectations of privacy may increase or diminish steps attorneys must talk to safeguard information sent over wireless networks).

[6] *See* N.H. Op. 2012-13/4 (noting that factors to be considered also include "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients") (quoting Comment [16] to ABA Model Rule 1.6).

[7] *See* RPC 1.6, cmt [17] (noting 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 the precautions a lawyer should take to protect confidential information).

[8] In New York, the duty of confidentiality is governed by Rule 1.6 of the Rules of Professional Conduct (the "RPCs"). Unless otherwise indicated, all references to the RPCs will be to the New York Rules.

- The duty to safeguard client **confidential information**, pursuant to RPC 1.6, which includes the duty to "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client";

- The duty to **maintain and preserve client records and deliver them** promptly upon request, pursuant to RPC 1.15, including records that are maintained in the cloud;

- The duty, upon termination of representation, promptly to **deliver all papers and property** to which the client is entitled, pursuant to RPC 1.16, again, including records maintained in the cloud; and

- The duty to **supervise the work and conduct of nonlawyers**, pursuant to RPC 5.3, including the work of cloud service providers.[9]

These types of ethical issues are not new to law firms that have been outsourcing administrative legal services for decades.[10] Long before cloud computing existed, it was common for law firms to send hundreds or thousands of boxes of confidential materials to outside vendors for photocopying or storage. Subsequently, with the advent of e-discovery, law firms began sending large quantities of electronic data for processing or storage by outside vendors. Outsourcing in this context has rarely been questioned as unethical, nor has it been seriously challenged as a waiver of privilege or confidentiality.[11] Ethics opinions have concluded that lawyers are permitted to outsource, provided they otherwise meet their ethical obligations, including rules concerning competence, confidentiality, and supervision.[12]

In many respects, cloud computing is another method of outsourcing nonlegal support services that were traditionally handled in-house.[13] In fact, it should not be assumed that

---

[9] Cloud computing also implicates the duty to detect and manage conflicts of interest, pursuant to RPCs 1.7, 1.9 and 1.10. Nevertheless, ethics opinions on cloud computing rarely focus on this aspect. At a minimum, conflict rules require cloud providers to take reasonable steps to keep client data segregated and to guard against disclosure to the providers' other customers. As long as reasonable precautions are taken to secure client data, however, cloud providers are probably not required to run conflict checks, nor are they likely to be barred from handling data belonging to an adversary or competitor of a client. In addition, cloud computing implicates the duty to charge reasonable fees and expenses, pursuant to RPC 1.5, including the expense of using an outside vendor. The issue of how to charge clients for the use of cloud computing is beyond the scope of this report.

[10] *See, e.g.*, ABA Formal Op. 08-451 (2008) (discussing the ethical considerations associated with outsourcing); NYCBA Formal Op. 2006-3 (2006) (same).

[11] *See* ABA Formal Op. 08-451 ("There 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.")

[12] *See, e.g.*, ABA Formal Op. 08-451; NYCBA Formal Op. 2006-3.

[13] Jeremy R. Feinberg & Maura R. Grossman, *Introduction to Cloud Computing and Its Ethical Implications – Is There a Silver Lining? (Part I of II)*, NYPRR, May 2010 (posing the question "Is the Cloud So Different From Outsourcing?"); *see also* N.H. Op. 2012-13/4 ("Cloud computing is a form of outsourcing the storage and transmission of data"); Penn. Op. 2011-200 (describing cloud computing

information stored in the cloud is less secure than information stored on law firm servers or in file rooms.[14] Lawyers that have suffered losses after several recent natural disasters, such as Superstorm Sandy, are painfully aware that on-site storage is not foolproof. Nevertheless, for most people, the "cloud" represents innovative and unfamiliar technology. Therefore, as a practical matter, lawyers who avail themselves of cloud services assume a higher burden of establishing that their conduct complies with ethical standards than a law firm that sends its client files to an off-site storage facility.

A number of ethics opinions from around the country have grappled with the ethical issues surrounding the use of cloud services both to communicate with clients and to store client information.[15] All of the ethics opinions conclude that lawyers are ethically

---

as "an online form of outsourcing"); NYSBA Op. 940 (2010) (noting that the principles applicable to cloud computing apply equally to the question of whether attorneys may use off-site backup tapes to store client confidential information).

[14] *See* New Jersey Op. 701 (2006) (recognizing that cloud providers often employ better security that law firms, so information is not necessarily safer when stored on a local server). The same can be said for client files stored in an off-site warehouse or data contained on other technological media, such as laptops, tablets, flash drives, and smart phones. *See* Penn. Op. 2011-200.

[15] To date, the following ethics opinions have been issued concerning various aspects of cloud computing: CT Informal Op. 2013-07 (lawyers may use the cloud to "transmit, store and process data" as long as they "undertake reasonable efforts to prevent unauthorized access to or disclosure of such data"); N.H. Op. 2012-13/4 (lawyer who uses "cloud computing" must take reasonable steps to ensure client information remains confidential); N.C. Formal Ethics Op. 6 (2012) (storage of confidential materials on remote servers is permitted as long as steps are taken to minimize risk of disclosure); Cal. Op. 2010-179 (attorneys using public wireless connections must use reasonable precautions to comply with confidentiality and competence obligations); Iowa Op. 11-01 (2011) (lawyer must take reasonable precautions when using cloud computing services, which may include special security measures if required by client); Or. Op. 2011-188 (2011) (lawyer may use remote servers to store client files, as long as reasonable steps are taken to keep information confidential); Penn. Op. 2011-200 (2011) (client information may be stored in "the cloud" provided reasonable care is taken to ensure materials remain confidential data is protected from breaches, data loss and other risks); NYSBA Op. 842 (2010) (addressing use of online data storage); Al. Op. 2010-02 (2010) (attorneys must exercise reasonable care when using online electronic storage systems); Ariz. Op. 09-04 (2009) (approving use of encrypted online file storage for confidential client information, but noting that what constitutes reasonable precautions to safeguard confidentiality may change over time); Ill. Op. 10-01 (2009) (lawyer may use outside network administrator as long as reasonable efforts are made to protect confidential information); NYSBA Op. 820 (2008) (lawyer may use web-based email services that scan emails to generate computer advertising); Fla. Op. 06-1 (2006) (discussing confidentiality issues associated with electronic filing of client information); Maine Op. 194 (addressing use of remote computer services outside the lawyer's direct control or supervision); N.J. Op. 701 (2006) (lawyer may use outside service provider for storage of electronic documents provided lawyers exercises "reasonable care" to preserve confidentiality); Nev. Op. 33 (2006) (discussing duty of confidentiality with respect to storage of electronic client information on server not exclusively in lawyers' control); Ariz. Op. 05-04 (2005) (permitting electronic storage of client files provided law firms take competent and reasonable steps to ensure confidences are not disclosed); Va. Op. 1818 (2005) (discussing selection of service provider for technical assistance and support for electronic storage); Mass. Op. 05-04 (2005) (discussing use of vendor to maintain law firm's document management application); Vt. Op. 2003-03 (2003) (discussing confidentiality issues raised by use of vendor for database recovery); N.D. Op. 99-03 (1999) (discussing confidentiality issues raised by transmission of data over the Internet and storage or electronic data). In January 2013, a proposed ethics opinion was issued in Florida concerning the use of cloud computing. *See* Fla. Bar Prop. Adv. Op. 12-3 (2013). The ABA has not yet issued an ethics opinion on cloud computing, although in 2010 the ABA Commission on

permitted to use cloud computing, with significant conditions. While the opinions identify issues that attorneys should consider when using the cloud, most are reluctant to offer specific guidelines. This section will summarize the guidance in the existing opinions and then offer practical guidelines for lawyers who use cloud computing.

Competence

RPC 1.1 provides that a "lawyer shall provide competent representation to a client," which requires the "legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." In the context of cloud computing, the duty of competence is the engine that drives all of the other ethical obligations.[16] Competency requires that lawyers take reasonable steps to ensure that information stored in the cloud is properly maintained, organized, kept confidential when required, and accessible when needed.[17] Subject to the standard of reasonable care (as discussed further below), fulfilling the duty of competence may include a range of skills and activities, including:

- Evaluating various aspects of the cloud provider's services, policies and practices;
- Ensuring that any agreements with the cloud provider are consistent with the attorney's ethical obligations;
- Supervising the cloud provider to ensure it is handling client data properly;
- Taking steps to ensure that information stored in the cloud is safeguarded from unauthorized disclosure, is properly backed up, and is accessible to the attorney when needed;
- Ascertaining whether the servers used to store confidential information are located outside the United States and, if so, whether those jurisdictions offer sufficient legal protection and security for data;
- Monitoring the cloud providers policies and practices on an on-going basis; and
- Staying abreast of technological and legal developments that implicate cloud computing.

Technological ignorance does not absolve lawyers of their duty of competence. Ethics opinions agree that lawyers who take advantage of the benefits of various technologies must have a basic understanding of those services and keep up with technological

---

Ethics 20/20 Working Group on the Implications of New Technologies published an "issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology," which addresses the ethical implications of using the cloud.

[16] *See* Cal. Op. 2010-179 (noting that the actions an attorney must take to preserve confidentiality and supervise vendors are "governed by the duty of competence").

[17] *See, e.g.*, Penn. Op. 2011-200 (2011) (duty of competence requires "suitable measures to protect confidential electronic communications and information" and "to reliably access and provide information relevant to a client's case when needed").

changes.[18] This theme is echoed in various revisions that were made to the ABA Model Rules in 2012 to address the developing and increasing use of technology by lawyers and law firms. Based on recommendations by the ABA Commission on Ethics 20/20, amendments were made to Rules 1.1 (competency), 1.4 (communication), 1.6 (confidentiality), and 5.3 (supervision). In addition, extensive commentary was added to these rules making it clear that lawyers must understand the technology they are using, be familiar with the confidentiality and security commitments being made by providers with whom they contract, and stay abreast of technological changes to the extent necessary to protect the security and confidentiality of client information. This duty to stay current with evolving technologies may require the attorney to consult with experts, if the attorney is unable to spend the time and effort necessary to become competent in this area.[19]

Confidentiality:

RPC 1.6 provides that "[a] lawyer shall not knowingly reveal confidential information" and "shall exercise reasonable care to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client." Comment 16 to the rule further provides that a lawyer must "exercise reasonable care to prevent disclosure of information related to the representation by others whose services are utilized in connection with the representation."[20] Disclosure of confidential information is permitted under RPC 1.6 if "the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community."[21]

As with traditional vendors, such as storage facilities or copy services, cloud computing implicates RPC 1.6 in two distinct, but related, ways: first, with respect to the delivery of confidential information to the vendor itself; and second, with respect to the potential disclosure to third parties once the information is outside the attorney's control. Ethics opinions that discuss traditional outsourcing have resolved the first issue in one of two ways. They either view the delivery of confidential information to a vendor as a "disclosure" that is "impliedly authorized to advance the best interests of the clients"[22] or they do not view it as a disclosure of confidential information at all.[23] Regardless of

---

[18] NYSBA Op. 842 (duty to "stay current" with "technological advances applies to a lawyer's contemplated use of an online data storage system"); *see also* N.H. Op. 2012-13/4 ("Competent lawyers must have a basic understanding of the technologies they use" and must "keep abreast of . . . changes"); Al. Op. 2010-02 (lawyers should stay on top of emerging technologies); Ariz. Op. 09-04 (competence is not limited to legal competence, but includes understanding of technology used by the lawyer).

[19] Ariz. Op. 09-04.

[20] New York State courts have adopted only the RPCs and not the comments. Therefore, the comments, while providing helpful guidance on how to interpret the RPCs, are not binding authority.

[21] RPC 1.6(a)(2).

[22] *See, e.g.*, NYSBA Op. 471 (1977) (use of outside agency for accounting of client trust funds is impliedly authorized, as long as lawyer exercises reasonable care to prevent agency from revealing information).

[23] *See, e.g.*, Tx. Op. 572 (2006) (lawyer's use of outside copy service does not constitute "disclosure" as long as lawyer reasonably expects service provider will respect confidentiality of materials). *But see* Ohio Op. 2009-6 (2009) (outsourcing support services, such as photocopying, is not "impliedly

which textual justification is used to address this first issue, however, the more significant concern is the potential disclosure of confidential information to third parties. To resolve that issue, outsourcing opinions state that lawyers must take reasonable steps to ensure that vendors implement safeguards to protect confidential information.[24]

Ethics opinions on cloud computing take a similar analytical approach. Of particular significance to New York lawyers is a 2010 NYSBA opinion concerning the use of an "outside online storage provider to store client confidential information."[25] The opinion concludes that lawyers may ethically use online "cloud" storage systems provided they take "reasonable care to ensure that the system is secure and that client confidentiality is maintained."[26] The opinion notes that exercising "reasonable care" in this context "does not mean the lawyer guarantees that the information is secure from *any* unauthorized access."[27] The opinion lists four steps that a lawyer *may* take in exercising reasonable care:

> 1. "Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information";
>
> 2. "Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances";
>
> 3. "Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored"; and/or
>
> 4. "Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or, for other reasons changes, storage providers."[28]

Emphasizing the rapidly changing nature of technology, the opinion further cautions that lawyers should "periodically reconfirm that the provider's security measures remain

---

authorized" and requires client consent); Cal Op. 1971-25 (1971) (using outside data processing service without client consent violates duty of confidentiality). Even in states that permit the use of outside vendors without consent, however, lawyers must abide by a client's express instruction to the contrary. *See, e.g.*, NYSBA Op. 820, n. 4 (2008) ("*Unless the client otherwise directs*, lawyer may give limited information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, banking, printing, or other legitimate purposes, provide the lawyer exercises due care in the selection of the agency and warns the agency that the information must be kept confidential.) (emphasis added); Tx. Op. 572 (unless the client instructs otherwise, lawyer may deliver confidential materials to outside vendor in furtherance of the representation without express client consent).

[24] In the past, this has generally been accomplished "by some combination of contractual agreement, industry practice, and general custom." Feinberg & Grossman, *supra* note 13.

[25] NYSBA Op. 842.

[26] *Id.*

[27] *Id.*

[28] *Id.*

effective in light of advances in technology."[29] The opinion also states that lawyers should monitor legal developments relating to technology and confidentiality.[30]

The NYSBA approach comports with other ethics opinions around the country. These opinions reflect a general consensus that lawyers are ethically permitted to use cloud computing, as long as they take reasonable precautions to ensure that client information is protected from disclosure. The opinions emphasize that lawyers are not guarantors of cloud computing services.[31] Thus, the applicable standard is reasonable care, not strict liability. A synthesis of the existing ethics opinions indicates that lawyers should consider taking some or all of the following precautions subject to the reasonableness standard:

> Stay on top of emerging technologies to ensure client information is safeguarded.[32]
>
> Research any cloud providers they are considering using to ensure the providers are well established, reputable, and have appropriate policies and practices to ensure that information is secure, properly handled, and backed up.[33]
>
> Take steps to ensure that the vendor and its personnel are competent to perform the tasks required.[34]
>
> Review all contracts and terms of service to ensure they comply with all ethical requirements.[35]
>
> Take steps to ensure that service contracts: (a) require the cloud provider to safeguard client information;[36] (b) have appropriate provisions about the

---

[29] *Id.*; *see also* NYSBA Op. 782 (2004) (stressing importance of staying abreast of technological developments when using technology to communicate with clients).

[30] *Id.*

[31] *See, e.g.*, N.H. Op. 2012-13/4 (rules do not "impose a strict liability standard" on cloud computing); N.C. Op. 6 (duty of confidentiality does not require lawyer to use "infallibly secure methods"); N.J. Op. 701.

[32] *See, e.g.*, Or. Op. 2011-188 ("As technology advances, the third-party vendor's protective measures may become less secure"); Cal. Op. 2010-179 (noting that laws imposing penalties on unauthorized revelation of data may increase expectations of privacy, which in turn increase the ethical obligations of lawyers to safeguard confidential information in various contexts); Ariz. Op. 09-04 (lawyers must keep up to date on technological changes and avoid using security techniques that have become obsolete); N.J. Op. 701 (although standard is reasonable care, the reasonableness of the steps taken is measured against the technology "available at the time to secure data against unintentional disclosure"); *see also* N.C. Op. 6; Al. Op. 2010-02.

[33] *See, e.g.*, N.H. Op. 2012-13/4 (provider should offer "robust security measures," including "password protections . . . data back-up and restoration, a firewall, or encryption," as well as "periodic audits by third parties," and "notification procedures in case of a breach"); N.C. Op. 6 (lawyers should evaluate the vendor's security measures, including "firewalls, encryption techniques, socket security features, and intrusion detection systems" and should evaluate "the extent to which the . . . vendor backs up hosted data); *see also* Penn. Op. 2011-200; Or. Op. 2011-188.

[34] *See, e.g.*, Penn. Op. 2011-200.

[35] N.C. Op. 6.

ownership of data, handling of subpoenas and other legal process, and notification of data breaches; [37] and (c) have appropriate end-of-contract or termination provisions, including the ability to retrieve data regardless of the reason for termination and proper procedures for deleting data from the cloud.[38]

Take steps to determine the geographical location of servers to ensure they are located in jurisdictions with adequate legal protections for data.[39]

Take steps to ensure that data stored in the cloud is accessible when needed, even if the contract is terminated or the vendor goes out of business.[40]

Protect against "end-user" vulnerabilities, such as the failure to use strong passwords or the use of unsecure Internet connections.[41]

Notify clients in the event of a significant data security breach.[42]

The general consensus among ethics opinions is that lawyers are not, as rule, required to obtain client consent to the use of cloud computing.[43] In some circumstances, however, client notification or consent may be required. For example, if the client information is particularly sensitive or if the client is especially averse or suspicious of technology or the Internet, the lawyer may be required to obtain the client's consent.[44] In addition, the less control that lawyer is able to exercise over the cloud provider, the more likely that client consent will be required. By the same token, some information may be so sensitive and important that it should never be stored in the cloud, given the risk – however unlikely – of a massive cyber-attack that no reasonable precautions could avert.[45] Attorneys may, in an abundance of caution, take the safest course and enter into an express agreement with clients about the use of cloud computing.

---

[36] *See, e.g.*, N.H. 2012-13/4; N.C. Op. 6; Penn. Op. 2011-200; Or. Op. 2011-188; Ala. Op. 2010-02; Maine Op. 194; New Jersey Op. 701; Vt. Op. 2003-03.

[37] *See, e.g.*, N.H. 2012-13/4; Penn. Op. 2011-200; Or. Op. 2011-188.

[38] *See, e.g.*, N.H. 2012-13/4; Penn. Op. 2011-200; Or. Op. 2011-188.

[39] *See, e.g.*, N.C. Op. 6; *N.H.* 2012-13/4; Penn. Op. 2011-200.

[40] N.C. Op. 6.

[41] N.C. Op. 6 (passwords); *see also* Cal. Op. 2010-179 (wireless connections); N.D. Op. 99-03 (passwords).

[42] Vt. Op. 2003-03.

[43] *See, e.g.*, N.H. Op. 2012-13/4 (as cloud computing becomes more prevalent it "may be deemed an impliedly authorized disclosure to the provider, so long as the lawyer takes reasonable steps to ensure that the provider . . . has adequate safeguards"); Penn. Op. 2011-200 (use of cloud computing "may be 'impliedly authorized' to handle client data," pursuant to Rule 1.6); Mass. Op. 05-04 (clients have "impliedly authorized" lawyers to provide third-party vendors with access to confidential client data, as long as the lawyers "make reasonable efforts to ensure" the vendor's conduct comports with professional obligations).

[44] *See, e.g.*, N.H. Op. 2012-13/4 (noting that "if the information is highly sensitive, consent of the client to use cloud computing may be necessary); Penn. Op. 2011-200 (consent "may be necessary, depending on the scope of the representation and the sensitivity of the data involved").

[45] *See* Penn. Op. 2011-200

Communication:

Rule 1.4 sets forth the circumstances under which lawyers are required to communicate with their clients. The obligation to communicate includes, *inter alia*, "promptly" informing the client of "any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(j), is required" and explaining "a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." At a minimum, if there is any question as to the level of security required to be implemented in order to protect client confidential information, the lawyer should provide the client with sufficient information regarding the risks and advantages associated with using the cloud and, if appropriate, obtain the client's informed consent.[46] In addition, Rule 1.4 would require the lawyer to promptly notify the client of any security breaches or other developments that compromise the client's confidential information.[47]

Supervision:

Rule 5.3 requires an attorney to make reasonable efforts to supervise the work of nonlawyers that are "associated with" the lawyer. Ethics opinions have extended this supervisory duty to the outsourcing context.[48] As with any form of outsourcing, lawyers who use cloud computing services are responsible for supervising third-party providers, by ensuring that the work is delegated to "competent people and organizations."[49] The duty of supervision also requires lawyers to take reasonable steps to ensure that the cloud provider is able "to limit authorized access to the data to only necessary personnel" and ensure the information "is backed up, reasonably available to the attorney, and reasonably safe from unauthorized intrusion."[50] Lawyers must also take reasonable steps to ensure that "the vendor understands, embraces, and is obligated to conform to the professional responsibilities required of lawyers."[51]

Safekeeping of Client Property:

RPC 1.15 sets forth numerous obligations relating to the handling, retention and delivery of client property, which generally includes files, information and documents, including electronic data.[52] In addition, RPC 1.16 requires that lawyers must, at the end of the representation, promptly deliver all property "to which the client is entitled." As a

---

[46] *See id.*
[47] *See* Vt. Op. 2003-03.
[48] *See, e.g.*, ABA Formal Op. 08-451; NYCBA Formal Op. 2006-3.
[49] Penn. Op. 2011-200; *see also* N.H. Op. 2012-13/4.
[50] Penn. Op. 2011-200.
[51] *Id.*; *see also* Vt. Op. 2003-03 (lawyer may fulfill duty to supervise by obtaining "written acknowledgement" from vendor concerning the obligation to keep the information "in the strictest confidence").
[52] *See* Penn. Op. 2010-200.

general rule, lawyers are permitted to use electronic means to preserve client documents, except for documents that are required by rule to be maintained in original form.[53]

Any use of cloud computing must comply with the obligations, under RPC 1.15, to safeguard client property. Thus, lawyers must take "reasonable precautions to ensure that electronic data stored in the cloud is secure and available while representing client."[54] In addition, the "data must be returned to the client and deleted from the cloud after representation is concluded or when the lawyer decides to no longer preserve the file."[55] Agreements with cloud providers must state that the customer – not the provider – owns the data. Otherwise, the lawyer "may run afoul of Rule 1.15, which requires that the client's property 'be identified as property of the client."[56] Most of the precautions discussed above in connection with safeguarding confidentiality and RPC 1.6 will also encourage compliance with RPC 1.15.[57]

C. Suggested Guidelines

For now, and perhaps well into the foreseeable future, the ethical opinions contain very few instructions on what answers are sufficient to meet ethical requirements and/or avoid malpractice liability. Accordingly, attorneys are left on their own to answer the practical question: What steps are enough to be "reasonable," to not leave themselves exposed to sanctions by using cloud services? The uncertainty this creates is exacerbated by the reality that the issue will only become significant *after the fact*, when a breach has occurred or data access is lost at a critical moment. With classic 20/20 hindsight, a distraught client will be combing every detail of the attorney's practices to find the one thing that he or she didn't do.

Below are several guidelines that will help practitioners comply with their ethical obligations. These are by no means requirements, but adopting some or all of them can be very helpful in building a strong case that your use of the cloud complies with the reasonableness standard.

Suggested Guideline 1 – Only Use Reliable Providers

> *Only use reliable providers and, even with well-established providers, keep up to date on their business condition and prospects.*

---

[53] *See* NYSBA Op. 680 (1996) (client file may be stored electronically except for documents required to be in original form, provided lawyer ensure that documents cannot be inadvertently destroyed and can be readily produced when needed); *see also* Fla. Op. 06-1 (2006) (lawyers may store files electronically unless required by law to retain original document).

[54] N.H. Op. 2012-13/4.

[55] *Id.*

[56] *Id.*

[57] *See, e.g.*, Penn. Op. 2010-200 (service agreements should contain appropriate provisions about ownership of data to ensure compliance with RPC 1.15); Or. Op. 2011-188 (In light of duty to preserve client data, under RPC 1.15, client data should be properly backed up so that any data that is lost, corrupted or deleted can be restored).

One reason many prefer to proceed slowly in adopting Cloud computing services is the nascent state of some aspects of the industry.[7] The typical market cycle for technological innovations certainly applies to the cloud environment as much as to any other new technology. When it is new and "HOT," a multitude of players enter the market. The offerings have varied degrees of sophistication and quality, and the players themselves vary from large, well-established providers to smaller startups. As the market matures, many of the weaker entrants fall by the wayside, either because a stronger participant provides something better (or commits more marketing dollars to gain acceptance) or because the smaller entrants simply don't have the capital to sustain themselves until profitability. Because Cloud computing is currently in a relatively early phase of this cycle, prospective users must be very careful in choosing providers, since some may not be around for the long haul.

Keep informed, too, of your provider's plans for the future. Be aware in advance if they are deciding to drop the Cloud services segment of their business, and monitor their website periodically for updates to their Privacy and Acceptable Use policies, terms of service, and service changes.

Suggested Guideline 2 – Document Due Diligence

> *Spend time performing due diligence on a proposed provider and its contract (Service Level Agreement, or "SLA") and document the process, including your review, any negotiations with the provider and the reasons why you concluded that your client's information is going to be secure.*

For example, if you conclude that a provider has given adequate assurance that it will notify you when it receives a subpoena for disclosure of information, write down what led you to that conclusion, such as "SLA and/or Provider's website expressly states that it will not turn over information until 15 days after it gives me formal notice of the request."

Due diligence should include all of the risk factors discussed in Sections II and III above, especially security protections such as intrusion-detection systems, firewalls, passwords, back-up procedures, etc., as well as the provider's business, especially its financial condition, reliability, and ability to meet its ongoing commitments. Investigate your own systems, too. Verify, for example, that your office has information management protocols that include technical safeguards (password policies, etc.), and that your equipment and software are capable of sending encrypted transmissions.

In this regard, attorneys should request copies of the prospective provider's certifications from one of the agencies that independently audit the security practices of Cloud providers. Internationally recognized standards used by these auditors include SSAE-16 (Statement on Standards for Attestation Engagements, the successor to SAS 70, Statement No, 70 of the Statement on Auditing Standards, Service Organizations), and SOC3, SysTrust/Webtrust. An attorney using providers who demonstrate having received one of these certifications would probably be held, in a dispute, to have exercised reasonable care in assessing the provider's security regime.

---

[7] As the late Professor Gary Munneke (formerly Chair of the NYSBA Law Practice Management section) points out, the Internet is not new; neither is downloading content from it new. Cloud computing deserves relatively greater care because of the rate of innovation, the newness of remote application offerings, and the number of companies, small and large, rushing to provide new services or latest "app."

Suggested Guideline 3 - Read the Contract, then Decide Your Risk Tolerance

> *Never just click "Agree" to a provider's "Terms and Conditions of Use." Obtain, and review, the complete Service Level Agreement and all Addenda and Attachments. Read all website information referenced in links in the SLA.*

Almost universally, the standard contracts (the "Terms and Conditions of Use") utilized by cloud providers disclaim all liability if anything goes wrong. Sometimes, these limitations can be negotiated, but often they cannot.

Compare, for example, the requirements discussed above to have unfettered access to client data with the following term in a user license from a provider of online billing and document management services for lawyers:

> [Provider] reserves the right to temporarily suspend access to the Service for operational purposes, including, but not limited to, maintenance, repairs or installation of upgrades, and will endeavor to provide reasonable notice prior to any such suspension.

It is also insightful to learn that the provider is a Canadian company and that the laws of British Columbia govern the contract. Nothing in the contract acknowledges any duty to comply with U.S. state or federal privacy laws. It says nothing at all about the attorney retaining ownership of content uploaded to the site. Finally, in the area of protecting data from hackers, the contract states:

> You acknowledge and agree that the technical processing and transmission of data associated with the Service, ***including Content, may be transmitted unencrypted*** and involve: (a) transmissions over various networks; and (b) changes to conform and adapt to technical requirements of connecting networks or devices. [emphasis added]

Also, be careful of "Changes in Terms" clauses. Many online terms and conditions include a provision allowing the provider to change the terms without affirmative notice to subscribers and deeming the new terms accepted by use of the service after the undisclosed change. Some such provisions could sound the death-knell for your use of this provider, if you are relying on contract terms for comfort in using a particular service.

Until this imbalance of bargaining position changes, you must determine what other assurances will be enough to be considered "reasonable" when you probably can never collect damages in the event of a failure. [Consider ending the sentence after "reasonable" to keep the focus on compliance with duty and safeguards against injury to clients (rather than mitigation of financial risk to counsel).]

Suggested Guideline 4 – Key Contractual Terms

> *Get promises from a prospective Cloud Provider, in the SLA, that it will meet your key requirements, and check the Provider's track record of meeting them with reliable references.*

As with all of these Suggested Guidelines, it is unlikely that an attorney will find a Cloud Provider whose SLA provides for each of the following contractual obligations, nor would that be necessary. Instead what follows is a list of key contractual terms that

were gleaned from the Subcommittee's review of the outstanding ethics opinions.[8] When reviewing a potential provider's SLA, an attorney should be on the lookout for the following commitments:

1. **Ownership of Data.** To preserve and keep segregated from all other tenants your confidential information, and a statement that you own the intellectual property rights in your data; the best commitment is acknowledgement of your legal and beneficial ownership of all content you upload to a provider's system. It's also absolutely imperative that you avoid a vendor that claims ownership rights to the information you post in the cloud.

2. **Frequent Back-ups.** To back up your data at least weekly to a different location from its main storage facility (daily if you have significant, time sensitive documents).

3. **Data Storage Location.** Consider whether a clause limiting storage of data to servers within the United States is in the best interests of your firm and/or your clients. Without it, you'll have to address the multitude of foreign laws on government access, consumer privacy rights, etc., and enforcement of your rights will be much more difficult. Also, some state regulators require their licensees to keep all customer data in that state. If your client is one of those licensees, you will be subject to the same regulations when you're holding their property.[9] Yet, in certain circumstances, and for certain multinational clients, storage of data outside the U.S. may be beneficial, given more stringent privacy, security and data protection laws in countries in which the provider has servers and the business locations of the particular client.

4. **Unfettered Access.** To provide you with unfettered access to client data (or critical cloud software) on a 24/7 basis as practicable (i.e., sometimes the system must go down for routine maintenance), to have a process for you to retrieve said data using easily accessible software or other media upon termination of the relationship, and to ensure that the data will be destroyed in a non-recoverable manner when you so request.[10]

5. **State-of-the-Art Security.** To have the most up-to-date security practices (electronic and physical), including encryption, firewalls, locked facilities, redundant storage, etc., and a commitment to respond to technological changes.

---

[8] See appendix, *supra,* for examples of contractual terms that may raise questions, as taken from Terms and Conditions of services offered by Microsoft, Google and Apple

[9] On this point, attorneys must remember that many Cloud providers don't store data on servers they own and data is rarely stored on only one server.

[10] Ability to use the data once it is retrieved is most critical when an attorney subscribes to Software as a Service, such as online word processing or document management. Since the software that allows the data to be manipulated is housed at the provider, the attorney must know that compatible software is available to continue using the data once it is retrieved from the provider.

6. **Timely Breach Notice.** To timely notify you of any actual or suspected security breaches, and to have "adequate" procedures to address any breach and protect against further fallout.

7. **Timely Subpoena Notice.** To notify you in a timely fashion, as permitted by applicable law, of any governmental or third party requests for access to information sufficiently ahead of disclosing the information in order for you to react and resist disclosure if in the best interests of a client.

8. **Access Without Internet Connection.** Ideally, you should have access to the cloud any time you need it, and an Internet connection should not be a limiting factor. A potential solution would be finding a vendor who offers synchronization and storage of the cloud data to your device, or gives you the option of backing up your data automatically or manually to your local device.

9. **Meaningful Support.** You are willing to try something new, and vendors should be sensitive to that fact. Look for vendors who offer support, training videos, and who have an online knowledge base. Again, your investment is more than just the subscription payment; it's also the time you invest in familiarizing yourself with the service

Suggested Guideline 5 - Get Client Consent

Obtain your clients' consent before storing their information in the cloud or relying on cloud-based software for client-critical functions.

No matter how careful an attorney is, no system of storing confidential information (cloud-based or otherwise) is foolproof. That is why the standard for using cloud computing is "reasonable care," not strict liability. Although express client consent to cloud computing is not necessarily required under the RPCs, lawyers may wish to consider inserting into their engagement letters a provision granting the client's consent to use of the cloud.

In addition, lawyers should consider discussing with the client whether certain information entrusted to the attorney is particularly sensitive and, therefore, needs a higher level of protection than the rest of the client's information. For example, even if a client would generally have no objection to the attorney storing encrypted client documents in the cloud, the client might object to storing its recent unpublished financial statements in the cloud during the quiet period leading up to an IPO. Under circumstances where the client's consent is required to store information on the cloud, as discussed in Section III.B above, lawyers should not do so before obtaining client consent in writing.

Suggested Guideline 6 - Understand the Technology

Be sure you know the technology or engage an expert to assist you.

Most lawyers are not tech gurus who spend their days keeping up to date on the latest Internet security practices, though courts are far less inclined to accept an excuse similar to "Judge, I just don't understand this computer stuff." As mentioned above, the opinions are replete with cautions for an attorney who is not able to understand (in detail) and keep abreast of technologies and trends. That attorney must engage expert help, and

not rely on the provider to say "oh yeah, we'll make sure you're ok." In the terms of the NYSBA opinion above, how is it reasonable to "[i]nvestigat[e] the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances" if you don't know what technology is adequate?

Suggested Guideline 7 – Keep Data Encrypted

Client and firm data housed with a Cloud provider should be encrypted in transit from your firm to the provider and back again, and at the provider's locations. The provider should not possess the encryption key unless there is a compelling reason for it to have the key. Encryption is the process of transforming information so that it is unreadable to those who don't have a key that can decrypt it or make it readable again. Whenever you use Cloud computing, your data can reside in three places. Your files can reside on your computer hard-drive, they can be in transit to the cloud, or they can reside on the Cloud service provider's servers. Make sure your data is encrypted in all three situations, to the extent practical. Use encryption applications to encrypt your computer hard-drive, and portable media such as USB drives, laptops, tablets and smartphones. This will ensure that those who can remove your hard-drive cannot read the data using another device. You should also set a password to your computer user account. This way, those who get to your computer cannot read the data on the hard-drive using your computer.

Suggested Guideline 8 – Establish Data Management Policies and Procedures

More than one ethics opinion has stressed that picking the right provider is not enough. It is imperative to sensitize all staff (professional and non-professional) to the importance of maintaining security (such as protecting the privacy of passwords, avoiding unsecure networks to access the cloud, etc.) and to the operation of the online service so that data entry and manipulation is conducted in the manner necessary for the provider to fulfill its part of the protection regimen. For example, some sites offer postings of both private and public information. If particular coding by the attorney is needed to keep the information in the private area, all staff of the firm must know this and know how to enter the codes. Documented electronic information policies and procedures, and documented training of the work force on those protocols, is strongly recommended. It is important to remember that few states or courts require perfection, but most, if not all, require reasonable steps and due diligence in safeguards for client information. Those steps and diligence would be difficult to prove without appropriate documentation.

IV. Conclusion – Go Forth, with Care

Lawyers have a wide variety of choices in Cloud services, and these will expand as Internet access gains nationwide reach and portable devices to access those services become cheaper, more durable and more secure. Lawyers will be able to access their documents and office data from anywhere, courtrooms, client sites, airports and hotels, as though they were sitting at their offices. As the practice of law becomes more mobile and virtual, such remote access to documents, data and applications will be almost mandatory. We return, then to the question posed at the outset of this Paper: the issue is not whether to proceed (economics and clients demand that we must), but how to do so safely and within the bounds of the lawyers' ethical obligations and regulatory requirements.

Outages can happen to even the largest cloud providers, such as the GoDaddy.com outage in September 2012 or Amazon's outage in April of 2011 when it took three days for its systems to be fully restored. Consider the malpractice exposure of relying on Amazon to store data, without backup on other media, if a client's brief was due on day two of that outage. Also, several of the Cloud software providers are not major, well-financed entities with reliable histories. There is a risk that some of these providers may fail in the current economic climate.

At the other end of the spectrum, however, is the value of having data stored remotely and accessible from anywhere when major disasters drive a lawyer from his or her office or destroy the firm's equipment. This was made starkly clear by 2012's Hurricane Sandy, when nearly all the law offices in lower Manhattan and much of coastal New Jersey were without power and, in many cases, uninhabitable for extended periods.

It would be helpful for pioneering courts to render decisions that provide guidance and clarity to the due diligence standards required of attorneys who utilize Cloud services. Also, as the industry matures, many vendors will likely adopt the practices and contract terms required to assist attorney-customers in meeting their applicable standards of care. The risks we have noted should lessen after the industry goes through its shakeout phase, so attorneys can be more confident that enough providers will have the commitment and wherewithal to stay in the market for the long term.

However, unlike most other prospective users of Cloud-computing services, lawyers are cloaked with a heightened duty to protect confidential client information. In addition, in most states, all information received from a client is presumed to be confidential until it is proven to be otherwise. Also, lawyers are not permitted to contractually limit their potential malpractice liability, so their risks can be much higher than the risks of other users who possess confidential information of their clients or customers.

Therefore, until clarification is provided by courts and state bar associations, and the provider landscape improves with regard to the requirements of those who work with sensitive or otherwise protected information, it is advisable that counsel exercise great caution to select only those vendors whose terms and practices most closely meet their specialized needs and those of their clients. [11]

The authors of this report certainly would prefer to give a definitive answer to the question: "Should I use the Cloud?" However, the answer is an ultimately personal one. The authors recommend that each lawyer analyze his or her own decision matrix, balancing costs versus benefits, and risks versus rewards. Each lawyer will have a different view of the competing risks of hackers and provider outages, on the one hand, and convenience of access and protection from natural or other 'local' disasters, on the

[11] To be clear, the ethical risks discussed in this article are limited to two critically important functions: storing client data where it might be accessed by the wrong parties or might be inaccessible by the attorney when needed; and exclusive reliance on software or other critical functions not housed under a lawyer's direct control. Cloud services may be well suited to functions like internal practice management (such as sharing calendars over the web) or proprietary client-communication platforms (such as an extranet where client and attorney can share files – as long as other copies are kept instantly available). Cloud services can be a valuable addition to streamlining the management of many types of data; but lawyers must be diligent and selective in what data is placed in the Cloud and which provider they select. Lawyers cannot blindly believe any hyperbole claiming, "it's easy." Time and caution must be invested to have comfort that they use the Cloud in a way that meets their professional responsibilities.

other. The one constant, however, is that a decision must be made thoughtfully, and the lawyer must be prepared to demonstrate to clients, regulators and, perhaps at some point, a court how the decision was reached and what factors went into it.