ALFA International
The Global Legal Network
Local Relationships Worldwide

2015 INTERNATIONAL CLIENT SEMINAR

FAIRMONT SCOTTSDALE PRINCESS

SCOTTSDALE, ARIZONA

MARCH 5 – 8, 2015

Client Confidentiality in the Cloud

Patrick Michael
DINSMORE & SHOHL LLP
Louisville, Kentucky
(502)581-8022
patrick.michael@dinsmore.com

William G. Ireland
HAIGHT, BROWN AND BONESTEEL, LLP
Los Angeles, California
(213)542-8035
wireland@hbblaw.com

Barbara Stevens
Vice President & Corporate Counsel
PRUDENTIAL
New York, New York
www.prudential.com

James C. Green
VP, General Counsel & Secretary
MANITOU AMERICAS, INC.
West Bend, Wisconsin
www.us.manitou.com

John Ruzich
Senior Vice President & General Counsel
LEGENDS
New York, New York
www.legends.net

Client Confidentiality in the Cloud

Cloud Computing and Professional Ethics: Making the Cloud Work for You[1]

I. The Cloud

Like most technological innovations, the cloud seemingly appeared out of nowhere one day and immediately established itself as a household name. Before anyone could so much as blink, the multinational technology giants Apple, Microsoft, Google and even Amazon had already integrated the cloud into their Smartphone and Tablet platforms. As a result, most Smartphone and Tablet users in the U.S., groups that represent approximately 58% and 42% of U.S. adults, respectively[2], are familiar on some level with the basic concept of the cloud. To most people, the cloud is where their data, pictures, messages, and phone numbers are backed up; it's what saves them when their device crashes. But what exactly is this ethereal cloud?

A. What is the Cloud?

In the mid 1990's, the term cloud was used generally as a metaphor for the Internet.[3] As the Internet became less a creature of abstract fantasy and more widely understood,

---

[1] Article prepared by Patrick Michael and Justin Brown, Dinsmore & Shohl LLP, Louisville, Kentucky.

[2] Pew Research Center, http://www.pewInternet.org/fact-sheets/mobile-technology-fact-sheet (last visited Dec. 5, 2014)

[3] David A. Couillard, Note, *Defogging the Cloud*: Applying Fourth Amendment Principles to Evolving Privacy Expectations in *Cloud Computing*, 93 MINN. L. REV. 2205, 2216 (2009); Dennis Kennedy, *Working in the Cloud*, ABAJOURNAL.COM (last visited Nov 29, 2014), http://www.abajournal.com/magazine/article/working_in_the_clouds/

the cloud began to take on a more refined meaning. By 2006, the cloud was no longer just a synonym for the Internet; instead, the cloud had come to mean a large, interconnected network of servers which allows users to access data stored on the server from anywhere that they can connect to the Internet.[4] In its simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of from your computer's hard drive.

Figure 1. A row of secured, air-cooled Cloud servers.

Within a few years, the National Institute of Standards and Technology ("NIST") developed the first working definition for cloud computing[5]. The NIST defines cloud computing as "a model for enabling convenient, on-demand network access to a shared

[4] *Id.*

[5] The terms Cloud and Cloud Computing are used interchangeably.

pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released."[6]

B. How Does the Cloud Work?

Cloud computing service falls into one of three distinct categories: Infrastructure-as-a-Service ("IaaS"), Platform-as-a-Service ("PaaS"), and Software-as-a-Service ("SaaS").[7] The IaaS provides companies with computing resources, including servers, storage, and data center space on a pay-per-use basis.[8] The PaaS provides a cloud-based environment with everything required to support the complete life cycle of cloud applications without the complexity of buying and managing the underlying hardware, software, provisioning and hosting.[9]

However, the cloud service model that is probably most familiar to the average attorney is SaaS. In Saas, the user operates cloud-based applications on remote computers that are owned and operated by others and that connect to users' computers via the Internet.[10] SaaS programs are so widely used today that many attorneys probably

[6] Peter Mell & Timothy Gance, National Institute of Standards and Technology Special Publication 800-145, The NIST Definition of Cloud Computing (2011).

[7] *What is Cloud Computing?*, IBM http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html.

[8] *Id.*

[9] *Id.*

[10] *Id.*

utilize them without realizing it. Google's Gmail, Yahoo! Mail, Dropbox, Google Drive, Box.net, and iCloud are all well-known examples of SaaS.[11]

Using Dropbox as an example, the following illustrates how SaaS operates. The process begins when the user moves a file or files into the Dropbox by 'dragging and dropping' them into the Dropbox folder. All of the data that comprises that file is then encrypted and stored on Amazon's Simple Storage Service in multiple data centers across the United States. When users wish to view the files, they can either access their Dropbox account from any web-connected computer or they can load the Dropbox program onto their netbook, tablet, or Smartphone. Utilizing the loaded software allows the user to access the latest version of any given file and to make any changes to the file that they want.

In addition to the three different platforms of cloud computing services, there are four different mechanisms by which these computing services are deployed. First, there are public clouds, which are operated by third-party providers and made available to the general public or a large industry group.[12] Next, there are private clouds, which are operated by companies that have the funds available to invest in off-site or on-site servers to serve their own personnel.[13] Third, there are community clouds, which are located on-premise or off-premise, managed by the participating organizations or a third party, shared by participating organizations, and used to support a specific community

[11] Chuck Tesla, *The Explosive Growth of Cloud Computing*, Tumotech (April 21, 2014) http://www.tumotech.com/2014/04/21/what-you-need-to-know-about-the-explosive-growth-of-cloud-computing/.

[12] Gathering Clouds: The Takeover Talks Between IBM and Sun Highlight a Shift in the Industry, The Economist, (Mar. 19, 2009) http://www.economist.com/node/13331334

[13] *Id.*

that shares certain objectives.[14] Last, there are hybrid clouds. These clouds are composed of two or more clouds (private, public, or community), each of which remains a separate entity, which are linked by shared standards or shared proprietary technology that enhances the portability and movement of data and applications.[15]

II. What are the Advantages and Disadvantages of the Cloud?

A. Advantages

Attorneys often take for granted that they can, at any time, simply travel to their office to work. While this is almost always true, inclement weather, natural disasters, and even acts of terrorism, such as those seen in New York and Boston, can shut down cities and highways, bringing travel to a complete standstill. Those attorneys with paper-based practices or whose servers are stored inter-office would likely be unable to provide services to their clients during this time. However, firms that utilize the cloud would remain able to access their data and continue with business as usual.

There are many benefits to transitioning to a cloud computing solution for a law firm's client and office data. Four of those benefits are articulated below.

[14] *Id.*

[15] *Id.*

1. Efficiency and Convenience

Traditionally, law firms have just purchased computers, servers, and software, and have hired an IT professional or professionals to manage everything. Not only is this expensive, but it is likely that there are not many electronic security measures in place. Moving information to the cloud can allow the law firm to lower its expenses, enjoy better service, and be better protected. In addition to costs savings, law firm data will be more physically secure in the cloud than in the office. Cloud providers often go to great lengths to ensure that their servers are physically protected against the elements, fires, electrical shorts, and even intrusions by would be thieves.

Additionally, cloud service is more efficient than IT service is in regards to problem resolution. Often with in-house problems, an attorney must wait for the IT professional to come to his/her office, which can be not only time-consuming, but intrusive. With a problem on the cloud, the provider can simply access the system and begin troubleshooting the problem remotely. Also, when it is time to update or install new software, the provider can do so without the need of any involvement by the attorney or the firm.

2. Increased Data and Analytics and Better Management

The cloud also gives an attorney or a firm access to better information regarding the efficiency of how the firm operates. “Utilizing cloud architecture and services can allow the firm to efficiently collect data about its practice and its staff, enabling the firm to better devise ways to increase its productivity and profits. For instance, a cloud-based practice can more easily and accurately track and analyze metrics such as utilization of

software applications and platforms and an attorney's time. These metrics can, in turn, be used to make firm-wide overhead decisions such as staffing, and whether or not to offer alternative billing for certain tasks."[16]

3. Disaster Readiness and Recovery

Disasters, whether natural or man-made, can not only bring work to a standstill, but can result in the destruction of a firm's office, including all physical files. Using the cloud can minimize, and even prevent, the risks of a natural disaster having a negative impact on a law firm because files saved in the cloud are physically stored in a location different from the firm. Additionally, the backed-up files are typically duplicated or stored on more than one server. Cloud providers tend to have multiple server sites in several geographic regions, which helps ensure the safety of data in the event of a natural or even a regional disaster.

4. Flexibility

Today, it is more necessary than ever for an attorney to be able to work outside of the office. "An attorney's ability to review documents on the road and to retrieve information while in court or at a client meeting is an important aspect of running a profitable practice. With a cloud-based system, all of a firm's data is saved, cataloged, and indexed in a centralized location that is remotely accessible to the attorney." [17] This gives the attorney the flexibility to work from home, on a trip, while traveling, and even from the courthouse.

---

[16] Kenneth N Rashbaum, et al, Five Reasons to Consider Moving Law Firm Data to the Cloud, Logicworks, http://www.logicworks.net/blog/2014/06/five-reasons-consider-moving-law-firm-data-cloud/.

[17] *Id.*

B. Disadvantages

While the cloud does offer numerous advantages to attorneys and law firms, like any technology, it comes with its own set of problems and concerns. Consider the following four problems.

1. Security

Because we are beyond the time when all files can be physically secured under lock and key, security has taken on a new meaning. Instead of locks and file cabinets, we now have firewalls and 256-bit encryption. Burglars are now called hackers. These hackers, such as the group *Anonymous*, have managed to infiltrate some of the largest and most well equipped cloud providers, including Dropbox, Apple and Amazon. However, it is the interconnectedness of the cloud that poses the greatest risk. Once a hacker gains access to the cloud servers, they can navigate their way through the interconnected systems, accessing more information than they could on a private server.

An additional security risk is that posed by the cloud employees themselves. Any cloud employee who has access to the data can essentially steal that data at any time. In addition to the risks posed to a client's interests, this can also destroy confidentiality.

2. Internet Connection Failure

By virtue of being a server based service, access to the cloud will always be through the Internet. Whether because of loss of power or maintenance by the Internet Service Provider, if the network connection is down, then the cloud is down. This forces the

attorney to either wait for the connection to return, or to relocate to find a suitable alternative Internet source.

3. Server Maintenance or Failure

On some occasions, it will not be the Internet connection that is down, but the cloud servers themselves. During this time, the attorney will be entirely unable to access client documents on the cloud. Unless the provider has built in a workaround such that the data stored on the failed servers is accessible through another server, there is nothing the attorney can do but wait. This places the attorney in a precarious position, especially if he or she is preparing for trial, making time sensitive court filings, or in the middle of mediation and attempting to access documents.

4. Provider Business Failure

Cloud service providers can be bought, sold, dissolved, 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."[18]

[18] Ashwini Jayaratnam, et al., T*he Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations, Committee on Small Law Firms*, New York Bar Association (November 2013). http://*nylawblog.typepad.com/files/nyc-bar-report.pdf.*

III. An Examination of State Bar Ethics Committees Opinions on Cloud Computing.

Some law firms find that the advantages of cloud computing outweigh the disadvantages. As a result, they have abandoned their traditional data storage solutions in favor of the Cloud. Because cloud computing places client data on remote servers outside of the lawyer's direct control, it has given rise to some concerns regarding its acceptability under applicable ethics rules. This has catalyzed a response from nineteen State Bar Associations in the form of Ethics Opinions.[19]

The opinions universally adopt "reasonable care" as the standard for attorneys looking to store data in the cloud. Unfortunately, it is ultimately impossible to find substantive guidelines on what constitutes reasonable care. Even where some guidelines do exist, they vary by jurisdiction. This is likely attributable to the rapidly changing nature of technology and the needs of attorneys in that jurisdiction.

In order to insure a geographically diverse representation, this paper examines opinions from California, Iowa, New York, Pennsylvania, Massachusetts, and North Carolina.

A. California – Reasonable Care

The State Bar of California's Standing Committee on Professional Responsibility and Conduct issued an opinion in December of 2010 that "sets forth the general analysis

[19] To date, the following state's State Bar Associations have rendered ethics opinions on cloud computing: Alabama, Arizona, California, Connecticut, Florida, Iowa, Maine, Massachusetts, New Hampshire, New Jersey, New York, Nevada, North Carolina, Ohio, Oregon, Pennsylvania, Vermont, Virginia and Washington.

that an attorney should undertake when considering use of a particular form of technology."[20]

The Committee stated that "transmission of information through a third party reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information," but that the "manner in which an attorney acts to safeguard confidential information is governed by the duty of competence."[21] On the issue of competence, the Committee declared: "the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney's handling of such information does not result in a waiver of any privileges or protections."[22]

Before using a given type of technology, the Committee suggested that an attorney should consider the following factors:

1. The nature of the technology in relation to more traditional counterparts (i.e. e-mail versus mail);
2. Reasonable precautions possible to improve the security of a given technology;
3. Limitations on who can monitor the use of technology and disclose activity;
4. The lawyer's own level of technological competence, and whether it's necessary to consult with an expert;
5. Legal ramifications to third parties for intercepting or otherwise interfering with electronic information;

[20] State Bar of California's Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179.

[21] *Id.*

[22] *Id.*

6. The sensitivity of the data;

7. Impact of possible disclosure on the client;

8. Urgency of the situation; and

9. Client instructions.[23]

In conclusion, the Committee said "An attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential client information to an undue risk of unauthorized disclosure."[24]

B. Iowa – Due Diligence

On September 9, 2011, The Iowa State Bar Association's Ethics Committee issued an opinion on whether a lawyer or law firm may use cloud computing, with particular emphasis on SaaS. The Committee stated: "We believe the Rule establishes a reasonable and flexible approach to guide a lawyer's use of ever-changing technology. It recognizes that the degree of protection to be afforded client information varies with the client, matter and information involved. But it places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly."[25]

[23] *Id.*

[24] *Id.*

[25] The Iowa State Bar Association, Committee on Ethics and Practice Guidelines, Ethics Opinion 11-01 Use of Software as a Service – Cloud Computing.

The opinion goes on to provide that lawyers who wish to utilize the cloud "must ensure that there is unfettered access to the data when it is needed."[26] The onus is on the lawyer to "determine the nature and degree of protection that will be afforded the data while residing elsewhere."[27]

In order to perform their due diligence, the opinion states that lawyers should inquire about:

1. The reputation of the provider;
2. The physical location of their cloud servers;
3. Their ability to remove data from the service;
4. What type of password protection is used, who has access to data; and
5. How is the data encrypted?[28]

The opinion goes on to acknowledge the inherent difficulty in performing due diligence, especially considering that it must be performed by individuals who have the "requisite technology expertise and as well as an understanding of the Iowa Rules of Professional Conduct."[29] However, the opinion concludes that lawyers may discharge their ethical duties "by relying on the due diligence services of independent companies, bar associations or other similar organizations or through its own qualified employees."[30]

---

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

C. New York – Four Factor Approach

The New York State Bar Association's Committee on Professional Ethics published an opinion outlining the ethical considerations for attorneys who hire third-party providers to electronically store client files.[31] The Committee concluded that, "just as an attorney may hire a third party to store hard-copies of client files, so too may an attorney use an online storage system, provided the attorney exercises *reasonable care* to ensure that confidential information will remain secure."[32] The Committee pointed out that "the exercise of reasonable care may differ from one case to the next."[33]

The Committee concluded that a lawyer may use a cloud computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained. Reasonable care may include consideration of the following steps:

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

---

[31] N.Y. State Bar Assoc. Comm. on Prof'l Ethics, Opinion No. 842 (2010)

[32] American Bar Association, *New York State Bar Association Tackles Ethics of Cloud Computing,*(May 2011) http://www.americanbar.org/newsletter/groups/labor_law/ll_flash/1105_aball_flash/1105_aball_flash_ethics.html

[33] New York State Bar Assoc. Comm. on Prof'l Ethics, s*upra* note 31.

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.[34]

D. Pennsylvania – Internal and External Due Diligence

In November of 2011, The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility released their opinion on cloud computing. The Committee acknowledged that the cloud would "reduce costs, improve efficiency and provide better client service."[35]

The Committee provided a fifteen point list of possible steps a firm "may" take in exercising reasonable care with cloud computing:

1. Backing up data;
2. Installing a firewall;
3. Limiting information that is provided to others;
4. Avoiding inadvertent disclosure of information;
5. Verifying the identity of individuals to whom the attorney provides confidential information;
6. Refusing to disclose confidential information to unauthorized individuals;
7. Encrypting confidential data;
8. Monitor who is accessing the data;
9. Creating plans to address security breaches;
10. Ensuring the provider does not have any ownership of the data;

[34] *Id.*

[35] Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200.

11. Investigate the provider and their reputation;
12. Determine if the data is in a non-proprietary format;
13. Require training for all individuals accessing the cloud;
14. Ensuring a copy of digital data is stored onsite; and
15. Having an alternate means to connect to the Internet. [36]

E. Massachusetts – Client's Consent

On May 17, 2012, the Massachusetts Bar Association issued their ethics opinion on cloud computing. The MBA Committee concluded: "the use of an Internet based storage provider to store confidential client information would not violate Massachusetts Rule of Professional Conduct 1.6(a) in ordinary circumstances *so long as the* Lawyer undertakes reasonable efforts to ensure that the provider's data privacy policies, practices and procedures are compatible with Lawyer's professional obligations."[37]

The Committee listed several examples of what constitutes reasonable efforts:

1. examining the provider's policies and procedures regarding confidential data;
2. ensuring that those terms prohibit unauthorized access to data;
3. ensuring that the lawyer will have reasonable access and control over the data;
4. examining the provider's security practices; and
5. periodically revisiting these topics to ensure continued acceptability.[38]

[36] *Id.*

[37] Massachusetts State Bar Association, Ethics Opinion 12-03.

[38] *Id.*

Most unique about this opinion is the Committee's directive that a lawyer "should refrain from storing or transmitting particularly sensitive client information by means of the Internet *without first seeking and obtaining the client's express consent* to do so."[39] [Emphasis added].

The Committee concluded by stating that whether the cloud "is compatible with [a] Lawyer's ethical obligation to protect his clients' confidential information is one that the Lawyer must answer for himself based on the criteria set forth in this opinion, the information that he is reasonably able to obtain regarding the relative security of the various alternatives that are available, and his own sound professional judgment."[40]

F. North Carolina – Guidelines for Professional Judgment

The North Carolina State Bar's Ethics Committee issued their opinion on October 20, 2011. The Committee opined that lawyers may use the cloud, "provided steps are taken to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property."[41] In taking these steps, the lawyer should apply "the same diligence and competency to managing the risks of SaaS that the lawyer is required to apply when representing clients."[42]

Regarding the steps a lawyer should take, the Committee noted that their opinion "does not set forth specific security requirements because mandatory security measures

[39] *Id.*

[40] *Id.*

[41] North Carolina Bar Association Ethics Committee, 2011 Formal Ethics Opinion 6.

[42] *Id.*

would create a false sense of security in an environment where the risks are continually changing."[43] Rather, the Committee stated "due diligence and frequent and regular education are required."[44]

The Committee concluded by generally recommending the following security measures:

1. Include an agreement on how the vendor will handle confidential client information in keeping with the lawyer's professional responsibilities;

2. Have a method for retrieving the data, including a provision that vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm;

3. Careful review of the terms of the law firm's user or license agreement with the SaaS vendor including the security policy;

4. Evaluation of the SaaS vendor's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems; and

5. Evaluation of the extent to which the SaaS vendor backs up hosted data.[45]

IV. Suggested Guidelines.

The aforementioned ethical opinions contain limited instructions on what exactly attorneys should do in order to comply with their ethical responsibilities. It is no surprise that this places the attorney in an unenviable position, as they must determine what is ethical and what is not. The following guidelines are intended to assist today's attorney in navigating the undefined and confusing waters of reasonable care in regards to cloud computing.

---

[43] *Id.*

[44] *Id.*

[45] *Id.*

A. Use Only Reliable Providers

With technology as new as the cloud, it is difficult to ascertain whether a service provider has a respectable reputation. Some providers, such as Microsoft, Google, and Apple have deep roots in the IT field, whereas other smaller market-participants have not yet earned a reputation at all. In order to meet his or her ethical duties, an attorney should consult with news sources, Internet search engines, and an IT specialist to determine the reputations of potential service providers.

B. Request Documents to Evidence Due Diligence

In order to demonstrate that he or she has done their due diligence, the attorney should request copies of the prospective provider's certifications from one of the agencies that independently audit the security practices of cloud providers.[46] "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."[47] By selecting and using a provider who has received one of these certifications, the attorney increases the likelihood that, if there was a dispute, they would be held to have exercised reasonable care.

[46] Jayaratnam, *supra* note 18.

[47] *Id.*

C. Get Consent From Your Client

The easiest procedural safeguard to accomplish is obtaining the client's express written consent prior to storing their information in the cloud. One of the most effortless and efficient ways to do this is through the engagement letter. The attorney should simply include a provision in the engagement letter, with an accompanying line for initialing, which states that the client consents to having their information stored on cloud servers.

D. Keep All of Your Data Encrypted

Whenever an attorney uses the cloud to store client data, this information will reside in one of three places: on the computer, in transit to the cloud, or on the cloud server. Regardless of where this information is located, the data should be encrypted at all times.[48] This can be accomplished through the use of encryption applications to encrypt the computer hard-drive, and portable media such as USB drives, laptops, tablets and smartphones. Because not everyone is familiar with encryption software and how to effectively utilize it, those who are unfamiliar should consult with an IT specialist to receive advice and training.

E. Establish Data Management Policies and Procedures

In order to perform their due diligence, an attorney must do more than simply select a reputable provider.[49] It is necessary that the attorney "sensitize all staff (professional and non-professional) to the importance of maintaining security (such as protecting the

[48] 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.

[49] Jayaratnam, s*upra* note 18.

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."[50] It is also prudent that all training policies and procedures are documented and acknowledged by the employee. Because all states require reasonable care and due diligence in order to store data on the cloud, it is necessary to have some documentation to evidence that reasonable care was taken.[51]

F. Include Key Terms in the Contract / Service Level Agreement

We have saved the most important suggested guideline for last. It is imperative that an attorney scrutinize and negotiate terms of the cloud contract to meet not only the attorney's needs, but also to comply with ethical guidelines. When reviewing a potential provider's Service Level Agreement ("SLA"), an attorney should be on the lookout for the following commitments and should negotiate for their inclusion into the contract.

1. Definition of Confidential Information

There should be a comprehensive definition for Confidential Information. The following is an example of a broad definition of Confidential Information:

> Confidential Information" means and includes any and all of the following information that has been, or may be disclosed to Recipient, by the Discloser or directors, officers, employees, agents, consultants, advisors, or other representatives, including legal counsel, accountants, and financial advisors ("Representatives") of the Discloser, regardless of the medium:

[50] *Id.*

[51] *Id.*

i. all information that is a trade secret under applicable trade secret or other law;

ii. all information concerning product specifications, patents, trademarks, copyrights, service marks, patent applications, data, know-how, formulae, compositions, processes, designs, sketches, photographs, graphs, drawings, samples, inventions, and ideas, past current and planned research and development, current and planned manufacturing or distribution methods and processes, customer lists, client lists, current and anticipated customer requirements, price lists, bidding processes, market studies, business plans, computer hardware, Software and computer software and database technologies, systems, structures, and architectures;

iii. all information concerning the business and affairs of the Discloser and its clients (which includes historical and current financial statements, financial projections and budgets, tax returns and accountants' materials, historical, current and projected sales, capital spending budgets and plans, business plans, strategic plans, marketing and advertising plans, publications, client and customer lists and files, contracts, the names and backgrounds of key personnel and personnel training techniques and materials, however documented) and all information obtained from review of the Discloser's documents, property, or discussions with the Discloser, regardless of the form of communication;

iv. all notes, analyses, compilations, studies, summaries and other material prepared by the Recipient to the extent containing or based, in whole or in part, upon any information included in the foregoing; and

v. all information transmitted between a client and his [or her] lawyer in the course of that relationship and in confidence by a means which, so far as the client is aware, discloses the information to no third persons other than those who are present to further the interest of the client in the consultation or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted, and includes a legal opinion formed and the advice given by the lawyer in the course of that relationship. This includes, but is not limited to, an attorney's legal opinions, impressions, and conclusions, regardless of whether they have been communicated to the client.

2. Ownership of Data

The agreement should explicitly state that the cloud provider does not have any ownership or security interest either in the confidential information or the data uploaded to that provider's system. Conversely, the agreement should also state that the attorney owns all of the intellectual property rights in his or her data. The vendor should also agree to keep the client's confidential data separate from other data. Lastly, it is imperative that attorneys completely avoid vendors who claim any ownership rights to information stored in the cloud.

3. Data Storage Location

Depending on the nature of an attorney's practice, as well as specific state regulations, it may be beneficial to include a provision establishing geographic parameters for where the data may be stored. For example, if data is stored out of the country, the attorney may be faced with foreign laws on government access and consumer privacy rights. This could prove to be especially difficult for some attorneys unfamiliar with international law.

4. Unfettered Access

The provider should agree to provide unfettered access to client data at least 99.9% of the time.[52] This takes into account reasonable downtime for the provider to conduct necessary maintenance on its servers.

5. Up to Date Security

[52] The total cloud server downtime should only be approximately forty-five minutes per month.

Due to concerns of data security breaches, the provider should possess the technology to withstand a foreseeable attempt by a third party to infiltrate its servers. The contract should include a provision that the provider will maintain the most up-to-date security practices for both the physical and electronic safety and security of its servers. This includes encryption, firewalls, locked facilities, redundant storage, and most importantly, an obligation to react to advancements and developments in the relevant technology.

6. Timely Notice of Breach

The onus should be on the provider to give timely notice to the attorney when there is either a physical or electronic breach of data, or an attempted breach of data. Include a provision that the degree of breach or attempted breach is irrelevant; even the smallest attempt triggers mandatory notice.

7. Timely Subpoena Notice

The provider should agree to timely notify the attorney as soon as a third party requests the provider to make available confidential information, client information, or any data the attorney has stored on the cloud server. The attorney should be provided with enough time to determine if they want to resist disclosure and act accordingly.

8. Access Without Internet Connection

The cloud data should be automatically synchronized and stored on any personal computer, tablet, or other device in the attorney's control that is capable of supporting the cloud data. This will allow the attorney to access the data in the event of a loss of Internet connectivity.

9. Data Retrieval

The provider should offer a method of retrieving data if and when the attorney or law firm terminates the use of the cloud service, the provider stops offering the service or goes out of business, or there is a break in continuity.

V. Conclusion

Given the numerous advantages that cloud computing has to offer, coupled with its universal acceptance by state bar associations, attorneys and law firms should be willing to embrace the cloud. So long as the attorney acts with reasonable care in selecting a provider and storing the data, it is likely that he or she will be deemed to have acted within the boundaries of acceptable ethics practice.