LIFE IN THE CLOUDS:
ETHICAL ISSUES ARISING FROM CLOUD COMPUTING

CASSIE MCGARVEY, *Houston*
Sanders McGarvey, LLP

State Bar of Texas
31ST ANNUAL
ADVANCED INTELLECTUAL PROPERTY LAW
February 8-9, 2018
Houston

CHAPTER 14

CASSIE MCGARVEY
Sanders McGarvey LLP
12 Greenway Plaza, Suite 210
Houston, TX 77046
713-493-7547
FAX: 713-955-9670

BIOGRAPHICAL INFORMATION

EDUCATION

B.A. with Honors, University of St. Thomas, Houston
J.D., University of Houston

PROFESSIONAL ACTIVITIES

Partner, Sanders McGarvey LLP, Houston TX
Chair-Elect, Houston Bar Association Real Estate Section
Co-Chair, Houston Bar Association Law Week Fun Run Committee
Leadership Houston, Class XXXIV
Founder, McGarvey Launch Group
Texas Rising Star, 2014-2018
Houstonia Top Lawyers, 2016-2017
Houston Bar Association President's Award, 2017

PUBLICATIONS, ACADEMIC APPOINTMENTS, & HONORS

Ethics of Negotiations, Houston Association of Professional Landmen, Fall 2017
New Ethics Opinions on Confidential Information and Metadata, State Bar of Texas CLE / Webinar, April 2017
Ethical Issues When Your Firm Has a BYOD Policy, Houston Paralegal Association, April 2017
New Ethics Opinions on Confidential Information and Metadata, Houston Association of Professional Landmen, Spring 2017
BYOD Advice for Business Owners, Friendswood Chamber of Commerce, March 2017
Real Estate Basics for Probate Attorneys, Houston Attorneys in Tax and Probate, March 2017
Ethical Issues in BYOD, State Bar of Texas CLE / Webinar, December 2016
Ethical Use of Cloud Computing, Houston Bar Association Real Estate Section, December 2016
Life in the Clouds: Protecting Confidentiality in the Virtual World, HBA Real Estate Section, December 2016
BYOD: Ethical and Strategic Considerations, Texas Bar CLE Webinar, December 2016
Real Estate Issues in Litigation, Northwest Bar Association, August 2016
Put Down the Smartphone: Live and Work with Focus and Intention, Women's Energy Network, June 2016
BYOD: Advice for Employers and Employees, Houston Bar Association, May 2016
BYOD: Advice for Employers and Employees, Houston Association of Professional Landmen, Spring 2016
Life in the Clouds: Protecting Confidentiality in the Virtual World, The Driven Speaker Series, January 2016
Head in the Clouds: Preserving Attorney-Client Privilege in the Digital World, HBA Oil & Gas Section, November 2015
Has Anyone Seen My Phone? Protecting Confidential Information in the Digital Age, South Texas College of Law, 2015 Energy Law Institute
Quick, Where's Your Floppy Drive? Document Retention in the Age of Constant Format Change, Houston Association of Professional Landmen, Spring 2015
Attorney Client Privilege with Cloud Computing, Houston Association of Professional Landmen, Fall 2014
Surface Use and Access in Oil & Gas Development: Introduction, EUCI Course, November 12, 2014

TABLE OF CONTENTS

LIFE IN THE CLOUDS: ETHICAL ISSUES ARISING FROM CLOUD COMPUTING

I. INTRODUCTION

A. What is Cloud Computing

For many, cloud computing evokes images of their data being stored in mystical "cloud" storage locations. In reality, cloud computing is nothing more than a method of harnessing the power of the internet to store your data. It is "a model for enabling ubiquitous, convenient, on-demand network access to a shared full 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."[1] Instead of storing data locally on your own computer hard drive (or even a local network server), you are storing it on a shared resource in a potentially remote location(s) and accessing it though the internet. Although many may think of the "cloud" as lacking a location, the data is in fact stored in a physical location accessed with minimal management control.

B. Characteristics of Cloud Computing

By outsourcing data storage, cloud computing makes data easily accessible from multiple locations and multiple devices by multiple users and reduces the interaction with network personnel (i.e., your firm's IT person). National Institute of Standards and Technology has identified the primary characteristics of cloud computing (listed below). While making the data more accessible, there are heightened security risks of which lawyers must be aware (concerning sections in italics).

- ***On-Demand Self Service***. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically *without requiring human interaction* with each service provider.
- ***Broad Network Access***. Capabilities are available over the network and accessed through standard mechanisms that *promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations*).
- ***Resource Pooling***. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the *customer generally has no control or knowledge over the exact location of the provided resources*, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
- ***Rapid Elasticity***. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- ***Measured Service***. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). *Resource usage can be monitored, controlled, and reported*, providing transparency for both the provider and consumer of the utilized service.

Cloud computing is more than data storage. It primarily takes the following service models:

- ***Software as Service (SaaS)***: The capability provided to the consumer is to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email, or a program interface). The consumer does not manage or control the underlying cloud infrastructure including network servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- ***Platform as a Service (PaaS)***. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- ***Infrastructure as Service (IaaS)***. The capability provided to the consumer is provision processing, storage, networks, and other fundamental

[1] Peter Mell & Timothy Grance, National Institute of Standards and Technology , the NIST Definition of Cloud Computing, Special Publication 800-145 (available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf)

computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, as well as possibly limited control of select networking components (e.g., host firewalls).

II. HOW ATTORNEYS USE THE CLOUD

It would be nearly impossible to run a law firm without using cloud computing. Many basic programs associated with the legal profession and business management have transitioned to cloud-based applications. As such, we must recognize that many of the services and programs used daily in law firms are cloud computing services and consider our ethical obligations in connection with those services. The following are examples of cloud storage at use in many law firms:

- ***Hosted Email***. Many firms have jettisoned the cost of an in-house mail server and are relying on hosted email such as Microsoft Exchange Server, Google Mail (i.e., Google for Business), and other hosted email providers. With hosted email, messages (and the attachments to them) are stored remotely on your provider's servers in various locations.
- ***Legal Research***. Legal research is almost exclusively cloud based. Westlaw, LexisNexis, and their competitors are only available online. Information regarding your searches (and for which clients/matters you performed those searches) is stored on their servers. In short, attorney work product is available remotely.
- ***Practice Management Software***. Much of the latest firm management software is purely cloud-based (you access the program through the internet and your data is stored on their servers). Examples of these programs are Clio, MyCase, RocketMatter, etc. Related to practice management software is a ***Customer Relationship Management*** software. This software may also store confidential client information.
- ***Billing & Accounting Software.*** Like practice management software, many billing and accounting software programs have moved to the internet and are based on a subscription model.
- ***Document Management***. Document management has moved from the server to the cloud with integrated platforms. Services/programs such as SmokeBall save some of your data in the cloud and other data on your server.
- ***Discovery Software/Litigation Support Software***. In litigation matters involving a large amount of discovery, firms are using discovery support software to manage the documents. These services are storing documents – both for your client and the opposing party – in remote locations. Some firms will upload all client documents (even those protected by privilege) to these systems.
- ***Backup***. Businesses may use a cloud backup provider to periodically make a copy of their data and hold that data if they need it. It provides an off-site copy of your documents.
- ***Raw Data Storage***. Cloud servers provide the means to have seemingly unlimited storage. Through these centers, companies can store many documents and data.
- ***Other Online Services***. The above is not a full list. Additionally, law firms may use web conferencing tools, translation services, date calculators, and others.

It is imperative that attorneys understand where they are using the cloud so that they can consider their ethical obligations. Additionally, an understanding of the services in use in general business and personal matters will result in better service to clients. For instance, attorneys can more fully respond to discovery requests and protect from spoliation claims by fully understanding the breadth of where communications and documents may be stored.

III. WHY IS THIS AN ETHICS ISSUE

Cloud computing is an ethics issue because data comprised of your client's confidential information is being entrusted to a third-party. When handing over client information to a third-party, an attorney must understand the associated risks and the benefits.

While storing documents with a third-party storage company is not new for attorneys, never before have all client files – active and closed – been handed over to a third party for storage at an unknown location(s). For instance: with off-site storage, a firm entrusts its files (that are typically closed) to a local company whose security systems are easily verifiable. In contrast, with cloud computing, client data for current matters are given to third parties for storage in potentially multiple locations and jurisdictions, in areas where you cannot visit and confirm security protocols. Additionally, because the information is easily accessible by you, it is also accessible to others via the internet, not just at the brick and mortar location. When storing your paper files off site at a brick and mortar location, you were tasked with the obligation to ensure the safekeeping of those files. At the brick and mortar, you could physically inspect the security protocols and understand who had access to your files.

Now, we cannot physically inspect the warehouse(s) holding the servers/computers storing our firms' data. We must review the published security standards of the cloud provider to confirm that our client's documents are being held securely. Furthermore, we must recognize that the information stored in the cloud is more valuable than what was previously stored off-site. Rather than storing old or closed files, we are moving current files to the cloud. These files include vast quantities of commercially valuable information. Many firms contain information concerning patent applications, upcoming mergers and acquisitions, and litigation work-product. Because of the value of the information law firms hold, we must ensure that it is held safely.

IV. ETHICAL RULES APPLICABLE TO CLOUD COMPUTING

A. Texas Standards

1. Which rules apply

Texas has not amended the Disciplinary Rules of Professional Conduct to specifically address technology, nor has the Texas Committee on Professional Ethics issued an opinion concerning the use of cloud computing by lawyers. However, Opinions 572 (use of third-party copy service), 648 (client communication via email), and 665 (inadvertent disclosure of metadata) consider similar issues. These opinions centered on the interpretation of the following provisions of Rule 1.05:

> (a) "Confidential information" includes both "privileged information" and "unprivileged client information." "Privileged information" refers to the information of a client protected by the lawyer-client privilege of Rule 503 of the Texas Rules of Evidence or of Rule 503 of the Texas Rules of Criminal Evidence or by the principles of attorney-client privilege governed by Rule 501 of the Federal Rules of Evidence for United States Courts and Magistrates. "Unprivileged client information" means all information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client.
>
> (b) Except as permitted by paragraphs (c) and (d), or as required by paragraphs (e) and (f), a lawyer shall not knowingly:
>
> (1) Reveal confidential information of a client or a former client to:
>
> (i) a person that the client has instructed is not to receive the information; or
>
> (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm.
>
> (c) A lawyer may reveal confidential information:
>
> (1) When the lawyer has been expressly authorized to do so in order to carry out the representation.
> (2) When the client consents after consultation.
> (3) To the client, the client's representatives, or the members, associates, and employees of the lawyer's firm, except when otherwise instructed by the client.
>
> (d) A lawyer also may reveal unprivileged client information:
>
> (1) When impliedly authorized to do so in order to carry out the representation.
> (2) When the lawyer has reason to believe it is necessary to do so in order to:
>
> (i) carry out the representation effectively.

In the context of the evaluation of cloud computing and technology, the sections of the following Rules also apply:

> Rule 1.01: Competent and Diligent Representation
>
> (a) A lawyer shall not accept or continue employment in a legal matter which the lawyer knows or should know is beyond the lawyer's competence, unless:
>
> (1) another lawyer who is competent to handle the matter is, with the prior informed consent of the client, associated in the matter.
>
> Rule 1.03: Communication
>
> (b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

> Rule 5.03: Responsibilities Regarding Nonlawyer Assistants
>
> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> (a) A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer;…

2. Discussion of relevant ethics opinions

As noted, Texas does not have a specific ethics opinion on the issue of cloud computing, however the Ethics Committee has already specifically addressed the use of a sub-contractor for managing confidential client information, electronic communications with clients, and technological competence for disclosing electronic information contained in documents (metadata). These opinions have a similar theme: *A lawyer must act reasonably to safeguard confidential client information. When using third-party providers, there must be a reasonable expectation that confidential client information will not be disclosed.*

Although two of the opinions deal with technology, the Ethics Committee does not provide specific technological guidelines. Any specific guidelines provided would quickly become obsolete with the rapid advancements in technology. However, the opinions do provide a list of items that would be considered in determining whether there is a reasonable expectation that information will be kept confidential:

- ***Reputation of the Provider***
- ***Prior Dealings***
- ***Written Agreement***
- ***Client Education***
- ***Consideration of the Type of Documents Being Stored***

The above list is not meant to be an exhaustive list for considerations in cloud computing. Rather, it is included to demonstrate that while Texas does not have an opinion specifically addressing cloud computing, there are opinions already that can be applied to this issue. I do not anticipate that different or heightened duties would apply based on the manner of storage or type of communication (i.e., no different duty for sub-contractor copy service and sub-contractor for document service or for email and regular mail). Instead, how a lawyer confirms the existence of a reasonable expectation that confidential data will not be disclosed differs between the platforms. Confirming the reasonable expectation of nondisclosure in cloud computing would require additional considerations.

B. ABA Model Rules

In 2012, the American Bar Association adopted technology amendments to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c) and a new Comment to Rule 1.6, addressing a layer's obligation to take reasonable measures to prevent inadvertent and unauthorized disclosure of information relating to the representation.

1. Duty of Competence

Model Rule 1.1 reads: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." In 2012, the scope of this requirement was clarified to address the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment 8 was amended to read:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

> Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] specifies that, to remain competent, lawyers need to "keep abreast of changes in the law and its practice." The Commission concluded that, in order to keep abreast of changes in law practice in the digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficult providing competent legal services in today's environment without knowing how to use email or create an electronic document.[2]

2. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Mode Rule 1.6(a)

[2] ABA Commission on Ethics 20/20 Report 105A (Aug. 2012).

requires that "A lawyer shall not reveal information relating to the representation of a Client" unless certain circumstances arise. The 2012 modification added a new duty to paragraph (c) that states: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

Amended Comment [18] provides, in part:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Then Comment [18] goes on to provide a non-inclusive list to guide lawyers in making "reasonable efforts" to prevent disclosure:

1) The sensitivity of the information;
2) The likelihood of disclosure if additional safeguards are not employed;
3) The cost of the additional safeguards;
4) The difficulty of implementing the safeguards; and
5) The extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

3. Duty to Communicate

Model Rule 1.4 generally addresses the communications between lawyers and their clients. However, Comment [18] to Rule 1.6 also address communications and provides: "A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communications that would otherwise be prohibited by this Rule.

C. ABA Ethics Opinion

In May 2017, the ABA Center for Professional Responsibility issued opinion 14-006 concerning email communication with clients. The Opinion concluded that:

> A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken *reasonable efforts* to prevent inadvertent or unauthorized access to information relating to the representation. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with client or by law, or when the nature of the information requires a higher degree of security. (emphasis added)

The opinion considered the 2012 amendments to the Model Rules (as discussed above) to conclude that use of electronic communications is acceptable – provided that reasonable efforts have been taken to protect against the inadvertent or unauthorized disclosure of client information. These considerations would/should also apply in the cloud computing analysis.

D. Other States

Many state ethics committees have directly addressed the issue of cloud computing.[3] No state has prohibited the use of cloud computing. Rather, throughout the opinions the consistent standard is that **attorneys must exercise reasonable care to evaluate the vendor and confirm an expectation of nondisclosure of confidential client information.** No opinion provides a standard for selecting a vendor, because any standard would quickly become obsolete. Further, the states are consistent that cloud storage must be decided on a case-by-case basis. For each matter, the attorney/firm must determine if the cloud storage and/or electronic communications are appropriate.

[3] The following states have an ethics opinion concerning cloud computing: Alabama, Alaska, Arizona, California, Connecticut, Delaware, Florida, Illinois, Iowa, Kentucky, Maine, Massachusetts, Nevada, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oregon, Pennsylvania, Vermont, Virginia, Washington, and Wisconsin.

The ABA has prepared a map and summary of many of the cloud computing opinions - https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html As of the date of this article, the map is not up-to-date.

V. COMPLYING WITH THE OBLIGATION OF REASONABLE CARE

The ethical considerations of cloud computing center on the disclosure and/or theft of confidential client information. The ABA 20/20 report identified the following concerns with cloud computing:

- Unauthorized access to confidential client information by a vendor's employees (or sub-contractors) or by outside parties (e.g., hackers) via the internet
- The storage of information on servers in countries with fewer legal protections for electronically stored information
- A vendor's failure to back up data adequately
- Unclear policies regarding ownership of stored data
- The ability to access the data using easily accessible software in the event that the lawyer terminates the relationship with the cloud computing provider or the provider changes businesses or goes out of business
- The provider's procedures for responding to (or when appropriate, resisting) governmental requests for access to information
- Policies for data destruction when a lawyer no longer wants the relevant data available, or transferring the data if a client switches law firms
- Insufficient data encryption
- The extent to which lawyers need to obtain client consent before using cloud computing services to store or transmit the client's confidential information.

It is clear from the Texas opinions concerning technology and third-party access to confidential client information, the ABA Model Rules and opinions, and the opinions from other states, that there is no clear standard for determining whether cloud computing is appropriate. Rather, a lawyer should develop a checklist to confirm that a reasonable expectation of nondisclosure of confidential client information exists.

A. STEP ONE: Read and Understand the Terms and Conditions

Texas Ethics Opinion 572 raised the importance of the contract with a sub-contractor vendor for determining whether there is a reasonable expectation for nondisclosure of confidential client information. With cloud computing, the contract is the terms and conditions. In selecting a cloud storage provider, the following issues must be addressed within the terms and conditions:

1. Who Owns the Data?

With many providers, especially SaaS providers, the question of data ownership must be addressed. Some services, especially consumer-grade services (read: free internet-based programs) include a provision that they own the data that is entered into the site or have a license to use the data.

2. With Whom Will You Share My Data? Who Has Access to the Data?

Some providers include provisions that will allow the provider to share your data with their sub-contractors or other third-parties. An attorney must be mindful of who the provider is allowed to share with, and to whom they allow access to the data. The application of the Rules focuses on ensuring nondisclosure of confidential client information. Know if the terms and conditions give your provider the right to disclose the data with others.

3. When Will You Destroy My Data?

When data is stored in multiple locations, deleting a file may not result in the complete destruction of the file. For instance, emails stored with Microsoft Exchange may still be recovered. Additionally, because of redundancies, a file may still exist in some locations but not others. The terms and conditions must provide a schedule or explanation of how data will be deleted/destroyed when requested by you.

4. What Will You Do With My Data?

Many providers reserve the right to copy, duplicate, or otherwise manipulate your data. Some of these rights are needed to provide better service – and even protect your data by creating redundancies across multiple locations. However, sometimes the data may be used for research or to determine how better to market to you. Ensure the terms and conditions explain how the provider will use your data.

5. Where Will You Store My Data?

Cloud storage providers have locations around the world. Locations outside the United States may not have the same restrictions on privacy as a location within the United States. Consider the location of the storage.

6. Will You Notify Me Before Disclosing Data?

A third party may disclose data in response to a subpoena or in response to a court order. To ensure that documents are not improperly disclosed, you must confirm that the provider will not disclose documents unless they notify you first. If responding to a court order, you would want the opportunity to limit production.

7. What Are Your Limitations on Liability? Do You Warrant Your Services?

Unfortunately, cloud computing providers may not be accessible for numerous reasons. For instance, their facilities could lose power or they could have internet problems. During this downtime, you may be unable to work or complete necessary tasks. For some types of services, the downtime could be a minor inconvenience. However, if you cannot access documents and have a deadline, you could miss the deadline. Or, if you cannot conduct legal research and need to finish a brief, you may not make your briefing deadline. In these instances, you and your client may be adversely impacted. The terms and conditions should address the provider's liability for outages. Additionally, there will be information regarding any warranty that the services will operate as marketed.

8. Will You Notify Me of Security Breaches?

The terms and conditions should include notice in the event of security breaches. Again, the primary consideration in selecting a provider is whether there is reasonable expectation that information will not be disclosed. If information has been compromised, you must know about the compromise.

9. Will You Notify Me of Amendments to the Terms and Conditions and/or Security Policies?

The terms and conditions govern your agreement with the cloud computing service provider. Unlike almost every other contract, a cloud computing provider can likely amend the contract without your consent. As such, you must be notified of the changes.

10. How Can I Remove My Data From Your Service?

This consideration is incredibly important with SaaS providers. When you decide to cease using the service, you need confirmation that you will be able to remove your information. For instance, with a case management system, the data must be exported from the software in a manner that would be usable by another software.

B. STEP TWO: Examine the Provider's Existing Practices

1. Data Encryption

Confirm that the cloud provider complies with industry standards for data encryption.

2. Password Protection

Review the provider's password policies for its users. Also, if possible, review the password policies for its employees and internal users. The passwords to access the information must be secure.

3. Who Has the Security Keys?

Review where the encryption key for the provider is located and who has access to this key. Remember, if one has access to the encryption key, then he can view your data.

4. What Protections Does the Provider Have: Firewalls, Intrusion-detection Systems, and System Backups?

Review the provider's protections. You must have assurances that the provider is, at a minimum, complying with industry standards for security and backups.

C. STEP THREE: Examine the Provider's Service History and Reputation

When selecting a service provider, be sure to consider their history of service outages and security breaches. A history of outages can be a warning that you will not have access to the service and/or your data when you need it. Security breaches can indicate that the provider has not fully updated its security. Note that, even though a company/vendor has a history in the industry, be aware that they may cancel service. Pay attention to credible industry information that a service may be discontinued.

D. STEP FOUR: Continue to Evaluate the Service Provider

As technology evolves, a service provider must continually be evaluated. If a service provider does not keep pace with advances in technology, your client's data will be at risk. A re-evaluation of the service provider must be done at regular intervals. Establish a policy and schedule for a review of cloud service providers. If a vendor no longer provides a reasonable expectation that confidential client documents will not be disclosed, then you must change vendors.

E. STEP FIVE: Determine if Client Consent is Necessary

Use of cloud computing should be determined on a case-by-case basis. In each case, determine if client consent is necessary and if you should even be storing the data in the cloud. For instance, in determining whether a lawyer may store and synchronize electronic work files containing confidential client information across several devices and platforms, the Massachusetts ethics committee notes that a lawyer "should refrain from storing or transmitting particularly sensitive client information by means of the internet without first seeking the client's express consent to do so."[4] Note the opinion does not define

[4] Mass. Ethics Opinion 12-03 (March 2012) available at: https://www.massbar.org/publications/ethics-opinions/ethics-opinions-2012-opinion-12-03.

"sensitive client information." Regardless, it requires an attorney to consider whether cloud computing is appropriate in that situation.

Similarly, the New Hampshire Ethics Committee notes that "if the information is highly sensitive, consent of the client to use cloud computing may be necessary." [5] Again, the focus is on a case-by-case analysis and the obligation to educate your client on the risks and benefits associated with the technology.

F. STEP SIX: Establish and Enforce a Technology Policy at Your Firm

This article focuses on firm-implemented cloud computing. It does not address the implications of technological solutions employed without client or firm approval. For instance, do firm employees use a cloud storage to save documents so that they can work remotely or bypass cumbersome remote access programs? Do firm employees use LinkedIn, Facebook, WhatsApp, or other applications to communicate with clients? While many employees will use these consumer-grade applications to better work, they may not be considering the ethical implications using these solutions. To prevent this from occurring, a firm must have a policy prohibiting the use of non-firm sanctioned technology and enforce that policy.

[5] NH Ethics Op. 2012-23/4, available at: https://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp.