PENNSYLVANIA BAR ASSOCIATION COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY

ETHICAL OBLIGATIONS FOR ATTORNEYS USING CLOUD COMPUTING/ SOFTWARE AS A SERVICE WHILE FULFILLING THE DUTIES OF CONFIDENTIALITY AND PRESERVATION OF CLIENT PROPERTY

FORMAL OPINION 2011-200

I. Introduction and Summary

If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using "cloud computing." While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely "a fancy way of saying stuff's not on your computer." [1]

From a more technical perspective, "cloud computing" encompasses several similar types of services under different names and brands, including: web-based e-mail, online data storage, software-as-a-service ("SaaS"), platform-as-a-service ("PaaS"), infrastructure-as-a-service ("IaaS"), Amazon Elastic Cloud Compute ("Amazon EC2"), and Google Docs.

This opinion places all such software and services under the "cloud computing" label, as each raises essentially the same ethical issues. In particular, the central question posed by "cloud computing" may be summarized as follows:

> May an attorney ethically store confidential client material in "the cloud"?

In response to this question, this Committee concludes:

> Yes. An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.

****

In recent years, technological advances have occurred that have dramatically changed the way attorneys and law firms store, retrieve and access client information. Many law firms view these

[1] Quinn Norton, "Byte Rights," *Maximum PC*, September 2010, at 12.

technological advances as an opportunity to reduce costs, improve efficiency and provide better client service. Perhaps no area has seen greater changes than "cloud computing," which refers to software and related services that store information on a remote computer, *i.e.*, a computer or server that is not located at the law office's physical location. Rather, the information is stored on another company's server, or many servers, possibly all over the world, and the user's computer becomes just a way of accessing the information.[2]

The advent of "cloud computing," as well as the use of electronic devices such as cell phones that take advantage of cloud services, has raised serious questions concerning the manner in which lawyers and law firms handle client information, and has been the subject of numerous ethical inquiries in Pennsylvania and throughout the country. The American Bar Association Commission on Ethics 20/20 has suggested changes to the Model Rules of Professional Conduct designed to remind lawyers of the need to safeguard client confidentiality when engaging in "cloud computing."

Recent "cloud" data breaches from multiple companies, causing millions of dollars in penalties and consumer redress, have increased concerns about data security for cloud services. The Federal Trade Commission ("FTC") has received complaints that inadequate cloud security is placing consumer data at risk, and it is currently studying the security of "cloud computing" and the efficacy of increased regulation. Moreover, the Federal Bureau of Investigations ("FBI") warned law firms in 2010 that they were being specifically targeted by hackers who have designs on accessing the firms' databases.

This Committee has also considered the client confidentiality implications for electronic document transmission and storage in Formal Opinions 2009-100 ("Metadata") and 2010-200 ("Virtual Law Offices"), and an informal Opinion directly addressing "cloud computing." Because of the importance of "cloud computing" to attorneys – and the potential impact that this technological advance may have on the practice of law – this Committee believes that it is appropriate to issue this Formal Opinion to provide guidance to Pennsylvania attorneys concerning their ethical obligations when utilizing "cloud computing."

This Opinion also includes a section discussing the specific implications of web-based electronic mail (e-mail). With regard to web-based email, *i.e.*, products such as Gmail, AOL Mail, Yahoo! and Hotmail, the Committee concludes that attorneys may use e-mail but that, when circumstances require, attorneys must take additional precautions to assure the confidentiality of client information transmitted electronically.

II. Background

For lawyers, "cloud computing" may be desirable because it can provide costs savings and increased efficiency in handling voluminous data. Better still, cloud service is elastic, and users can have as much or as little of a service as they want at any given time. The service is sold on demand, typically by the minute, hour or other increment. Thus, for example, with "cloud computing," an attorney can simplify document management and control costs.

[2] *Id.*

The benefits of using "cloud computing" may include:

- Reduced infrastructure and management;
- Cost identification and effectiveness;
- Improved work production;
- Quick, efficient communication;
- Reduction in routine tasks, enabling staff to elevate work level;
- Constant service;
- Ease of use;
- Mobility;
- Immediate access to updates; and
- Possible enhanced security.

Because "cloud computing" refers to "offsite" storage of client data, much of the control over that data and its security is left with the service provider. Further, data may be stored in other jurisdictions that have different laws and procedures concerning access to or destruction of electronic data. Lawyers using cloud services must therefore be aware of potential risks and take appropriate precautions to prevent compromising client confidentiality, *i.e.*, attorneys must take great care to assure that any data stored offsite remains confidential and not accessible to anyone other than those persons authorized by their firms. They must also assure that the jurisdictions in which the data are physical stored do not have laws or rules that would permit a breach of confidentiality in violation of the Rules of Professional Conduct.

III. Discussion

A. Prior Pennsylvania Opinions

In Formal Opinion 2009-100, this Committee concluded that a transmitting attorney has a duty of reasonable care to remove unwanted metadata from electronic documents before sending them to an adverse or third party. Metadata is hidden information contained in an electronic document that is not ordinarily visible to the reader. The Committee also concluded, *inter alia*, that a receiving lawyer has a duty pursuant to RPC 4.4(b) to notify the transmitting lawyer if an inadvertent metadata disclosure occurs.

Formal Opinion 2010-200 advised that an attorney with a virtual law office "is under the same obligation to maintain client confidentiality as is the attorney in a traditional physical office." Virtual law offices generally are law offices that do not have traditional brick and mortar facilities. Instead, client communications and file access exist entirely online. This Committee also concluded that attorneys practicing in a virtual law office need not take additional precautions beyond those utilized by traditional law offices to ensure confidentiality, because virtual law firms and many brick-and-mortar firms use electronic filing systems and incur the same or similar risks endemic to accessing electronic files remotely.

Informal Opinion 2010-060 on "cloud computing" stated that an attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney makes reasonable efforts to protect confidential electronic communications and information. Reasonable efforts

discussed include regularly backing up data, installing firewalls, and avoiding inadvertent disclosures.

B. Pennsylvania Rules of Professional Conduct

An attorney using "cloud computing" is under the same obligation to maintain client confidentiality as is the attorney who uses offline documents management. While no Pennsylvania Rule of Profession Conduct specifically addresses "cloud computing," the following rules, *inter alia,* are implicated:

> Rule 1.0 ("Terminology");
> Rule 1.1 ("Competence");
> Rule 1.4 ("Communication");
> Rule 1.6 ("Confidentiality of Information");
> Rule 1.15 ("Safekeeping Property"); and
> Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistants").

Rule 1.1 ("Competence") states:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment [5] ("Thoroughness and Preparation") of Rule 1.1 provides further guidance about an attorney's obligations to clients that extend beyond legal skills:

> Competent handling of particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. …

Competency is affected by the manner in which an attorney chooses to represent his or her client, or, as Comment [5] to Rule 1.1 succinctly puts it, an attorney's "methods and procedures." Part of a lawyer's responsibility of competency is to take reasonable steps to ensure that client data and information is maintained, organized and kept confidential when required. A lawyer has latitude in choosing how or where to store files and use software that may best accomplish these goals. However, it is important that he or she is aware that some methods, like "cloud computing," require suitable measures to protect confidential electronic communications and information. The risk of security breaches and even the complete loss of data in "cloud computing" is magnified because the security of any stored data is with the service provider. For example, in 2011, the syndicated children's show "Zodiac Island" lost an entire season's worth of episodes when a fired employee for the show's data hosting service accessed the show's content without authorization and wiped it out.[3]

[3] Eriq Gardner, "Hacker Erased a Season's Worth of 'Zodiac Island'," *Yahoo! TV* (March 31, 2011), available at http://tv.yahoo.com/news/article/tv-news.en.reuters.com/tv-news.en.reuters.com-20110331-us_zodiac

Rule 1.15 ("Safekeeping Property") requires that client property should be "appropriately safeguarded."[4] Client property generally includes files, information and documents, including those existing electronically. Appropriate safeguards will vary depending on the nature and sensitivity of the property. Rule 1.15 provides in relevant part:

> (b) A lawyer shall hold all Rule 1.15 Funds and property separate from the lawyer's own property. Such property shall be identified and appropriately safeguarded.

Rule 1.6 ("Confidentiality of Information") states in relevant part:

> (a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).
>
> (d) The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.

Comment [2] of Rule 1.6 explains the importance and some of the foundation underlying the confidential relationship that lawyers must afford to a client. It is vital for the promotion of trust, justice and social welfare that a client can reasonably believe that his or her personal information or information related to a case is kept private and protected. Comment [2] explains the nature of the confidential attorney-client relationship:

> A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. …

Also relevant is Rule 1.0(e) defining the requisite "Informed Consent":

> "Informed consent" denotes the consent by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.

Rule 1.4 directs a lawyer to promptly inform the client of any decision with respect to which the client's informed consent is required. While it is not necessary to communicate every minute

[4] In previous Opinions, this Committee has noted that the intent of Rule 1.15 does not extend to the entirety of client files, information and documents, including those existing electronically. In light of the expansion of technology as a basis for storing client data, it would appear that the strictures of diligence required of counsel under Rule 1.15 are, at a minimum, analogous to the "cloud."

detail of a client's representation, "adequate information" should be provided to the client so that the client understands the nature of the representation and "material risks" inherent in an attorney's methods. So for example, if an attorney intends to use "cloud computing" to manage a client's confidential information or data, it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of "cloud computing" and the advantages as well as the risks endemic to online storage and transmission.

Absent a client's informed consent, as stated in Rule 1.6(a), confidential client information cannot be disclosed unless either it is "impliedly authorized" for the representation or enumerated among the limited exceptions in Rule 1.6(b) or Rule 1.6(c).[5] This may mean that a third party vendor, as with "cloud computing," could be "impliedly authorized" to handle client data provided that the information remains confidential, is kept secure, and any disclosure is confined only to necessary personnel. It also means that various safeguards should be in place so that an attorney can be reasonably certain to protect any information that is transmitted, stored, accessed, or otherwise processed through cloud services. Comment [24] to Rule 1.6(a) further clarifies an attorney's duties and obligations:

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. 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 communication that would otherwise be prohibited by this Rule.

An attorney utilizing "cloud computing" will likely encounter circumstances that require unique considerations to secure client confidentiality. For example, because a server used by a "cloud computing" provider may physically be kept in another country, an attorney must ensure that the data in the server is protected by privacy laws that reasonably mirror those of the United States. Also, there may be situations in which the provider's ability to protect the information is compromised, whether through hacking, internal impropriety, technical failures, bankruptcy, or other circumstances. While some of these situations may also affect attorneys who use offline

[5] The exceptions covered in Rule 1.6(b) and (c) are not implicated in "cloud computing." Generally, they cover compliance with Rule 3.3 ("Candor Toward the Tribunal"), the prevention of serious bodily harm, criminal and fraudulent acts, proceedings concerning the lawyer's representation of the client, legal advice sought for Rule compliance, and the sale of a law practice.

storage, an attorney using "cloud computing" services may need to take special steps to satisfy his or her obligation under Rules 1.0, 1.6 and 1.15.[6]

Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistants") states:

> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> (a) A partner and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer.
>
> (b) 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; and
>
> (c) A lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and in either case knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

At its essence, "cloud computing" can be seen as an online form of outsourcing subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are associated with an attorney. Therefore, a lawyer must ensure that tasks are delegated to competent people and organizations. This means that any service provider who handles client information needs to be able to limit authorized access to the data to only necessary personnel, ensure that the information is backed up, reasonably available to the attorney, and reasonably safe from unauthorized intrusion.

It is also important that the vendor understands, embraces, and is obligated to conform to the professional responsibilities required of lawyers, including a specific agreement to comply with all ethical guidelines, as outlined below. Attorneys may also need a written service agreement that can be enforced on the provider to protect the client's interests. In some circumstances, a client may need to be advised of the outsourcing or use of a service provider and the identification of the provider. A lawyer may also need an agreement or written disclosure with the client to outline the nature of the cloud services used, and its impact upon the client's matter.

C. Obligations of Reasonable Care for Pennsylvania/Factors to Consider

[6] Advisable steps for an attorney to take reasonable care to meet his or her obligations for Professional Conduct are outlined below.

In the context of "cloud computing," an attorney must take reasonable care to make sure that the conduct of the cloud computing service provider conforms to the rules to which the attorney himself is subject. Because the operation is outside of an attorney's direct control, some of the steps taken to ensure reasonable care are different from those applicable to traditional information storage.

While the measures necessary to protect confidential information will vary based upon the technology and infrastructure of each office – and this Committee acknowledges that the advances in technology make it difficult, if not impossible to provide specific standards that will apply to every attorney – there are common procedures and safeguards that attorneys should employ.

These various safeguards also apply to traditional law offices. Competency extends beyond protecting client information and confidentiality; it also includes a lawyer's ability to reliably access and provide information relevant to a client's case when needed. This is essential for attorneys regardless of whether data is stored onsite or offsite with a cloud service provider. However, since cloud services are under the provider's control, using "the cloud" to store data electronically could have unwanted consequences, such as interruptions in service or data loss. There are numerous examples of these types of events. Amazon EC2 has experienced outages in the past few years, leaving a portion of users without service for hours at a time. Google has also had multiple service outages, as have other providers. Digital Railroad, a photo archiving service, collapsed financially and simply shut down. These types of risks should alert anyone contemplating using cloud services to select a suitable provider, take reasonable precautions to back up data and ensure its accessibility when the user needs it.

Thus, the standard of reasonable care for "cloud computing" may include:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
- Installing a firewall to limit access to the firm's network;
- Limiting information that is provided to others to what is required, needed, or requested;
- Avoiding inadvertent disclosure of information;
- Verifying the identity of individuals to whom the attorney provides confidential information;
- Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
- Implementing electronic audit trail procedures to monitor who is accessing the data;

- Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;

- Ensuring the provider:
    - explicitly agrees that it has no ownership or security interest in the data;
    - has an enforceable obligation to preserve security;
    - will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
    - has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
    - includes in its "Terms of Service" or "Service Level Agreement" an agreement about how confidential client information will be handled;
    - provides the firm with right to audit the provider's security procedures and to obtain copies of any security audits performed;
    - will host the firm's data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania;
    - provides a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity; and,
    - provides the ability for the law firm to get data "off" of the vendor's or third party data hosting company's servers for the firm's own use or in-house backup offline.

- Investigating the provider's:
    - security measures, policies and recovery methods;
    - system for backing up data;
    - security of data centers and whether the storage is in multiple centers;
    - safeguards against disasters, including different server locations;
    - history, including how long the provider has been in business;
    - funding and stability;
    - policies for data retrieval upon termination of the relationship and any related charges; and,
    - process to comply with data that is subject to a litigation hold.

- Determining whether:
    - data is in non-proprietary format;
    - the Service Level Agreement clearly states that the attorney owns the data;
    - there is a 3rd party audit of security; and,
    - there is an uptime guarantee and whether failure results in service credits.

- Employees of the firm who use the SaaS must receive training on and are required to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

- Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.[7]

- Having an alternate way to connect to the internet, since cloud service is accessed through the internet.

The terms and conditions under which the "cloud computing" services are offered, *i.e.*, Service Level Agreements ("SLAs"), may also present obstacles to reasonable care efforts. Most SLAs are essentially "take it or leave it,"[8] and often users, including lawyers, do not read the terms closely or at all. As a result, compliance with ethical mandates can be difficult. However, new competition in the "cloud computing" field is now causing vendors to consider altering terms. This can help attorneys meet their ethical obligations by facilitating an agreement with a vendor that adequately safeguards security and reliability.[9]

Additional responsibilities flow from actual breaches of data. At least forty-five states, including Pennsylvania, currently have data breach notification laws and a federal law is expected. Pennsylvania's notification law, 73 P.S. § 2303 (2011) ("Notification of Breach"), states:

> (a) GENERAL RULE. -- An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.
>
> (b) ENCRYPTED INFORMATION. -- An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

---

[7] This is recommended even though many vendors will claim that it is not necessary.

[8] Larger providers can be especially rigid with SLAs, since standardized agreements help providers to reduce costs.

[9] One caveat in an increasing field of vendors is that some upstart providers may not have staying power. Attorneys are well advised to consider the stability of any company that may handle sensitive information and the ramifications for the data in the event of bankruptcy, disruption in service or potential data breaches.

> (c) VENDOR NOTIFICATION. -- A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

A June, 2010, Pew survey highlighted concerns about security for "cloud computing." In the survey, a number of the nearly 900 internet experts surveyed agreed that it "presents security problems and further exposes private information," and some experts even predicted that "the cloud" will eventually have a massive breach from cyber-attacks.[10] Incident response plans should be in place before attorneys move to "the cloud", and the plans need to be reviewed annually. Lawyers may need to consider that at least some data may be too important to risk inclusion in cloud services.

One alternative to increase security measures against data breaches could be "private clouds." Private clouds are not hosted on the Internet, and give users completely internal security and control. Therefore, outsourcing rules do not apply to private clouds. Reasonable care standards still apply, however, as private clouds do not have impenetrable security. Another consideration might be hybrid clouds, which combine standard and private cloud functions.

D. Web-based E-mail

Web-based email ("webmail") is a common way to communicate for individuals and businesses alike. Examples of webmail include AOL Mail, Hotmail, Gmail, and Yahoo! Mail. These services transmit and store e-mails and other files entirely online and, like other forms of "cloud computing," are accessed through an internet browser. While pervasive, webmail carries with it risks that attorneys should be aware of and mitigate in order to stay in compliance with their ethical obligations. As with all other cloud services, reasonable care in transmitting and storing client information through webmail is appropriate.

In 1999, The ABA Standing Commission on Ethics and Professional Responsibility issued Formal Opinion No. 99-413, discussed in further detail above, and concluded that using unencrypted email is permissible. Generally, concerns about e-mail security are increasing, particularly unencrypted e-mail. Whether an attorney's obligations should include the safeguard of encrypting emails is a matter of debate. An article entitled, "Legal Ethics in the Cloud: Avoiding the Storms," explains:

> Respected security professionals for years have compared e-mail to postcards or postcards written in pencil. Encryption is being increasingly required in areas like banking and health care. New laws in Nevada and Massachusetts (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. As the use of encryption grows in areas like

[10] Janna Quitney Anderson & Lee Rainie, The Future of Cloud Computing. Pew Internet & American Life Project, June 11, 2010, http://www.pewinternet.org/Reports/2010/The-future-of-cloud-computing/Main-Findings.aspx?view=all

> these, it will become difficult for attorneys to demonstrate that confidential client data needs lesser protection.[11]

The article also provides a list of nine potential e-mail risk areas, including: confidentiality, authenticity, integrity, misdirection or forwarding, permanence (wanted e-mail may become lost and unwanted e-mail may remain accessible even if deleted), and malware. The article further provides guidance for protecting e-mail by stating:

> In addition to complying with any legal requirements that apply, the most prudent approach to the ethical duty of protecting confidentiality is to have an express understanding with clients about the nature of communications that will be (and will not be) sent by e-mail and whether or not encryption and other security measures will be utilized.
>
> It has now reached the point (or at least is reaching it) where most attorneys should have encryption available for use in appropriate circumstances.[12]

Compounding the general security concerns for e-mail is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

The Committee further notes that this issue was addressed by the District of Columbia Bar in Opinion 281 (Feb. 18, 1998) ("Transmission of Confidential Information by Electronic Mail"), which concluded that, "In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security."

The Committee concluded, and this Committee agrees, that the use of unencrypted electronic mail is not, by itself, a violation of the Rules of Professional Conduct, in particular Rule 1.6 ("Confidentiality of Information").

> Thus, we hold that the mere use of electronic communication is not a violation of Rule 1.6 absent special factors. We recognize that as to any confidential communication, the sensitivity of the contents of the communication and/or the circumstances of the transmission may, in specific instances, dictate higher levels of security. Thus, it may be necessary in certain circumstances to use extraordinary means to protect client confidences. To give an obvious example, a lawyer representing an associate in a dispute with the associate's law firm could very easily violate Rule 1.6 by sending a fax concerning the dispute to the law firm's mail room if that message contained client confidential

---

[11] David G. Ries, Esquire, "Legal Ethics in the Cloud: Avoiding the Storms," course handbook, *Cloud Computing 2011: Cut Through the Fluff & Tackle the Critical Stuff* (June 2011) (internal citations omitted).

[12] *Id*.

> information. It is reasonable to suppose that employees of the firm, other lawyer employed at the firm, indeed firm management, could very well inadvertently see such a fax and learn of its contents concerning the associate's dispute with the law firm. Thus, what may ordinarily be permissible—the transmission of confidential information by facsimile—may not be permissible in a particularly factual context.
>
> By the same analysis, what may ordinarily be permissible – the use of unencrypted electronic transmission – may not be acceptable in the context of a particularly heightened degree of concern or in a particular set of facts. But with that exception, we find that a lawyer takes reasonable steps to protect his client's confidence when he uses unencrypted electronically transmitted messages.

E. Opinions From Other Ethics Committees

Other Ethics Committees have reached conclusions similar in substance to those in this Opinion. Generally, the consensus is that, while "cloud computing" is permissible, lawyers should proceed with caution because they have an ethical duty to protect sensitive client data. In service to that essential duty, and in order to meet the standard of reasonable care, other Committees have determined that attorneys must (1) include terms in any agreement with the provider that require the provider to preserve the confidentiality and security of the data, and (2) be knowledgeable about how providers will handle the data entrusted to them. Some Committees have also raised ethical concerns regarding confidentiality issues with third-party access or general electronic transmission (*e.g.,* web-based email) and these conclusions are consistent with opinions about emergent emergent "cloud computing" technologies.

The American Bar Association Standing Committee on Ethics and Professional Responsibility has not yet issued a formal opinion on "cloud computing." However, the ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies, published an "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology" (Sept. 20, 2010) and considered some of the concerns and ethical implications of using "the cloud." The Working Group found that potential confidentiality problems involved with "cloud computing" include:

- Storage in countries with less legal protection for data;
- Unclear policies regarding data ownership;
- Failure to adequately back up data;
- Unclear policies for data breach notice;
- Insufficient encryption;
- Unclear data destruction policies;
- Bankruptcy;
- Protocol for a change of cloud providers;
- Disgruntled/dishonest insiders;
- Hackers;
- Technical failures;
- Server crashes;
- Viruses;

- Data corruption;
- Data destruction;
- Business interruption (*e.g.*, weather, accident, terrorism); and,
- Absolute loss (*i.e.*, natural or man-made disasters that destroy everything).

Id. The Working Group also stated, "[f]orms of technology other than 'cloud computing' can produce just as many confidentiality-related concerns, such as when laptops, flash drives, and smart phones are lost or stolen." *Id*. Among the precautions the Commission is considering recommending are:

- Physical protection for devices (*e.g.*, laptops) or methods for remotely deleting data from lost or stolen devices;
- Strong passwords;
- Purging data from replaced devices (*e.g.*, computers, smart phones, and copiers with scanners);
- Safeguards against malware (*e.g.*, virus and spyware protection);
- Firewalls to prevent unauthorized access;
- Frequent backups of data;
- Updating to operating systems with the latest security protections;
- Configuring software and network settings to minimize security risks;
- Encrypting sensitive information;
- Identifying or eliminating metadata from electronic documents; and
- Avoiding public Wi-Fi when transmitting confidential information (*e.g.*, sending an email to a client).

Id. Additionally, the ABA Commission on Ethics 20/20 has drafted a proposal to amend, *inter alia*, Model Rule 1.0 ("Terminology"), Model Rule 1.1 ("Competence"), and Model Rule 1.6 ("Duty of Confidentiality") to account for confidentiality concerns with the use of technology, in particular confidential information stored in an electronic format. Among the proposed amendments (insertions underlined, deletions ~~struck through~~):

> Rule 1.1 ("Competence") Comment [6] ("Maintaining Competence"): "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 technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."
>
> Rule 1.6(c) ("Duty of Confidentiality"): "A lawyer shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client."
>
> Rule 1.6 ("Duty of Confidentiality") Comment [16] ("Acting Competently to Preserve Confidentiality"): "Paragraph (c) requires a ~~A~~ lawyer ~~must~~ to act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision or monitoring. See Rules 1.1, 5.1, and 5.3. Factors to

> be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, and the cost of employing additional safeguards. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

In Formal Opinion No. 99-413 (March 10, 1999), the ABA Standing Committee on Ethics and Professional Responsibility determined that using e-mail for professional correspondence is acceptable. Ultimately, it concluded that unencrypted e-mail poses no greater risks than other communication modes commonly relied upon. As the Committee reasoned, "The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of the law." *Id*.

Also relevant is ABA Formal Opinion 08-451 (August 5, 2008), which concluded that the ABA Model Rules generally allow for outsourcing of legal and non-legal support services if the outsourcing attorney ensures compliance with competency, confidentiality, and supervision. The Committee stated that an attorney has a supervisory obligation to ensure compliance with professional ethics even if the attorney's affiliation with the other lawyer or nonlawyer is indirect. An attorney is therefore obligated to ensure that any service provider complies with confidentiality standards. The Committee advised attorneys to utilize written confidentiality agreements and to verify that the provider does not also work for an adversary.

The Alabama State Bar Office of General Council Disciplinary Commission issued Ethics Opinion 2010-02, concluding that an attorney must exercise reasonable care in storing client files, which includes becoming knowledgeable about a provider's storage and security and ensuring that the provider will abide by a confidentiality agreement. Lawyers should stay on top of emerging technology to ensure security is safeguarded. Attorneys may also need to back up electronic data to protect against technical or physical impairment, and install firewalls and intrusion detection software.

State Bar of Arizona Ethics Opinion 09-04 (Dec. 2009) stated that an attorney should take reasonable precautions to protect the security and confidentiality of data, precautions which are satisfied when data is accessible exclusively through a Secure Sockets Layer ("SSL") encrypted connection and at least one other password was used to protect each document on the system. The Opinion further stated, "It is important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult experts in the field." *Id*. Also, lawyers should ensure reasonable protection through a periodic review of security as new technologies emerge.

The California State Bar Standing Committee on Professional Responsibility and Conduct concluded in its Formal Opinion 2010-179 that an attorney using public wireless connections to conduct research and send e-mails should use precautions, such as personal firewalls and encrypting files and transmissions, or else risk violating his or her confidentiality and competence obligations. Some highly sensitive matters may necessitate discussing the use of

public wireless connections with the client or in the alternative avoiding their use altogether. Appropriately secure personal connections meet a lawyer's professional obligations. Ultimately, the Committee found that attorneys should (1) use technology in conjunction with appropriate measures to protect client confidentiality, (2) tailor such measures to each unique type of technology, and (3) stay abreast of technological advances to ensure those measures remain sufficient.

The Florida Bar Standing Committee on Professional Ethics, in Opinion 06-1 (April 10, 2006), concluded that lawyers may utilize electronic filing provided that attorneys "take reasonable precautions to ensure confidentiality of client information, particularly if the lawyer relies on third parties to convert and store paper documents to electronic records." *Id*.

Illinois State Bar Association Ethics Opinion 10-01 (July 2009) stated that "[a] law firm's use of an off-site network administrator to assist in the operation of its law practice will not violate the Illinois Rules of Professional Conduct regarding the confidentiality of client information if the law firm makes reasonable efforts to ensure the protection of confidential client information."[13]

The Maine Board of Overseers of the Bar Professional Ethics Commission adopted Opinion 194 (June 30, 2008) in which it stated that attorneys may use third-party electronic back-up and transcription services so long as appropriate safeguards are taken, including "reasonable efforts to prevent the disclosure of confidential information," and at minimum an agreement with the vendor that contains "a legally enforceable obligation to maintain the confidentiality of the client data involved." *Id*.

Of note, the Maine Ethics Commission, in a footnote, suggests in Opinion 194 that the federal Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rule 45 C.F.R. Subpart 164.314(a)(2) provide a good medical field example of contract requirements between medical professionals and third party service providers ("business associates") that handle confidential patient information. SLAs that reflect these or similar requirements may be advisable for lawyers who use cloud services.

45 C.F.R. Subpart 164.314(a)(2)(i) states:

> The contract between a covered entity and a business associate must provide that the business associate will:
>
> (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

[13] Mark Mathewson, *New ISBA Ethics Opinion Re: Confidentiality and Third-Party Tech Vendors*, Illinois Lawyer Now, July 24, 2009, available at http://www.illinoislawyernow.com/2009/07/24/new-isba-ethics-opinion-re-confidentiality-and-third-party-tech-vendors/

> (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
>
> (C) Report to the covered entity any security incident of which it becomes aware;
>
> (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

Massachusetts Bar Association Ethics Opinion 05-04 (March 3, 2005) addressed ethical concerns surrounding a computer support vendor's access to a firm's computers containing confidential client information. The committee concluded that a lawyer may provide a third-party vendor with access to confidential client information to support and maintain a firm's software. Clients have "impliedly authorized" lawyers to make confidential information accessible to vendors "pursuant to Rule 1.6(a) in order to permit the firm to provide representation to its clients." *Id.* Lawyers must "make reasonable efforts to ensure" a vendor's conduct comports with professional obligations. *Id*.

The State Bar of Nevada Standing Committee on Ethics and Professional Responsibility issued Formal Opinion No. 33 (Feb. 9, 2006) in which it stated, "an attorney may use an outside agency to store confidential information in electronic form, and on hardware located outside an attorney's direct supervision and control, so long as the attorney observed the usual obligations applicable to such arrangements for third party storage services." *Id*. Providers should, as part of the service agreement, safeguard confidentiality and prevent unauthorized access to data. The Committee determined that an attorney does not violate ethical standards by using third-party storage, even if a breach occurs, so long as he or she acts competently and reasonably in protecting information.

The New Jersey State Bar Association Advisory Committee on Professional Ethics issued Opinion 701 (April 2006) in which it concluded that, when using electronic filing systems, attorneys must safeguard client confidentiality by exercising "sound professional judgment" and reasonable care against unauthorized access, employing reasonably available technology. *Id*. Attorneys should obligate outside vendors, through "contract, professional standards, or otherwise," to safeguard confidential information. *Id*. The Committee recognized that Internet service providers often have better security than a firm would, so information is not necessarily safer when it is stored on a firm's local server. The Committee also noted that a strict guarantee of invulnerability is impossible in any method of file maintenance, even in paper document filing, since a burglar could conceivably break into a file room or a thief could steal mail.

The New York State Bar Association Committee on Professional Ethics concluded in Opinion 842 (Sept. 10, 2010) that the reasonable care standard for confidentiality should be maintained for online data storage and a lawyer is required to stay abreast of technology advances to ensure protection. Reasonable care may include: (1) obligating the provider to preserve confidentiality and security and to notify the attorney if served with process to produce client information, (2) making sure the provider has adequate security measures, policies, and recoverability methods,

and (3) guarding against "reasonably foreseeable" data infiltration by using available technology. *Id*.

The North Carolina State Bar Ethics Committee has addressed the issue of "cloud computing" directly, and this Opinion adopts in large part the recommendations of this Committee. Proposed Formal Opinion 6 (April 21, 2011) concluded that "a law firm may use SaaS[14] if reasonable care is taken effectively to minimize the risks to the disclosure of confidential information and to the security of client information and client files." *Id*. The Committee reasoned that North Carolina Rules of Professional Conduct do not require a specific mode of protection for client information or prohibit using vendors who may handle confidential information, but they do require reasonable care in determining the best method of representation while preserving client data integrity. Further, the Committee determined that lawyers "must protect against security weaknesses unique to the Internet, particularly 'end-user' vulnerabilities found in the lawyer's own law office." *Id*.

The Committee's minimum requirements for reasonable care in Proposed Formal Opinion 6 included:[15]

- An agreement on how confidential client information will be handled in keeping with the lawyer's professional responsibilities must be included in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement that states that the employees at the vendor's data center are agents of the law firm and have a fiduciary responsibility to protect confidential client information and client property;

- The agreement with the vendor must specify that firm's data will be hosted only within a specified geographic area. If by agreement the data is hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and the state of North Carolina;

- If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm must have a method for retrieving the data, the data must be available in a non-proprietary format that is compatible with other firm software or the firm must have access to the vendor's software or source code, and data hosted by the vendor or third party data hosting company must be destroyed or returned promptly;

[14] SaaS, as stated above, stands for Software-as-a-Service and is a type of "cloud computing."

[15] The Committee emphasized that these are minimum requirements, and, because risks constantly evolve, "due diligence and perpetual education as to the security risks of SaaS are required." Consequently, lawyers may need security consultants to assess whether additional measures are necessary.

- The law firm must be able get data "off" the vendor's or third party data hosting company's servers for lawyers' own use or in-house backup offline; and,

- Employees of the firm who use SaaS should receive training on and be required to abide by end-user security measures including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

In Opinion 99-03 (June 21, 1999), the **State Bar Association of North Dakota** Ethics Committee determined that attorneys are permitted to use online data backup services protected by confidential passwords. Two separate confidentiality issues that the Committee identified are, (1) transmission of data over the internet, and (2) the storage of electronic data. The Committee concluded that the transmission of data and the use of online data backup services are permissible provided that lawyers ensure adequate security, including limiting access only to authorized personnel and requiring passwords.

Vermont Bar Association Advisory Ethics Opinion 2003-03 concluded that lawyers can use third-party vendors as consultants for confidential client data-base recovery if the vendor fully understands and embraces the clearly communicated confidentiality rules. Lawyers should determine whether contractors have sufficient safety measures to protect information. A significant breach obligates a lawyer to disclose the breach to the client.

Virginia State Bar Ethics Counsel Legal Ethics Opinion 1818 (Sept. 30, 2005) stated that lawyers using third party technical assistance and support for electronic storage should adhere to Virginia Rule of Professional Conduct 1.6(b)(6)[16], requiring "due care" in selecting the service provider and keeping the information confidential. *Id*.

These opinions have offered compelling rationales for concluding that using vendors for software, service, and information transmission and storage is permissible so long as attorneys meet the existing reasonable care standard under the applicable Rules of Professional Conduct, and are flexible in contemplating the steps that are required for reasonable care as technology changes.

IV. Conclusion

The use of "cloud computing," and electronic devices such as cell phones that take advantage of cloud services, is a growing trend in many industries, including law. Firms may be eager to capitalize on cloud services in an effort to promote mobility, flexibility, organization and efficiency, reduce costs, and enable lawyers to focus more on legal, rather than technical and

[16] Virginia Rule of Professional Conduct 1.6(b) states in relevant part:

> To the extent a lawyer reasonably believes necessary, the lawyer may reveal:
>
> (6) information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential.

administrative, issues. However, lawyers must be conscientious about maintaining traditional confidentiality, competence, and supervisory standards.

This Committee concludes that the Pennsylvania Rules of Professional Conduct require attorneys to make reasonable efforts to meet their obligations to ensure client confidentiality, and confirm that any third-party service provider is likewise obligated.

Accordingly, as outlined above, this Committee concludes that, under the Pennsylvania Rules of Professional Conduct an attorney may store confidential material in "the cloud." Because the need to maintain confidentiality is crucial to the attorney-client relationship, attorneys using "cloud" software or services must take appropriate measures to protect confidential electronic communications and information. In addition, attorneys may use email but must, under appropriate circumstances, take additional precautions to assure client confidentiality.