American Bar Association
38th Annual Forum on Franchising

ETHICAL RISKS IN CYBERSPACE

Regina B. Amolsch
Plave Koch PLC
Reston, Virginia

and

Trishanda Treadwell
Parker, Hudson, Rainer & Dobbs LLP
Atlanta, Georgia

October 14 – 16, 2015
New Orleans, LA

Table of Contents

ETHICAL RISKS IN CYBERSPACE

I. INTRODUCTION

> We are living in the midst of a social, economic, and technological revolution. How we communicate, socialize, spend leisure time, and conduct business has moved onto the Internet. The Internet has in turn moved into our phones, into devices spreading around our homes and cities, and into the factories that power the industrial economy. The resulting explosion of data and discovery is changing our world.[1]

Like the rest of the world, franchisors, franchisees, and their counsel are increasingly using portable devices and storing data in "the cloud." But practicing law in cyberspace and using cloud storage may trigger unappreciated ethical risks, including threats to the attorney-client privilege, potential violations of the Rules of Professional Responsibility, and even violations of federal and state laws, including the Foreign Corrupt Practices Act, the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act.

As discussed in great detail below, many states have issued ethics opinions on attorneys' obligations when undertaking the use of the cloud. The most recent state ethics opinion on this issue is the comprehensive analysis from Wisconsin. The opinion describes cloud computing as "'a fancy way of saying stuff's not on your computer' . . . [and] includes the processing, transmission, and storage of the client's information using shared computer facilities or remote servers owned or leased by a third-party service provider. These facilities and services are accessed over the Internet by the lawyer's networked devices such as computers, tablets, and smart phones."[2]

Importantly, the lesson to be learned from the normalized use of cloud computing is that lawyers have to be aware of the technology and future advancements to comply with their ethical obligation to protect client confidentiality and data. The excuse that an attorney, particularly lead counsel, is just not technologically savvy does not comport with that ethical obligation. Moreover, the increased efficiency and decreased cost of cloud computing is likely to make it a necessity from the client's perspective, regardless of the potential increased security risk created by inserting a third-party provider between counsel and the client's data. Counsel should prepare to invest in and integrate into their practices cloud-computing providers, just as in previous years attorneys had to adjust to offsite storage (*i.e.*, Iron Mountain), electronic document management systems, and the use of facsimiles and email to communicate with clients.

This paper will analyze the recent trends and types of electronic data storage and cloud computing and the ethical and legal obligations of counsel. Finally, this paper will provide strategies for how to meet those ethical and legal obligations.

---

[1] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES PRESERVING VALUES at i (May 1, 2014).

[2] Wis. Formal Ethics Op. EF-15-01 at 2 (Mar. 23, 2015) (quoting Pa. Bar Ass'n Comm. on Legal Ethics and Professional Responsibility Formal Ethics Opinion 2011-200 at 1 (2011) (quoting Quinn Norton, *Byte Rights*, MAXIMUM PC, September 2010, at 12)).

II. RECENT TRENDS IN DATA STORAGE AND USE OF PORTABLE DEVICES

The vast amount of data required to be stored electronically has catapulted most law firms and individuals beyond the storage capacity of a computer's main drive or a portable compact disc. External hard drives, flash drives, and internet-based cloud storage all provide data storage alternatives with minimal cost and even less effort than physical storage or use of additional computers. The kind of electronic data storage a firm uses depends on the firm size, technology budget, clientele, and technical expertise, but all firms are moving away from the days of warehouses of bankers boxes, which held (and continue to hold) their own risks. While the focus of this paper is on data storage in the cloud, it is important to place that type of storage in context and to assess the alternative forms of storage.

A. Physical Document Storage

For every twenty-page hard copy original document, there may be ten electronic drafts and hundreds of relevant emails. For every hard copy letter sent through the mail, there are likely five hundred emails exchanged. To store that information in hard copy would require not only loss of the metadata information in the document but also costs and space for printing and storing those documents. Additionally, given that so much data is created and shared electronically without the need to be printed for its primary use, the physical storage of documents is on the decline for third party providers like Iron Mountain.[3] As an alternative, law firms are storing fewer hard copy documents internally and externally, opting instead for scanning and electronic storage.

Physical document storage is costly compared to electronic storage of the same amount and type of documents, so moving towards electronic storage is not a question at many law firms because it is an easy expense line item to reduce.

Ethical risks associated with physical document storage are generally limited to ensuring that the documents are secure both from unauthorized third-party access and from acts of nature. Lawyers should have client documents and confidential information stored and out-of-sight in cabinets, drawers, or other file storage rooms that have controlled access. For off-site providers, counsel should make certain that the provider is subject to confidentiality requirements, keeps the documents secured from unauthorized access, has the documents organized for adequate retrieval, and has sufficient insurance in the event of an unauthorized physical intrusion or unanticipated destruction of documents due to an act of nature. In addition, counsel should have a document retention policy, understood and acknowledged by each client, permitting the return or destruction of hard copy documents after a certain period of time.

B. Portable Storage Devices

Portable storage devices such as tablets, laptop computers, external hard drives, flash drives, and storage discs all provide basic electronic storage capacity with little investment in technology. Even the least technology-savvy attorney has some experience with saving documents on a computer or on a disc (floppy, compact disc (CD), or digital versatile disc (DVD)). The ubiquitous and casual use of these electronic storage media seems innocuous, but

[3] *See* Barbara Noverini, *Even as a REIT, Iron Mountain's Narrow Economic Moat Remains in Storage*, Analyst Note, June 8, 2015, MorningStar.com, http://analysisreport.morningstar.com/stock/research?t=IRM&region=USA&culture=en-US&productcode=MLE.

the loss or theft of these devices can create ethical risks because they are easily misplaced or stolen and the data stored on them is less likely to have been encrypted or password-protected. CDs and DVDs are also easily damaged, so they should not be used without maintaining the original data in a more protected format. Quickly replacing discs are USB flash drives or "thumb drives," which generally hold significantly more data and are sturdier and more convenient.

These types of devices present a dual risk. First, because information (and large amounts of information) is so easy to download and transport on thumb drive, lawyers will use them. They often contain copies of information stored elsewhere, so users may be less concerned about loss of a small, easily-pocketed thumb drive. However, the storage capacity presents an inherent risk simply because of the significant amount of data that could be lost or exposed in one fell swoop. Also, these small drives are often left unprotected, exposing counsel and their firms to possible ethical violations for failing to maintain the confidentiality of client data. Firms should require lawyers to password-protect any data saved to a thumb drive for use outside of the office and may want to consider limiting the use of thumb drives to firm-issued encrypted thumb drives. To avoid loss of data, counsel should be certain to maintain a back-up of client data stored on a disc or thumb drive.

External hard drives provide an even greater storage volume and are also easily portable. Because external hard drives are more often used for backing-up or copying electronic data, they are more likely to be password-protected or encrypted. Counsel should still be aware of the risks that sensitive client information can be lost.

C. Magnetic Tape Data Storage

A standard form of back-up and archival storage, particularly for high-density data storage, is magnetic tape. Most businesses, including law firms, do not use magnetic tape storage because the transfer and retrieval of the data are more difficult. The use of tape has generally been superseded by the rise of cloud storage and portable storage devices. Given these factors, magnetic tape use is generally now limited to large-scale storage in data storage centers and as back-up or temporary storage for high-density information, like camera footage, which the data owners are less likely to require immediate access or retrieval.[4]

D. Local Networks

Most attorneys and law firms use a private, local area network to connect firm computers to shared data on internal private servers managed and controlled by the firm. Generally, these networks will require a login or password. As a result, information contained in the network has some basic protection provided users log off, do not leave the network open and unattended on their computers, employ strong passwords, and maintain firewall, virus, and other network protections. A benefit to servers running local area networks is that they can store more data than any individual computer and can maintain shared data to free up individual computer space. Local area networks require an investment in equipment, maintenance, and qualified technical support.

[4] *See, e.g., Disability Rights Council of Greater Wash. v. Wash. Metro. Transit Auth.*, 242 F.R.D. 139, 145 (D.D.C. 2007) (requiring party to conduct expensive review of back-up media because it contained the only copy of electronically stored information).

E. Cloud Storage

The newest storage model is generically referred to as "cloud" storage, which can mean a great many things.[5] One simple form of cloud storage is through an email provider, like Gmail. The information stored in email is accessed via the Internet, which is, at its most basic, an area network with an "area" that covers the globe. As one of the most convenient forms of modern communication and electronic storage, emails are rife with ethical risks because they easily include or attach attorney-client privileged document, work product, or other confidential information. Email is also susceptible to viruses, hacking, phishing, and erroneously delivered messages.

Similar to email, most electronic applications on computers, smartphones, and tablets are cloud-based because third parties provide the software applications that users access via the Internet. Individuals and law firms, depending on the size, may use these software-as-a-service ("SaaS") cloud-based programs for official or unofficial data storage (*e.g.*, Dropbox, Hightail). These programs permit users to view and save a document from a desktop computer and also view and edit that document from mobile devices or other computers by logging into the program. The cloud also significantly reduces the physical security concerns of damage to or loss or theft of hard copy documents, discs, and thumb drives.

A firm may also use a privately managed cloud-based storage system provided by a third party, *i.e.*, Infrastructure as a Service ("IaaS") model. Under this version of cloud-based storage, a firm or other organization does not have to maintain its own network servers and eliminates the cost of storing and maintaining them. Instead, the firm "rents" a third party's servers, which could be maintained anywhere, and allows the firm to keep its *entire* infrastructure off-site, or "in the cloud," and accessible from anywhere with Internet access. Modern IaaS environments can provide more than data storage; they can run all of a law firm's technology functions, reducing the need for and cost of IT hardware, software, and personnel to only what is necessary to manage the connection and set users up on the system. It is this significant cost-reduction that is driving law firms to become entirely cloud-based. Moreover, the use of the cloud is on a trajectory unlikely to be halted, especially not by ethical, confidentiality, or privacy concerns. At this point, the use of the electronic data is akin to driving cars. Motor vehicle crashes might continue to be a leading cause of death in many age groups, but no one will relinquish the benefits and convenience of personal car travel based on that risk. Similarly, regardless of the risks presented by the use of electronic data and reliance on the cloud, the White House estimated that, in 2013, four *zettabytes* of data were generated worldwide, and that number is likely to increase ten-fold in the next five years.[6]

---

[5] Jody R. Westby, *Cybersecurity & Law Firms: A Business Risk*, 39 No. 4 LAW. PRAC. MAG. (July/Aug. 2013), *available at* http://www.americanbar.org/ publications/law_practice_magazine, select the 2013 archives to access the article.

[6] BIG DATA, *supra* note 1, at 2 (defining "zettabyte" as 1,000,000,000,000,000,000,000 units of information; one zettabyte would equal the data held if every person in the United States took a digital photo ever second of every day for over a month). *See also* http://gizmodo.com/5557676/how-much-money-would-a-yottabyte-hard-drive-cost (last accessed July 19, 2015) (explaining a "terabyte" could be 200,000 photos or mp3 songs, while a "zettabyte" of data would fill 1,000 four-story datacenters each the size of a city block, or about twenty percent of Manhattan, NY).

III. SOURCES OF ETHICAL OBLIGATIONS REGARDING CLIENT INFORMATION AND WORK PRODUCT

A. Model Rules of Professional Responsibility and ABA Commission on Ethics 20/20

For as long as there have been lawyers, there have been articulated ethical standards governing the duties and obligations lawyers have in guarding, safekeeping and maintaining their clients' secrets, confidences, and property. The ABA's Model Rules of Professional Responsibility (the "Model Rules")[7] have long established the model ethical standards in this arena. Most specifically at issue are Rules 1.1—Duty of Competence; 1.4—Communications with Clients; 1.6—Duty of Confidentiality; 1.15—Duty to Safeguard Client Property; 1.16—Terminating Representation; 5.1—Responsibilities of a Partner or Supervisory Lawyer; 5.2—Responsibilities of a Subordinate Lawyer; and 5.3—Responsibilities Regarding Nonlawyer Assistance. In summary, these Model Rules require that a lawyer: provide competent representation to the client; promptly inform and reasonably communicate with the client so the client may make informed decisions; keep client secrets and make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client; appropriately safeguard client property; return papers and property to which the client is entitled; and reasonably ensure that lawyers, legal assistants and service providers are familiar with and acting in matter consistent with the Model Rules.

But just as technology never stands still, neither do the ABA's efforts to ensure that its model ethical standards keep pace (when possible) with the reality that the modern law practice is one increasingly based in (or at least making considerable use of) cyberspace. The ABA's first foray into this arena came in 1986 when the ABA Committee on Lawyers' Responsibility for Client Protection issued the report *Lawyers on Line: Ethical Perspectives in the Use of Telecomputer Communication*. That report focused on the technology changes at the forefront at that time – notably email. The report cautioned against the use of email without first obtaining client approval or being reasonably assured, after competently investigating the email system, that the system was indeed secure. Though the report stopped short of actually requiring the use of encrypted email, there was enough concern that the ABA issued a subsequent opinion in 1999 addressing this question. ABA Formal Opinion No. 99-413 stated that encryption was not generally an ethical requirement, given the reasonable expectation of privacy inherent in the use of email.[8] The opinion did recognize, however, that there might be extraordinary cases involving particularly sensitive information that might require extraordinary security precautions. Notably, even in 1999, the Committee eschewed a "one size fits all" approach to addressing the ethical concerns governing the use of technology and instead defaulted to the overarching ethical requirement that a lawyer's duty to act reasonably and competently is context dependent.

Following up on Opinion 99-413, the ABA, through its Ethics 2000 Commission added two comments to Model Rule 1.6—Confidentiality of Information. What was then Comment 15 reiterated a lawyer's affirmative duty to protect the client's confidential information against inadvertent or unauthorized disclosure by the lawyer or those working with the lawyer; and then-

[7] AMERICAN BAR ASSOCIATION, MODEL RULES OF PROF'L CONDUCT (2013), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html (hereinafter "MODEL RULES").

[8] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999).

Comment 16 admonished the lawyer to be wary of the harm which might flow from such a disclosure and to consider whether circumstances call for enhanced security precautions. The 2000 Commission likewise stopped short of requiring the use of encrypted email.[9]

Most recently (and most relevant for this paper), in 2010, the ABA Commission on Ethics 20/20[10] (the "Commission")—specifically through the Working Group on the Implications of New Technologies (the "Working Group")—began examining the existing ethical rules and concluded that it was time for a periodic reexamination of the prevailing ethical framework governing the duties and obligations that lawyers have in guarding, safekeeping and maintaining their clients' secrets, confidences, and property.[11]

On September 20, 2010, the Commission released a formal request for comments on "what guidance to offer to lawyers who want to ensure that their use of technology complies with their ethical obligations to protect clients' confidential information."[12] The Commission's Working Group was particularly interested in the evolving model ethical standards governing a lawyer's use of "cloud computing." As defined by the National Institute of Standards and Technology, "[c]loud computing" is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[13] The Oxford Dictionary defines "cloud computing" as "[t]he practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer."[14] In simpler terms, however, if you are electronically storing client data anywhere other than on your hard drive or on a server located in your office or at your house, your data is being stored "in the cloud"." This includes data electronically stored on desktop and portable computers as well as on tablets and smartphones. As noted earlier, cloud computing has very aptly been described as "a fancy way of saying stuff's not on your computer."[15] Additionally, even if a lawyer does not

---

[9] ABA Ethics 2000 Comm., *Report on the Model Rules of Professional Conduct*, http://www.americanbar.org/groups/professional_responsibility/policy/ethics_2000_commission/e2k_report_home.html (Ethics 2000 Commission's changes to the Model Rules).

[10] ABA Comm. on Ethics 20/20, http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html (last visited June 26, 2015).

[11] *See also* Lance J. Rogers, *Ethics 20/20 Commission Invites Comments On Issues Raised by Growing Use of Internet*, 26 LAW. MAN. PROF. CONDUCT 586 (Sept. 29, 2010), *available at* http://www.americanbar.org/content/dam/aba/migrated/2011_build/ethics_2020/law_man_9_29_2010.authcheckdam.pdf

[12] ABA Comm. on Ethics 20/20, *For Comment: Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology* 1 (Sept. 20, 2010), *available at* http://www.americanbar.org/content/dam/aba/migrated/2011_build/ethics_2020/clientconfidentiality_issuespaper.authcheckdam.pdf.

[13] PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., THE NIST DEFINITION OF CLOUD COMPUTING 2, Spec. Publ'n. 800-145 (Sept. 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[14] Oxford Dictionaries. Oxford University Press, http://www.oxforddictionaries.com/us/definition/american_english/cloud-computing (accessed June 29, 2015).

[15] Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (quoting Quinn Norton, *Byte Rights*, MAXIMUM PC, September 2010, at 12), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf.

rely on cloud storage solutions, given the prevalence of electronic communications and use of online services in the digital age, the same ethical considerations should be evaluated in connection with electronic communications and transmissions of data among lawyers, their clients, service providers and other third parties.

By way of example, common cloud computing solutions include data storage services and applications (such as Dropbox, Crashplan, Amazon Cloud, and Microsoft Cloud); Internet-based email providers (such as Gmail, Yahoo, and Apple's iCloud); and software licensing and delivery models—commonly referred to "Software as a service" or "Saas"—through which software solutions are centrally hosted on offsite servers and then licensed for usage on a subscription basis (examples include MyCase, Clio, and Time Matters Cloud).

After reviewing the formal comments submitted in response to its September 2010 request, on September 19, 2011, the Commission adopted a resolution entitled "Technology and Confidentiality" in which it proposed certain changes to the Model Rules, some of which directly implicated the ethical considerations of cloud computing.[16] The ABA House of Delegates adopted the proposed Amendments to the Model Rules of Professional Conduct in August of 2012 (the "2012 Amendments"). Below, the authors discuss the individual Model Rules relevant to the ethical issues of cloud computing, as well as the additions and other changes (if any) to the Rules, either directly in the text of the Rules or in the Comments to these Rules, that were implemented as part of the 2012 Amendments. With the permission of the ABA, included as Attachment A to this paper is a copy of the portions of the 2012 Amendments that relate to the Model Rules discussed below.

1. Model Rule 1.1: Competence

A cornerstone of legal ethics is lawyer competency, which the Model Rules sets forth in simple terms. Model Rule 1.1 provides that "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[17] Comment 1 augments Rule 1.1, explaining that: "In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question."[18] Comment 1 makes clear, therefore, that the duty of competence is broad enough to encompass just about every aspect of the practice of law.

Given the "bewildering pace of technological change," however, the Commission believed it important to update the Model Rules to make explicit that a lawyer's duty of competence necessarily "requires the lawyer to stay abreast of changes in the law and its

[16] ABA Comm. on Ethics 20/20, Resolution (Sept. 19, 2011), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20110919_ethics_20_20_technology_and_confidentiality_revised_resolution_and_report_posting.authcheckdam.pdf.

[17] MODEL RULES, *supra* note 7, R. 1.1.

[18] *Id.* R. 1.1 cmt. 1.

practice, includ[ing] understanding relevant technology's benefits and risks."[19] To reflect this important clarification that competence requires being, and continuing to become, reasonably informed about emerging technologies such as cloud computing, the Commission in the 2012 Amendment supplemented Comment 8 to Rule 1.1.[20] so that it now reads:

> 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.[21]

Thus, while the 2012 Amendment created no new ethical obligation, the Commission aptly described that the 2012 Amendment "emphasizes that a lawyer should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent in a digital age."[22] Ethical lawyers, therefore, have both a current and ongoing obligation to remain aware of technological developments, as well as how those changes impact their ethical obligations.

2. Model Rule 1.4: Client Communication

The second Model Rule that we address relating to cloud computing is Model Rule 1.4 regarding communications with clients. Rule 1.4 reads as follows:

> (a) A lawyer shall:
>
> (1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;
>
> (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;
>
> (3) keep the client reasonably informed about the status of the matter;
>
> (4) promptly comply with reasonable requests for information; and
>
> (5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects

[19] ABA Comm. on Ethics 20/20, *Introduction and Overview* 8 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introduction_and_overview_report.authcheckdam.pdf (hereinafter "ABA 20/20 INTRODUCTION").

[20] Comment 8 was numbered as Comment 6 before the 2012 Amendment. Two additional comments, unrelated to cloud computing issues, were added, causing the numbering to change.

[21] MODEL RULES, *supra* note 7, R. 1.1 cmt. 8 (emphasis added).

[22] ABA 20/20 INTRODUCTION, *supra* note 19, at 8.

> assistance not permitted by the Rules of Professional Conduct or other law.
>
> (b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.[23]

Although it is not altogether clear from Rule 1.4 itself that it impacts a lawyer's initial use and choice to utilize a cloud computing solution, it does seem clear that this Rule requires lawyers to inform their clients of any actual or potential security breach resulting in the actual or potential loss of confidential information.[24] In fact, the 2012 Amendments left Rule 1.4 and its Comments intact, save for updating the last sentence of Comment 4 to read: "A lawyer should promptly respond to or acknowledge client communications."[25] This language replaced the somewhat anachronistic admonition that "[c]lient telephone calls should be promptly returned or acknowledged."

As reports of electronic data breaches and other cyber threats have become almost routine, additional questions have arisen as to whether legal ethical standards may render it necessary (or at least prudent) for a lawyer to inform clients about, or possibly even obtain client consent for, the lawyer's use of cloud computing and related cyber technologies in performing the legal representation. We discuss this issue further in Parts III.C. and V.B.

3. Model Rule 1.6: Confidentiality of Information

One of the Model Rules most directly and clearly implicated in cloud computing is Rule 1.6 regarding confidentiality. In Rule 1.6, paragraph (a) sets forth the general admonition against "reveal[ing] information relating to the representation of a client unless the client gives informed consent."[26] Though the duty of confidentiality is one of the bedrock ethical principles imposed upon lawyers, the Commission nevertheless "recognize[d] that lawyers cannot guarantee electronic security any more than lawyers can guarantee the physical security of documents stored in a file cabinet or offsite storage facility."[27] Accordingly, Rule 1.6 was substantively revised in the 2012 Amendments to extend the reasonableness standard into the cyber realm. Three substantive changes were made—one directly in the text of Rule 1.6 and two in Comments 18 and 19, all of which provide important discussions on safeguarding information both when the lawyer is holding the information and when the lawyer is transmitting the information.

---

[23] MODEL RULES, *supra* note 7, R. 1.4.

[24] For purposes of discussing the Model Rules, we are not addressing in this paper, the various laws and regulations regarding data breach and notification requirements. As discussed in some state ethics opinions, those laws and regulations are beyond the scope of the state ethics rules themselves, but may impose additional obligations upon attorneys in connection with their cloud computing activities.

[25] MODEL RULES, *supra* note 7, R. 1.4 cmt. 4.

[26] *Id.* R. 1.6.

[27] ABA 20/20 INTRODUCTION, *supra* note 19, at 8.

First, the ABA added a new section, paragraph (C) to amend the Rule. This new section makes clear that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[28].

Second, Comment 18[29] to Rule 1.6 was expanded to further emphasize the reasonability standard and to provide guidance on the relevant factors when analyzing the ethical implications of an accidental or wholly unauthorized disclosure of client information. Comment 18 reads as follows (the underlining in the text below reflects the principal additions to Comment 18):

> [18] 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. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. 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. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].[30]

Third, the 2012 Amendments added one sentence to Comment 19[31] to Rule 1.6. Comment 19 addresses the question of preserving confidentiality when making communications

[28] MODEL RULES, *supra* note 7, R. 1.6(C) (emphasis added).

[29] Comment 18 was numbered as Comment 16 before the 2012 Amendment.

[30] MODEL RULES, *supra* note 7, R. 1.6 cmt. 18.

[31] Comment 19 was numbered as Comment 17 before the 2012 Amendment.

that will transmit confidential data. Although it is not directed only at electronic communications and internet based services, it bears directly on cloud computing. Comment 19 reads (the underlining reflects the 2012 addition to Comment 19):

> [19] 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. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state or federal laws that govern data privacy, is beyond the scope of these Rules.[32]

It is interesting to note that Comment 19 itself was not new in the 2012 Amendments. It is also noteworthy that the Commission did not choose to revise this comment in 2012 to provide more specific examples regarding cloud computing or related security measures or tools. Instead, Comment 19 retains its message emphasizing that how the ethical standard is carried out in practice is circumstance dependent. Indeed, the only change to Comment 19 was to add the last sentence that reflects that the Model Rules (and similar state ethics rules) are only one source of a lawyer's obligations to take measures to protect confidential information, and that other laws may impose additional, and possibly more stringent, standards and obligations.

4. Model Rules 1.15 and 1.16: Safekeeping Property and Terminating Representation

Next up are Model Rules 1.15 and 1.16. As the focus of the present discussion is on the implications of cloud computing (and not the broader scope of post-representation obligations), the authors group these Rules together here.

In Rule 1.15, the relevant portion of Paragraph (a) reads that:

> (a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. . . . Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by

[32] MODEL RULES, *supra* note 7, R. 1.6 cmt. 19.

> the lawyer and shall be preserved for a period of [five years] after termination of the representation.[33]

Paragraph (d) of Rule 1.16 reads:

> (d) Upon termination of representation, a lawyer shall take steps to the extent reasonably practicable to protect a client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee or expense that has not been earned or incurred. The lawyer may retain papers relating to the client to the extent permitted by other law.[34]

Taken together, these Rules require lawyers to take appropriate steps to reasonably assure the proper storage, safekeeping and return of electronically stored information—both during and after the representation. Rules 1.15 and 1.16 were not revised in the 2012 Amendments and therefore offer no further guidance on what constitutes "appropriate steps" in the storage, safekeeping, and return of electronically stored information. Fortunately, however, the state ethics opinions, which are discussed in Part III.C below, do offer guidance and can help point lawyers in the right direction.

5. Model Rules 5.1 and 5.2: Responsibilities of Partners and Subordinate Lawyers

As many law practices consist of more than one lawyer, counsel must also consider Model Rules 5.1 and 5.2 regarding the responsibilities of partners, as well as other lawyers working in the practice.

Model Rule 5.1 reads as follows:

> (a) A partner in a law firm, 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 all lawyers in the firm conform to the Rules of Professional Conduct.
>
> (b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.
>
> (c) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:

[33] *Id.* R. 1.15.

[34] *Id.* R. 1.1.

> (1) the lawyer orders or, with 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 other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.[35]

Further, Model Rule 5.2 reads:

> (a) A lawyer is bound by the Rules of Professional Conduct notwithstanding that the lawyer acted at the direction of another person.
>
> (b) A subordinate lawyer does not violate the Rules of Professional Conduct if that lawyer acts in accordance with a supervisory lawyer's reasonable resolution of an arguable question of professional duty.[36]

Taken together, the ethical admonition is straightforward: lawyers must reasonably ensure that the lawyers over whom they have a supervisory role are familiar with and act in compliance with the Rules of Professional Conduct. Likewise, lawyers being supervised have an independent ethical obligation to adhere to the Rules of Professional Conduct, which continues to apply even if a supervisory lawyer acts in contravention of the Rules and directs a subordinate attorney to act in the same manner.

Rules 5.1 and 5.2 were not revised in the 2012 Amendments and therefore offer no guidance on applying these ethical mandates to the implementation and usage of cloud computing solutions. Again, state ethics opinions, discussed in Part III.C. *infra*, do offer some guidance.

6. Model Rule 5.3: Responsibilities Regarding Nonlawyer Assistance

As virtually all lawyers use the assistance of non-lawyers, Model Rule 5.3 regarding a lawyer's responsibilities with respect to non-lawyers is relevant. Unlike Model Rules 5.1 and 5.2, Rule 5.3 and its comments were revised in 2012 and directly identify cloud computing and more specifically, the use of outside cloud computing vendors. Rule 5.3 reads as follows:

> 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

[35] *Id.* R. 5.1.

[36] *Id.* R. 5.2.

> 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 knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.[37]

The 2012 Amendments brought multiple changes to Model Rule 5.3. Starting at the beginning, the subtitle was amended to "Responsibilities Regarding Nonlawyer Assistance" (rather than "Responsibilities Regarding Nonlawyer ***Assistant***").[38] The Commission's most significant changes were, however, to add Comments 3 and 4, which (in part) specifically address cloud computing.

Comment 3 reads:

> [3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4

[37] MODEL RULES, *supra* note 7, R. 5.3.

[38] ABA 20/20 INTRODUCTION, *supra* note 19, at 12.

> (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.[39]

Much of Comment 3 to Model Rule 5.3 has direct application to cloud computing used in a legal practice. As an initial matter, Comment 3 specifically included the use of "an Internet-based service to store client information" as a primary example of the ways in which lawyers may employ outside assistance in providing their services. The Comment also requires a lawyer to "make reasonable efforts to ensure" that the outsourced services (whether online or otherwise) are provided in a manner that is "compatible with the lawyer's professional obligations," though it simultaneously recognizes that this supervisory obligation is circumstance dependent. While an exhaustive list of circumstances and factors to consider is not realistic for many reasons, Comment 3 does identify the following circumstantial considerations as particularly relevant: "the education, experience and reputation" of the nonlawyer service provider; the nature of the services that will be provided; the terms of the arrangements that the lawyer puts in place with the nonlawyer for the protection of client information; and respecting confidentiality, the environment (in legal and ethical terms) in those jurisdictions where the services will be performed.

Comment 4 was also newly added by the 2012 Amendments. Comment 4 reads:

> [4] Where the client directs the selection of a particular nonlawyer service provider outside the firm, the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer. See Rule 1.2. When making such an allocation in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.[40]

According to the Commission, the change to the title of Rule 5.3 and the addition of Comments 3 and 4 were meant to emphasize two aspects of a lawyer's ethical responsibilities with respect to outside nonlawyers who provide assistance to the lawyer in the representation. One, lawyers must make "reasonable efforts" to safeguard that the selected service providers act in a manner that is consistent with the lawyer's professional obligations, which extend to protecting client information. Two, lawyers must give "appropriate instructions" to those outside servicers when retaining their services."[41]

---

[39] MODEL RULES, *supra* note 7, R. 5.3 cmt. 3.

[40] *Id.* R. 5.3 cmt. 4.

[41] ABA 20/20 INTRODUCTION, *supra* note 19, at 12.

B. Applicable State Professional Rules

Though each state has its own set of rules of professional conduct, this paper focuses on the applicability of the ABA's Model Rules of Professional Conduct to the concerns associated with cloud computing considering that (according to the ABA) fifty-one jurisdictions have adopted the Model Rules—49 states, the District of Columbia, and the Virgin Islands (recognizing that the states may have variations in their rules and may not adopt any or all Comments). The only non-conforming state is California which, according to the ABA, "is the only state that does not have professional conduct rules that follow the format of the ABA Model Rules of Professional Conduct."[42] But, fear not, dear reader, Justice Scalia recently opined that "California does not count" anyway.[43]

The ABA provides helpful resources on its website regarding the state professional rules. These resources include lists by date of state adoption of Model Rules[44]; links to state ethics opinions[45]; summaries of states' adoption of the comments to the Model Rule and the effects of the Comments.[46]

Importantly, all states that adopted the Model Rules did so before the 2012 Amendment, and some states, many years ago. However, as with the ABA, states have continued to evaluate their ethics rules for appropriate modernization. For example, in October 2014, North Carolina adopted Amendments to its professional rules, which included technology-related changes.[47]

C. State Ethics Opinions

At least twenty state bars across the county have examined ethical questions and implications involved in cloud computing and have issued opinions.[48] These opinions, both

[42] See generally MODEL RULES, *supra* note 7.

[43] *Obergefell v. Hodges*, Nos. 14–556, 14–562, 14–571, 14–574, 2015 WL 2473451, at *44 (June 26, 2015). Naturally, the authors refer to this only in jest and clarify that Justice Scalia's statement was limited to expressing the opinion that "California does not count" when determining who is a "genuine Westerner," as Justice Scalia described the geographic background of the current Supreme Court Justices. We also note that California has issued an ethics opinion regarding technology that is compatible with opinions issued by other states on the fundamental question of whether the use of third party technology can be consistent with a lawyer's ethical obligations.

[44] ABA, States Making Amendments to the Model Rules of Professional Conduct - Dates of Adoption, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/chrono_list_state_adopting_model_rules.html (last visited July 17, 2015).

[45] ABA, Links to Other Legal Ethics and Professional Responsibility Pages, http://www.americanbar.org/groups/professional_responsibility/resources/links_of_interest.html (last visited July 17, 2015).

[46] ABA, State Adoption of the Aba Model Rules of Professional Conduct and Comments, http://www.americanbar.org/content/dam/aba/migrated/cpr/pic/comments.authcheckdam.pdf (last visited July 17, 2015).

[47] Amends. to the Rules of Prof'l Conduct of the N.C. State Bar, 2014 N.C. Court Order 0037 (Oct. 2, 2014).

[48] The following states have issued ethical opinions concerning cloud-computing: Alabama, Arizona, California, Connecticut, Florida, Iowa, Maine, Massachusetts, New Hampshire, New Jersey, New York, Nevada, North Carolina, Ohio, Oregon, Pennsylvania, Vermont, Virginia, Washington, and Wisconsin.

formal and informal, provide helpful guidance in understanding the state ethical rules and how to apply those rules when evaluating whether and how to use cloud computing solutions while adhering to the necessary ethical standards. The ABA has been monitoring state ethics opinions relating to cloud computing and has prepared very helpful resources for lawyers and law firm administrators. One such resource is a chart of state ethics opinion summaries, which is available on the ABA's website,[49] and with the permission of the ABA, a copy of the online chart is included as Attachment B to this paper.

The first state advisory opinions discussing whether and under what conditions it is ethically permissible to engage third-party cloud computing vendors to store and transmit client data began appearing as early as 2006. Indeed, every state to consider the question has found that it *can be* ethically permissible to utilize cloud-based data storage facilities and other cloud-based services, as long as lawyers adequately appreciate and address the potential risks and make reasonable efforts to protect the confidentiality of client information to maintain reliable access to client data when needed. The state opinions, like the Commission with the 2012 Amendments, generally decline to specify what exactly constitutes "reasonable efforts" in this arena. Therein lies the rub.

Though no two state ethics opinions are identical, all of the opinions generally concern themselves with the same rules of professional conduct. The latest and greatest of these opinions, however, is Wisconsin Formal Ethics Opinion EF-15-01: The Ethical Obligations of Attorneys Using Cloud Computing, published March 23, 2015[50] (the "Wisconsin Opinion"). The Wisconsin Opinion does a remarkable job of surveying the legal ethics opinions issued by other states over the last decade as well as the Comments to the Model Rules, and distilling their lessons into a "reasonability" guide of sorts for lawyers to consider when deciding if, and under what circumstances to use cloud computing services. Such a guide, though neither dispositive nor controlling, is certainly useful if only because, as the opinion sagely notes, "whatever decision a lawyer makes must be made with reasonable care, *and the lawyer should be able to explain what factors were considered in making that decision*."[51]

When assessing the risk associated with utilizing cloud computing solutions, the Wisconsin Opinion advocates considering these (albeit non-exclusive) factors when assessing risk:

- how sensitive is the information;
- what are the instructions (if any) that the client may have given and what are the client's circumstances;
- what are the possible effects to the client or third party if there is an inadvertent disclosure or unauthorized interception of information;

[49] *See* ABA, Cloud Ethics Opinions Around the U.S., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited July 17, 2015).

[50] Wis. Formal Ethics Op. EF-15-01 (Mar. 23, 2015).

[51] *Id.* at 2 (emphasis added).

- what is the lawyer's ability to assess the level of security that will be provided through the technology intended for use in the practice;
- what is the likelihood of unauthorized disclosure using the technology if additional safeguards are not employed;
- what are the potential costs of employing additional safeguards;
- how difficult is it to implement additional safeguards;
- if additional safeguards are employed, to what extent would they adversely affect the lawyer's ability to represent clients;
- is there a need for "increased accessibility" and what is the "urgency of the situation;"
- what is the "experience and reputation of the service provider;"
- what are the agreement terms with the selected service provider; and
- what is the environment (legal and ethical) in the relevant jurisdiction(s) where the services are to be conducted, with particular importance with respect to confidentiality.[52]

After considering these risks and assessing their applicability to an individual's practice, the next question becomes: what steps should one reasonably take to minimize those risks? Given the relative impossibility of providing specific requirements for reasonable efforts that evolve along with technology changes, the Wisconsin Opinion nevertheless provides some base-level guidance for what constitutes a lawyer's reasonable exercise of professional judgment.[53]

At a minimum, lawyers should:

1. Possess "a base-level comprehension of the technology and the implications of its use"[54] and a "cursory understanding" sufficient to explain to the client the advantages and risks of using the technology;

2. Understand the importance of computer security as well as the security dangers inherent in the use of some forms of technology, such as public Wi-Fi and file sharing sites;

3. Understand and be familiar with the "qualifications, reputation, and longevity"[55] of the cloud-service provider, just like they should know the same criteria of any other service provider;

---

[52] *Id.* at 1.

[53] *Id.* at 11.

[54] Wisconsin Opinion at 11 (citing Joshua H. Brand, *Cloud Computing Services—Cloud Storage*, MINN. LAWYER, January 1, 2012, at 1, *available at* http://www.docstoc.com/docs/117971742/Cloud-Computing-Services-_-Cloud-Storage-by-Joshua-H-Brand).

[55] *Id.*

4. Review and understand the terms of use or other service agreement offered by the service provider;

5. Understand the importance that data be regularly backed-up in more than one location;

6. As needed, consult with a third party (such as a technology consultant), who has the requisite skill and expertise to help the lawyer determine what are the appropriate "reasonable" efforts; and[56]

7. Consider writing engagement agreements so that they "at the least" inform and explain to potential clients the lawyer's use of cloud-based services in the representation. While the Wisconsin Opinion does not mandate this step, it does note the practical effect that doing so would create opportunities for both the client to object and for the lawyer and client to discuss the risks and advantages associated with cloud computing.[57]

The Wisconsin Opinion's main focus is on the application of the rules governing Competence (1.1), Communication (1.4), Confidentiality (1.6), and Responsibilities regarding non-lawyer assistance (5.3). Other state opinions, however, have looked at other rules when analyzing the ethical concerns relating to cloud computing. We examine some of these below and also note some additional factors and guidelines that a few other states have noted in their opinions for lawyers' consideration.

In its 2011 Formal Ethics Opinion 6, the North Carolina State Bar looked at whether a lawyer may ethically subscribe to software as a service while fulfilling the duties of confidentiality and preservation of client property—specifically Rule 1.15 requiring a lawyer to preserve client property.[58] Recognizing that "the Ethics Committee has long held that this duty does not compel any particular mode of handling confidential information nor does it prohibit the employment of vendors whose services may involve the handling of documents or data containing client information," the Ethics Committee concluded

> that a law firm may use SaaS if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files. A lawyer must fulfill the duties to protect confidential client information and to safeguard client files by applying the same diligence and competency to manage the risks of SaaS that the lawyer is required to apply when representing clients.[59]

In looking at whether a law firm may use a third-party vendor to store client data in the

[56] Many commentators, including as part of state ethics opinions, have noted that it would be impractical to expect or require that attorneys possess the necessary levels of knowledge to evaluate particular technology.

[57] *Id.* at 11-12.

[58] N.C. Formal Ethics Op. 6 at p. 6 (2011).

[59] *Id.*

cloud, the Ohio State Bar Association similarly reviewed its Rule 1.15 and concluded through Informal Advisory Opinion 2013-03 that it permitted storing client information in the cloud if the chosen vendor had appropriate systems to protect the clients' data from "destruction, loss or unavailability," and on the condition that the terms of service with the cloud storage vendor included nothing to suggest that the vendor would acquire any ownership in the electronic data on its servers in the course of the representation.[60]

Washington State Bar Association Advisory Opinion 2215, issued in 2012, also reviewed online data storage in connection with its Rule 1.15.[61] The conclusion was that Rule 1.15 permits the usage of online data storage of client documents as long as the lawyer takes steps to reasonably ensure "that the documents will not be lost."[62] The WSBA opinion, much like the Wisconsin Opinion (as well as other state opinions) and the ABA, recognized the impossibility and impracticality of providing specific directions or guidelines as to the particular security measures that lawyers must have in effect with the selected service providers for cloud data storage and related services in order to satisfy the standard of adequate protection of client information and material.[63] The opinion did offer, however, a sample best practices checklist for a lawyer without advanced technological knowledge. Many are substantially similar to those in the Wisconsin Opinion, but the authors note below a few guidelines that vary somewhat from the Wisconsin Opinion—either in focus or in level of detail. A lawyer should:

> 1. Be familiar with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession, on cloud computing industry standards and desirable features.
>
> 3. Compare provisions in service provider agreements to the extent that the service provider recognizes the lawyer's duty of confidentiality and agrees to handle the information accordingly.
>
> 4. Compare provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business.
>
> 6. Ensure secure and tightly controlled access to the storage system maintained by the service provider.[64]

Similarly, after surveying the relevant extant state ethics opinions at the time it issued its opinion in 2010, the Vermont Bar Association, in Opinion 2010-6, concluded that Vermont lawyers were permitted to use software-as-a-service solutions for "storing, processing, and

[60] OSBA Informal Advisory Op. 2013-03 (2013).

[61] WSBA Advisory Op. 2215 (2012).

[62] *Id.*

[63] *Id.*

[64] *Id.* at 2.

retrieving client property," if the lawyers take "reasonable precautions to ensure the property is secure and accessible."[65] The opinion also opted against establishing a set of specific conditions precedent to using these services; rather, it advised that the lawyers must provide the "required level of due diligence" and opined that such due diligence would typically include a "reasonable understanding" of certain conditions of the intended cloud-based service.[66] Many of these due diligence items are similar to those described in the Wisconsin Opinion, so we include here only a few additional items. According to the Vermont opinion, the due diligence should include a "reasonable understanding of . . . the vendor's commitment to protecting confidentially of the data"; "notice provisions if a third party ***seeks*** or gains (whether inadvertently or otherwise) access to the data." (emphasis added).[67] Beyond the due diligence items, the Vermont Opinion went on to suggest additional considerations for lawyers. The additional considerations include (among other things): providing clients notice about the methods for storing client data that will be used; obtaining assistance from competent technical providers to review the selected vendor's security and access systems; and implementing a system for periodic reviews of those systems to determine if they continue to be compatible with the legal requirements as technology evolves.[68]

As set forth in several of the Ethics Opinions, including the opinion promulgated by the New York State Bar Association's Committee on Professional Ethics: "This is not a new requirement, however; these same individualized considerations are required when considering more traditional storage."[69] The most important addition is that an attorney has an affirmative obligation to stay abreast of technological developments to ensure that the security measures taken remain valid and current.

IV. LEGAL OBLIGATIONS REGARDING MAINTENANCE OF CLIENT INFORMATION AND CONFIDENTIALITY

In addition to the ethical obligations, attorneys have legal obligations to consider when flying in the cloud. These legal obligations may come from various sources as discussed below.

A. Federal Rules of Civil Procedure—Production of Documents

If a law firm uses a cloud-based platform for storing client documents and communications, it must ensure that privileged communications stay protected and that confidential information is treated confidentially. At the same time, a lawyer must be able to access the information and provide it in a usable format when responding to requests for production of documents.

Rules 26 and 34 of the Federal Rules of Civil Procedure specifically include electronically stored information ("ESI") that is in a party's (or its attorneys') custody, control, or

[65] Vt. Advisory Ethics Op. 2010-6 (2011).

[66] *Id.* at 8.

[67] *Id.*

[68] *Id.* at 22.

[69] N.Y. State Bar Comm. on Prof'l Ethics, Op. 842 (Sept. 10, 2010).

possession.[70] Accordingly, documents stored in counsel's cloud are subject to production because control is still vested with counsel. That means two things: (1) counsel should have the data stored in an accessible manner so that it can be produced as required by Rule 34; and (2) counsel should store and retain client data only as long as it is necessary (or risk creating a cache of discoverable documents that should have been destroyed).

Although a party may object to the production of unduly burdensome ESI, a party may not elect—and counsel should not advise—to store data in a format that makes it difficult to search and retrieve it and then claim that the production is unduly burdensome. In *Flagg v. City of Detroit*,[71] the United States District Court for the Eastern District of Michigan held that stored text messages still preserved by the City of Detroit's nonparty internet service provider were subject to production if requested from the City directly, which would then have to direct the service provider to produce them.[72] The court found unavailing the City's argument that it did not possess or have custody of the text messages because they were available only through the internet service provider's archived records.[73] Most internet service providers do not "control" the data supplied by their customers. Instead, a customer's right to access the information gives it "control" and makes the documents and information susceptible to production.

Another issue arising under the federal discovery rules is highlighted in *Disability Rights Council*, where the data was stored on back-up tapes that would be difficult to read and retrieve. Because the City did not store the information in any other format, the court held that it was not unduly burdensome to require that the tapes be searched.[74] In counseling clients, it is important to recommend technology that makes access to and retrieval of data faster and easier to enable clients to respond to legal and regulatory demands for electronically stored information. Using outdated or difficult to access technology may not be a sufficient ground to object.

Counsel should also be vigilant about the retention of client data stored in the cloud. Some providers may keep the data for months after the termination of a hosting or storage agreement. Counsel should ensure that the data is either destroyed or released to the client's sole control as soon as a matter has reached a certain ending, so that a source of responsive documents is not unwittingly created.

---

[70] FED. R. CIV. P. 26 and 34.

[71] *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008).

[72] *Id.* at 352 (disallowing a subpoena request made directly to the internet service provider because barred by the Stored Communications Act, 18 U.S.C. § 2701 et seq. ("SCA"), but permitting the production of the text messages if the request was routed properly through the party having control over the information, even if it did not have possession).

[73] *Id. See Elcometer, Inc. v. TQC-USA, Inc.*, No. 12-CV-14628, 2013 WL 5346382, at *4 (E.D. Mich. Sept. 23, 2013) ("The [Stored Communications Act] lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to a subpoena or court order.").

[74] *Disability Rights Council*, 242 F.R.D. at 145 (requiring party to conduct expensive review of back-up media because it contained the only copy of electronically stored information).

B. Foreign Corrupt Practices Act[75]

The Foreign Corrupt Practices Act was passed in 1977 after federal special investigators discovered U.S. companies secretly using corporate money to bribe foreign officials to obtain business.[76] The FCPA had two goals: (1) to make it illegal for anyone to corruptly offer, provide, promise, or authorize the provision of money or anything of value to foreign officers or employees to obtain or retain business;[77] and (2) to require publicly-traded U.S. businesses to keep accurate books and records to account for and fairly reflect their transactions and to maintain a system of accounting controls that provide reasonable assurances that they are not making unauthorized bribery payments.[78] The FCPA prohibits the making of bribes through the mail or any instrumentality of interstate commerce, including the internet. Today, businesses—including law firms which often follow wherever the clients go—have developed increasingly global footprints and use globally-connected data, communications, and networking systems, in both developed and developing nations. This globalization has catapulted the FCPA back into favor with its twin enforcement agencies—the Securities and Exchange Commission ("SEC") and the Department of Justice ("DOJ").

The FCPA can be a trap for the unwary lawyer in a few instances. First, in-house counsel who are officers of a company can be held liable for FCPA violations just like any other officer or director involved in a decision to facilitate an unlawful bribe of a foreign official.[79] Because wire transfers, email communications, and other information exchanges that occur in the cloud can touch data centers around the globe without one's knowledge, it would behove in-house counsel to be aware of the company's cloud computing and other electronic transmissions before providing legal advice or assisting in the arrangement of payments that the company believes will occur outside of the United States and thus fall outside the scope of the FCPA.[80] The SEC has asserted claims against foreign individuals and companies transacting business *in other countries* where money merely passed through a U.S. correspondent bank.[81]

---

[75] Foreign Corrupt Practices Act ("FCPA") of 1977, Pub. L. No. 95-213, 91 Stat. 1494 (codified as amended at 15 U.S.C. §§ 78dd-1 to -3 (2000)).

[76] William Alan Nelson II, *Attorney Liability Under the Foreign Corrupt Practices Act: Legal and Ethical Challenges and Solutions*, 39 U. MEM. L. REV. 255, 247 (2008-2009), *available at* http://ssrn.com/abstract=1883586.

[77] 15 U.S.C. § 78dd-2(a) (2006).

[78] 15 U.S.C. § 78m(b)(2)-(7) (2006).

[79] 15 U.S.C. § 78dd-2 (defining "issuer" to include "any person" committing bribery on U.S. territory); Sarah Bartle et al., *Foreign Corrupt Practices Act*, 51 AM. CRIM. L. REV. 1265, 1275-76 (2014) (describing impact of 1998 amendments to FCPA and expansion of covered persons).

[80] Bartle, *supra* note 79, at 1275-76.

[81] Shearman & Sterling LLP, *It Doesn't Take Much: Expansive Jurisdiction in FCPA Matters* (Mar. 2009), http://www.shearman.com/en/newsinsights/publications (search "FCPA") (last visited July 6, 2015) (discussing cases); *see also SEC v. Straub*, 921 F. Supp. 2d 244 (S.D.N.Y. Feb. 8, 2013) (finding use of an instrumentality in interstate commerce" in FCPA claim includes sending emails from Hungary to Macedonia where emails routed through or stored on network servers located in the United States); Andrew M. Hinkes, Cloud Computing and Unexpected FCPA Jurisdiction, CORPORATE COUNSEL, May 21, 2013, *available at* http://www.bergersingerman.com/wp-content/uploads/2013/07/2013.05.21-HINKES-Corporate-Counsel-Cloud-Computing-and-Unexpected-FCPA-Jurisdiction.pdf (last accessed July 19, 2015).

Second, in-house counsel should be careful when advising a company regarding the selection of a cloud storage provider because some providers will be subject to more or less stringent privacy laws if the companies are based or the servers are located in other countries. For example, Jottacloud, which bills itself as a cloud data storage provider similar to Dropbox, also touts that its servers are located in Norway where the privacy laws are stricter, increasing the difficulty for a third party to subpoena or otherwise obtain access to stored data.[82] A company can be held liable under the FCPA for the illicit conduct of a third-party intermediary.[83] Accordingly, it is an important part of corporate due diligence to identify a third-parties' ties to foreign governments and reputation in those localities, particularly those that are known for more corrupt business environments.

A critical conflict could arise if in-house counsel becomes aware of a reportable FCPA violation. Such knowledge triggers a duty to report that information to senior executives and possibly the board of directors.[84] Counsel must walk a fine line between determining when reporting up the ladder is necessary and when, despite the ethical obligation to maintain the attorney-client privilege and client confidentiality, counsel may have to withdraw from representation to avoid liability for any ongoing FCPA obligations.[85] The authors are unaware of any published decisions addressing this potential conflict.

In-house counsel may also face a potential FCPA issue under the portion of the statute requiring a company to maintain accurate accounting records and other documentation. Cloud users must be able to retrieve any necessary data, regardless of whether it is stored in another country or on servers maintained by an unreliable third-party provider. A company could face FCPA liability if unable to demonstrate its accurate and clean records to defeat an FCPA allegation.

The FCPA does not have a provision for direct liability for counsel, unless that attorney is also considered an "issuer" or agent of an issuer as an officer of a company. However, in a Rule 102(e) proceeding, the SEC can censure an attorney for providing client advice that results in an FCPA violation.[86] This is not a proceeding of which the SEC has made significant use. It is far more likely that a legal malpractice claim might be brought against counsel based on legal advice regarding a bribery payment or failure to alert the client regarding the appropriate accounting requirements. In *Stichting Ter Behartiging Van de Belangen Van Oudaandeel-*

[82] *See* JOTTACLOUD, https://www.jottacloud.com/its-your-stuff-guaranteed/ (last visited July 5, 2015). As a side note, the use of a cloud provider that uses lack of extradition or tight privacy and data control laws as selling points could result in the use of those facts against a client as "evidence" of an intent to hide information. In one situation of which the authors are aware, an attorney hired by a company in a non-legal capacity used Jottacloud to upload hundreds of work-related files while still employed. Following the employee's termination, the company discovered the files had been uploaded. In a lawsuit alleging violations of common law, state, and federal computer data theft claims, including a violation of the Computer Fraud and Abuse Act, the company argued that the employee's intentional use of a cloud storage provider with servers located in Norway (and protected by stringent privacy laws) was evidence of intent to avoid detection and having to return the company documents.

[83] Bartle, *supra* note 79, at 1305-07.

[84] *See* 15 U.S.C. s 78dd-1(f) (requiring reporting of knowledge of violation).

[85] Nelson, *supra* note 76, at 280-84.

[86] *Id.* at 278-79. *See* 17 C.F.R. s 201.102 (2007) (permitting the SEC to censure attorneys who practice before it for lacking integrity or character or for engaging in unethical or improper professional conduct).

houders In Het Kapitaal Van Saybolt Int'l B.V. v. Schreiber, the United States Court of Appeals for the Second Circuit held that corporate shareholders could bring an action for legal malpractice against the company's legal counsel.[87] There, the attorney was a member of the company's board of directors and had occasionally been retained for legal advice.[88] During company discussions about leasing property in Panama, the board concluded that the company could not secure the lease without bribing a Panamanian official with $50,000.00. An attorney first informed the board that such a payment could expose the company and its officers to criminal liability.[89] He revised that initial admonishment, however, and later informed the board that Saybolt North America could not make the bribe because it would be unlawful under the FCPA, but that Saybolt International, its Dutch affiliate, could lawfully make the bribe.[90] Schreiber neglected to make clear to Saybolt that the mere fact of Saybolt North America's involvement in arranging the affiliate's bribery payment created potential liability. Importantly, the *Schreiber* holding does not stand for the proposition that an attorney is liable for legal malpractice for providing advice that resulted in an FCPA violation, but it did permit the shareholders to file the lawsuit, regardless of the company's and other senior executives' guilty pleas.[91] The matter settled without a finding of liability.

C. Other Government Laws and Regulations

1. Computer Fraud and Abuse Act[92]

In fulfilling its ethical obligations with respect to cloud computing, counsel should consider the need to guard against violations of the Computer Fraud and Abuse Act ("CFAA") but also be prepared to use the CFAA as a sword against violators.[93] Among other things, the CFAA creates a cause of action for any person who accesses a computer or computer system without authority or exceeds his or her authorized access.[94] From an ethical perspective, the CFAA can create dilemmas in a few discrete areas.

An attorney may exceed the authorized use of or access to confidential client information if that information is uploaded to an unauthorized cloud account, transmitted improperly (e.g., emailed to a personal email account or to third party or in a manner that can be intercepted by a

[87] 327 F.3d 173 (2d Cir. 2003).

[88] Schreiber, 327 F.3d at 176.

[89] *Id.*

[90] *Id.*

[91] Nelson, *supra* note 76, at 292.

[92] 18 U.S.C. § 1030(a).

[93] *See* 18 U.S.C. § 1030(a)(1)-(3) (Supp. II 2008) (providing coverage for access to any computer "used in or affecting interstate or foreign commerce or communication").

[94] *Id. See* Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, WILLIAM & MARY L. REV., Vol. 52, Issue 4, at 1372 (examining federal courts three traditional approaches to defining "authorization" under the CFAA: agency, code, and contract); Bradley C. Nahrstadt, *Former Employee Sabotage? Invoke the Computer Fraud and Abuse Act*, J. INTERNET L., Feb. 2009, at 17, 25.

third party). Similarly, if a client's matter has ended, an attorney could arguably be liable under the CFAA for unauthorized access or use if the attorney still maintains electronic copies of the client's data in a shared storage environment. While this scenario is less likely to occur during an ongoing client relationship, it is a far greater consideration when a client is switching counsel or the attorney with primary responsibility for a client relationship leaves the firm.

A common situation that may arise is when an attorney leaves Firm A and takes with him possession or control of client documents created while at Firm A for use at Firm B. Once the employment relationship terminates, the attorney has no further right or authority to access Firm A's client documents and information, regardless of who authored the documents. It may be difficult to determine what damages are incurred as a result of this unauthorized use, especially if the documents are used only as a future resource. To protect itself in the event of such unauthorized use, a firm should maintain a clear policy for exiting attorneys to return or destroy all firm work product and not to maintain copies of that work product outside the firm's network. If an attorney leaves a firm and takes a matter or client with her, then the attorney with the continuing relationship will need all case information. In that circumstance, it will be the former firm that must return or destroy all work product.

Accordingly, firms must be vigilant to guard against attorneys continuing to access information in email or cloud-based storage in violation of the CFAA. The situation is no different from an attorney walking out the door with boxes of privileged communications or confidential client documents. Because electronic documents and entire electronic case files are so easy to replicate, there is a considered risk involved in permitting attorneys to store client information in a personal cloud. And there is a risk for the attorney of violating the CFAA by accessing or using that client data without authorization.

2. Electronic Communications Privacy Act[95]

The Electronic Communications Privacy Act of 1986 ("ECPA") expanded and revised federal wiretapping and electronic eavesdropping laws and attempted to assure consumers that their personal information would be safe despite the technological advancements that seemed to make personal information more vulnerable than ever.[96] Title 2 of the ECPA is the Stored Communications Act ("SCA").[97] The SCA provides that litigants cannot subpoena internet service providers ("ISPs") directly to demand the production of email or other stored electronic communications that are in the custody or possession of those ISPs. In general, ISPs are forbidden to "divulge to any person or entity the contents of any communication which is carried or maintained on that service," unless authorized by the customer or if the information requested is limited to "log data" (*i.e.*, name and email address of recipient). However, this prohibition only applies to emails stored for less than 180 days—after which, a warrantless subpoena is technically sufficient to obtain the data. There have been several demands for an amendment to this law considering the large amounts of data now stored in the cloud, including a recommendation in a 2014 White House Report to eliminate the "archaic" 180-day delineation

[95] 18 U.S.C. §§ 2510-3127 (2008).

[96] *Id.*

[97] 18 U.S.C. §§ 2701–2712 (2008).

and to reconsider warrantless access to metadata in light of substantial information generated from metadata fragments and server logs.[98]

From an attorneys' perspective, it is important to understand the ECPA in order to counsel clients appropriately regarding their stored communications and to create guidelines for the law firms' internal treatment of electronic information.

3. State laws governing computer theft

Every state in the union has passed a law related to computer crime, although not all specifically address unauthorized access through the internet.[99] An analysis of these state laws is outside the scope of this paper, but it is important for counsel to be aware of any criminal or civil laws impacting computer and cloud use in each jurisdiction in which data stored on the cloud may be accessed or physically stored.

D. Post-Representation Issues

As discussed above, Model Rule 1.16 imposes a continuing obligation to reasonably protect a client's interests, including the safekeeping of a client's electronically stored information. And, although a lawyer "may retain papers relating to the client to the extent permitted by other law," the potential exposure for a client and for a law firm in retaining client documents may outweigh any benefit in retaining those documents when the client relationship has ended. Thus, counsel should include a plan for destruction of stored documents either in the engagement letter or initial engagement terms or in a post-representation closing letter following the termination of a specific matter or of the client relationship.

A document retention timetable should take into consideration any reasonably foreseeable potential for litigation; legal malpractice claim or other litigation in connection with the handling of the matter; retention of client billing or other accounting records for purposes of state or federal tax audits; any state ethical obligations identifying a particular length of time to retain documents relating to a client representation; and client requirements under other state or federal laws regarding the retention of certain records. The document retention plan should

---

[98] BIG DATA, *supra* note 1, at 60, 66-7.

[99] ALA. CODE § 13A-8-5 (2015); ALASKA STAT. § 11.46.740 (2015); ARIZ. REV. STAT. ANN. § 13-2316 (2015); ARK. CODE ANN. § 5-41-101 (2015); CAL. PEN. CODE § 502 (West 2015); COL REV. STAT. § 18-5.5-101 et seq. (2015); CONN. GEN. STAT. § 53a-250 (2015); DEL. CODE ANN. tit. 11, §§ 931 (2015); FLA. STAT. §§ 815.01-815.07 (2015); GA. CODE ANN. § 16-9-91 (2015); HAW. REV. STAT. § 708-890 (2015); IDAHO CODE ANN. § 18-2201 (2015); 720 ILL. COMP. STAT. 5/16D-1 (2015); IND. CODE §§ 35-43-1-4, -2-3 (2015); IOWA CODE §§ 714, 716.6B (2015); KAN. STAT. ANN. § 21-5839 (2015); KY. REV. STAT. ANN. §§ 434.845 to 855 (West 2015); LA. REV. STAT. ANN. § 14:73.1 (2015); ME. REV. STAT. tit. 17-A, § 431 (2015); MD. CODE ANN., CRIM. LAW § 7-302 (West 2015); MASS. GEN. LAWS ch. 266, § 33A (2015); MICH. COMP. LAWS § 752.791 (2015); MINN. STAT. § 609.87 (2015); MISS. CODE ANN. § 97-45-1 (West 2015); MO. REV. STAT. §§ 537.525, 569.094 (2015); MONT. CODE ANN. §§ 45-2-101, -6-310, -6-311 (2015); NEB. REV. STAT. § 28-1343 (2015); NEV. REV. STAT. § 205.473 (2015); N.H. REV. STAT. ANN. § 638:16 (2015); N.J. STAT. ANN. § 2C:20-23 (West 2015); N.M. STAT. ANN., § 30-45-1 (2015); N.Y. PENAL LAW § 156 (McKinney 2015); N.C. GEN. STAT. §§ 14-453 to -459 (2015); N.D. CENT. CODE § 12.1-06.1-08 (2015); OHIO REV. CODE ANN. § 2913.01 (West 2015); OKLA. STAT. tit. 21, § 1952 (2015); OR. REV. STAT. §§ 164.125, 164.377 (2015); 18 PA. CONS. STAT.§§ 7601-7661 (2015); R.I. GEN. LAWS § 11-52-1 (2015); S.C. CODE ANN. § 16-16-10 (2015); S.D. CODIFIED LAWS §§ 43-43B-1 to -8 (2015); TENN. CODE ANN. §§ 39-14-601, 14-105 (2015); TEX. PENAL CODE ANN. §33.1 (West 2015); UTAH CODE ANN. § 76-6-701 (West 2015); VT. STAT. ANN. tit. 13, §§ 4101-4107 (2015); VA. CODE ANN. § 18.2-152.1 (2015); WASH. REV. CODE § 9A.52.110 (2015); W.V. CODE § 61-3C-1 (2015); WIS. STAT. § 943.70 (2015); WYO. STAT. ANN. § 6-3-501 (2015).

explain the manner and timing for the return or destruction of any client data. This plan must consider the cost to both the firm and the client if the information is stored with a cloud-based provider that charges for such storage, so that neither is caught off guard if the storage services terminate and the data is deleted prior to being backed-up or transferred. Encrypting and saving all relevant client data to a password-protected flash drive or similar storage device and returning it to the client is a good option.

V. STRATEGIES FOR USE AND PROTECTION

A. Factors for Satisfying "Reasonable Care" Standard and Selecting Service Providers

As discussed in Part III above, a significant number of states have issued ethics opinions in light of the ABA's Model Rules and Amendments thereto and the ABA 20/20 Commission's research and recommendations respecting cloud computing. All of the ethics opinions conclude that an attorney may use cloud-based computing for client data and correspondence as long as the attorney uses reasonable care to ensure that the information remains secure and confidential. A reasonable care analysis is primarily two-fold: first, what actions should counsel take at the outset to understand a client's cloud-computing needs, and second what actions counsel should take to adequately appreciate the risks associated with the intended cloud computing services and appropriately select a provider and maintain that service. Additionally, attorneys must consider what measures are needed to ensure that their measures continue to be reasonable and adequate.

Although subject to specific state ethical guidelines, federal and state laws, and the particular demands of a client or circumstance, included as Attachment C to this paper are sample checklists to guide that "reasonable care" determination. The checklists are organized into three phases of analysis: (1) Developing an Understanding of Cybersecurity Benefits and Risks—Internal and External; (2) Due Diligence and Assessments; and (3) Ongoing Due Diligence—Monitoring and Policies. Naturally, given the many different ways for lawyers to use cloud-based computing (and certainly the future will hold many new options), each factor may not be universally relevant and the checklists in Attachment C will serve as a guide rather than a one-size-fits-all approach.

B. Communications with Clients Regarding Cloud Computing Practices

As noted in Part III.A.2, the 2012 Amendments left Model Rule 1.4 and its Comments almost entirely intact, so it is not altogether clear from the Rule itself that a lawyer's initial use and choice to utilize a cloud computing solution is impacted by this Rule. But in light of what can seem to be regularly occurring data breaches and cyber-attacks, the question has arisen as to whether the legal ethical standards may render it necessary for a lawyer to inform clients about, or possibly even obtain client consent for, the lawyer's use of cloud computing and related cyber technologies in performing the legal representation.

To the extent the existing state opinions have addressed the application of Model Rule 1.4, the general conclusion is that storage of electronic client information may be ethically permitted as long as the lawyer has taken reasonable steps to competently safeguard the confidentiality of the client information, and that client consultation or consent may not be required by the ethics rules in some situations. For example, an Ohio advisory opinion explains that: "We do not conclude that storing client data in 'the cloud' always requires prior client consultation, because we interpret the [Rule 1.4(a)] language 'reasonably consult' as indicating

that the lawyer must use judgment in order in order to determine if the circumstances call for consultation."[100] Similarly, a Pennsylvania opinion in 2011 stated that "it is not necessary to communicate every minute detail of a client's representation."[101] Based on the trend in the state opinions and that reality seems to demonstrate that it is impossible to guaranty total online security, lawyers may consider it a best practice to provide information to clients, in engagement letters or otherwise, regarding their cloud computing policies or practices.

Many state opinions suggest notifying clients as to the lawyer's use of cloud-based data storage and related services—even if the opinions do not go so far as to opine that notice is necessary from an ethics compliance standpoint in most scenarios. For example, Vermont suggests giving notice to the client about the proposed method for storing client information.[102] Additionally, situations involving highly sensitive data may lead to a heightened standard. For instance, the New Hampshire opinion suggests that client consent may be necessary for use of a third-party service provider when the information is highly sensitive.[103] The New Hampshire admonition is in line with the Pennsylvania opinion, which similarly acknowledges that "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."[104]

Accordingly, the general consensus regarding a lawyer's duty to communicate with the client regarding the initial decision to use cloud computing solutions can be fairly summarized as follows:

> While a lawyer is not required in all representations to inform clients that the lawyer uses the cloud to process, transmit or store information, a lawyer may choose, based on the needs and expectations of the clients, to inform the clients. A provision in the engagement agreement or letter is a convenient way to provide clients with this information.[105]

The duty to inform the client that there has been a security breach that affects the confidentiality or security of the client's information, however, is quite a different matter. The ethics rules, as well as other laws and regulations, will address requirements for the lawyer to inform the client of the breach.[106]

---

[100] OSBA Informal Advisory Op. 2013-03 (2013) at 6.

[101] Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Opinion 2011-200 (2011) at 5-6. *See also* State Bar of Nev., Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 33 (Feb. 9, 2006).

[102] Vt. Advisory Ethics Op. 2010-6 (2011) at 8.

[103] N.H. Bar Ass'n Ethics Comm., Advisory Op. 2012-13/4 (Feb. 21, 2013) at 2.

[104] Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Opinion 2011-200 (2011) at 6.

[105] Wis. Formal Ethics Op. EF-15-01 (Mar. 23, 2015) at 4.

[106] For example, page 5 of the Wisconsin Opinion identifies that Model Rules 1.4(a)(3) and 1.4(b) require notice of breaches.

C. Cyber Insurance

How does that old saying go "Never forget to be your own best friend"? Well, no matter its applicability to rest of your life, in this arena it means only one thing: get thee some cyber insurance. Because, no matter how carefully you plan and no matter how many precautions you take to avoid the inadvertent disclosure of client information, there are two realties: (1) the risk is never zero and (2) the costs can be enormous.

In 2013, the ABA published an article entitled "Protect your firm: Invest in cyber liability insurance" outlining the risks of a cyber-attack and the associated costs. According to the article, the average annual cost of a cybercrime incident in 2012 was $8.9 million, according to the Ponemon Institute's 2012 Cost of Cyber Crime report.[107] And those were 2012 dollars.

What should a cyber insurance policy typically cover? According to the Bloomberg article "Think You Don't Need Cyber Insurance? Think Again!," the typical policy should cover investigation, legal defense costs, costs of a regulatory investigation, business interruption, third-party liability, and various and sundry other exposures such as digital asset loss and cyber extortion.[108] Just as with what constitutes "reasonable" measures to protect client information in the cyber realm, there is no single cyber insurance policy that fits all legal practices or firms. Lawyers are strongly advised to consult with qualified insurers or agents regarding the options available to their practices.

At the end of the day, all you can do is the best you can and "hope to end up with the right regrets."[109]

VI. CONCLUSION

The advances in technology offer great opportunities to legal professionals, in small and multi-national firms alike, to achieve efficiencies and elevate their practices. Fortunately, the existing legal and ethical framework allows lawyers to take advantage of the technological advances offered by cloud computing—so long they actively evaluate and implement measures to ensure that their policies and practices remain reasonable in light of the changing technological landscape and the needs of their client.

---

[107] American Bar Ass'n, *Protect your firm: Invest in cyber liability insurance*, YOURABA, July 2013, http://www.americanbar.org/newsletter/publications/youraba/201307article04.html.

[108] Monica Bay, *Think You Don't Need Cyber Insurance? Think Again!*, BLOOMBERG BNA, May 22, 2015, https://bol.bna.com/think-you-dont-need-cyber-insurance-think-again/.

[109] ARTHUR MILLER, THE RIDE DOWN MT. MORGAN 20 (Penguin Books Rev. ed. 1999) (1991).

Attachment A:

August 2012 Amendments to ABA Model Rules of Professional Conduct

AUGUST 2012 AMENDMENTS TO
ABA MODEL RULES OF PROFESSIONAL CONDUCT

Rule 1.0 Terminology

(a) ''Belief'' or ''believes'' denotes that the person involved actually supposed the fact in question to be true. A person's belief may be inferred from circumstances.

(b) ''Confirmed in writing,'' when used in reference to the informed consent of a person, denotes informed consent that is given in writing by the person or a writing that a lawyer promptly transmits to the person confirming an oral informed consent. See paragraph (e) for the definition of ''informed consent.'' If it is not feasible to obtain or transmit the writing at the time the person gives informed consent, then the lawyer must obtain or transmit it within a reasonable time thereafter.

(c) ''Firm'' or ''law firm'' denotes a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization.

(d) ''Fraud'' or ''fraudulent'' denotes conduct that is fraudulent under the substantive or procedural law of the applicable jurisdiction and has a purpose to deceive.

(e) ''Informed consent'' denotes the agreement 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.

(f) ''Knowingly,'' ''known,'' or ''knows'' denotes actual knowledge of the fact in question. A person's knowledge may be inferred from circumstances.

(g) ''Partner'' denotes a member of a partnership, a shareholder in a law firm organized as a professional corporation, or a member of an association authorized to practice law.

(h) ''Reasonable'' or ''reasonably'' when used in relation to conduct by a lawyer denotes the conduct of a reasonably prudent and competent lawyer.

(i) ''Reasonable belief'' or ''reasonably believes'' when used in reference to a lawyer denotes that the lawyer believes the matter in question and that the circumstances are such that the belief is reasonable.

(j) ''Reasonably should know'' when used in reference to a lawyer denotes that a lawyer of reasonable prudence and competence would ascertain the matter in question.

(k) ''Screened'' denotes the isolation of a lawyer from any participation in a matter through the timely imposition of procedures within a firm that are reasonably adequate under the circumstances to protect information that the isolated lawyer is obligated to protect under these Rules or other law.

(l) ''Substantial'' when used in reference to degree or extent denotes a material matter of clear and weighty importance.

(m) ‘‘Tribunal’’ denotes a court, an arbitrator in a binding arbitration proceeding or a legislative body, administrative agency or other body acting in an adjudicative capacity. A legislative body, administrative agency or other body acts in an adjudicative capacity when a neutral official, after the presentation of evidence or legal argument by a party or parties, will render a binding legal judgment directly affecting a party’s interests in a particular matter.

(n) ‘‘Writing’’ or ‘‘written’’ denotes a tangible or electronic record of a communication or representation, including handwriting, typewriting, printing, photostating, photography, audio or videorecording, and ~~e-mail~~ electronic communications. A ‘‘signed’’ writing includes an electronic sound, symbol or process attached to or logically associated with a writing and executed or adopted by a person with the intent to sign the writing.

Comment

...

Screened

...

[9] The purpose of screening is to assure the affected parties that confidential information known by the personally disqualified lawyer remains protected. The personally disqualified lawyer should acknowledge the obligation not to communicate with any of the other lawyers in the firm with respect to the matter. Similarly, other lawyers in the firm who are working on the matter should be informed that the screening is in place and that they may not communicate with the personally disqualified lawyer with respect to the matter. Additional screening measures that are appropriate for the particular matter will depend on the circumstances. To implement, reinforce and remind all affected lawyers of the presence of the screening, it may be appropriate for the firm to undertake such procedures as a written undertaking by the screened lawyer to avoid any communication with other firm personnel and any contact with any firm files or other ~~materials~~ information, including information in electronic form, relating to the matter, written notice and instructions to all other firm personnel forbidding any communication with the screened lawyer relating to the matter, denial of access by the screened lawyer to firm files or other ~~materials~~ information, including information in electronic form, relating to the matter, and periodic reminders of the screen to the screened lawyer and all other firm personnel.

...

Rule 1.1 Competence

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

...

Retaining or Contracting With Other Lawyers

[6] Before a lawyer retains or contracts with other lawyers outside the lawyer's own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and must reasonably believe that the other lawyers' services will contribute to the competent and ethical representation of the client. See also Rules 1.2 (allocation of authority), 1.4 (communication with client), 1.5(e) (fee sharing), 1.6 (confidentiality), and 5.5(a) (unauthorized practice of law). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer's own firm will depend upon the circumstances, including the education, experience and reputation of the nonfirm lawyers; the nature of the services assigned to the nonfirm lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

[7] When lawyers from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other and the client about the scope of their respective representations and the allocation of responsibility among them. See Rule 1.2. When making allocations of responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

Maintaining Competence

[~~6~~ 8] 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.

Rule 1.4 Communication

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

Comment

...

Communicating with Client

...

[4] A lawyer's regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request, or if a prompt response is not feasible, that the lawyer, or a member of the lawyer's staff, acknowledge receipt of the request and advise the client when a response may be expected. ~~Client telephone calls should be promptly returned or acknowledged.~~ A lawyer should promptly respond to or acknowledge client communications.

...

Rule 1.6 Confidentiality of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; ~~or~~

(6) to comply with other law or a court order~~.~~; or

(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Comment

...

Detection of Conflicts of Interest

[13] Paragraph (b)(7) recognizes that lawyers in different firms may need to disclose limited information to each other to detect and resolve conflicts of interest, such as when a lawyer is considering an association with another firm, two or more firms are considering a merger, or a lawyer is considering the purchase of a law practice. See Rule 1.17, Comment [7]. Under these circumstances, lawyers and law firms are permitted to disclose limited information, but only once substantive discussions regarding the new relationship have occurred. Any such disclosure should ordinarily include no more than

the identity of the persons and entities involved in a matter, a brief summary of the general issues involved, and information about whether the matter has terminated. Even this limited information, however, should be disclosed only to the extent reasonably necessary to detect and resolve conflicts of interest that might arise from the possible new relationship. Moreover, the disclosure of any information is prohibited if it would compromise the attorney-client privilege or otherwise prejudice the client (e.g., the fact that a corporate client is seeking advice on a corporate takeover that has not been publicly announced; that a person has consulted a lawyer about the possibility of divorce before the person's intentions are known to the person's spouse; or that a person has consulted a lawyer about a criminal investigation that has not led to a public charge). Under those circumstances, paragraph (a) prohibits disclosure unless the client or former client gives informed consent. A lawyer's fiduciary duty to the lawyer's firm may also govern a lawyer's conduct when exploring an association with another firm and is beyond the scope of these Rules.

[14] Any information disclosed pursuant to paragraph (b)(7) may be used or further disclosed only to the extent necessary to detect and resolve conflicts of interest. Paragraph (b)(7) does not restrict the use of information acquired by means independent of any disclosure pursuant to paragraph (b)(7). Paragraph (b)(7) also does not affect the disclosure of information within a law firm when the disclosure is otherwise authorized, see Comment [5], such as when a lawyer in a firm discloses information to another lawyer in the same firm to detect and resolve conflicts of interest that could arise in connection with undertaking a new representation.

[15~~3~~] A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4. Unless review is sought, however, paragraph (b)(6) permits the lawyer to comply with the court's order.

[16~~4~~] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified. Where practicable, the lawyer should first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose. If the disclosure will be made in connection with a judicial proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[17~~5~~] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(6). In exercising the discretion conferred by this Rule, the lawyer may consider such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the lawyer's own involvement in the transaction and factors that may extenuate the conduct in question. A lawyer's decision not to

disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may be required, however, by other Rules. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). See Rules 1.2(d), 4.1(b), 8.1 and 8.3. Rule 3.3, on the other hand, requires disclosure in some circumstances regardless of whether such disclosure is permitted by this Rule. See Rule 3.3(c).

Acting Competently to Preserve Confidentiality

[18~~6~~] Paragraph (c) requires a ~~A~~ lawyer ~~must~~ 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. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. 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. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19~~7~~] 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. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Former Client

[20~~18~~] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.

...

Rule 4.4 Respect for Rights of Third Persons

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.

(b) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.

Comment

...

[2] Paragraph (b) recognizes that lawyers sometimes receive a document~~s~~ or electronically stored information that ~~were~~ was mistakenly sent or produced by opposing parties or their lawyers. A document or electronically stored information is inadvertently sent when it is accidentally transmitted, such as when an email or letter is misaddressed or a document or electronically stored information is accidentally included with information that was intentionally transmitted. If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning or deleting the document or electronically stored information ~~original document~~, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged status of a document or electronically stored information has been waived. Similarly, this Rule does not address the legal duties of a lawyer who receives a document or electronically stored information that the lawyer knows or reasonably should know may have been ~~wrongfully~~ inappropriately obtained by the sending person. For purposes of this Rule, ''document or electronically stored information'' includes, in addition to paper documents, email and other forms of electronically stored information, including embedded data (commonly referred to as "metadata"), that is ~~email or other electronic modes of transmission~~ subject to being read or put into readable form. Metadata in electronic documents creates an obligation under this Rule only if the receiving lawyer knows or reasonably should know that the metadata was inadvertently sent to the receiving lawyer.

[3] Some lawyers may choose to return a document or delete electronically stored information unread, for example, when the lawyer learns before receiving it ~~the document~~ that it was inadvertently sent ~~to the wrong address~~. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document or delete electronically stored information is a matter of professional judgment ordinarily reserved to the lawyer. See Rules 1.2 and 1.4.

...

Rule 5.3 Responsibilities Regarding Nonlawyer Assistance~~ts~~

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 knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Comment

[~~2~~1] Paragraph (a) requires lawyers with managerial authority within a law firm to make reasonable efforts ~~to establish internal policies and procedures designed to provide~~ to ensure that the firm has in effect measures giving reasonable assurance that nonlawyers in the firm and nonlawyers outside the firm who work on firm matters ~~will~~ act in a way compatible with the professional obligations of the lawyer. ~~with the Rules of Professional Conduct~~. See Comment [6] to Rule 1.1 (retaining lawyers outside the firm) and Comment [1] to Rule 5.1~~.~~ (responsibilities with respect to lawyers within a firm). Paragraph (b) applies to lawyers who have supervisory authority over ~~the work of a nonlawyer.~~ such nonlawyers within or outside the firm. Paragraph (c) specifies the circumstances in which a lawyer is responsible for the conduct of ~~a nonlawyer~~ such nonlawyers within or outside the firm that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer.

Nonlawyers Within the Firm

[~~1~~2] Lawyers generally employ assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising nonlawyers should take account of the fact that they do not have legal training and are not subject to professional discipline.

Nonlawyers Outside the Firm

[3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.

[4] Where the client directs the selection of a particular nonlawyer service provider outside the firm, the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer. See Rule 1.2. When making such an allocation in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

Attachment B:

American Bar Association's – Cloud Ethics Opinions Around the U.S. –

Quick Reference and Opinion Summaries

Cloud Ethics Opinions Around the U.S.

Cloud Ethics Opinions

There's a compelling business case for cloud computing, but can lawyers use it ethically? We've compiled these comparison charts to help you make the right decision for your practice.

What is Cloud Computing?

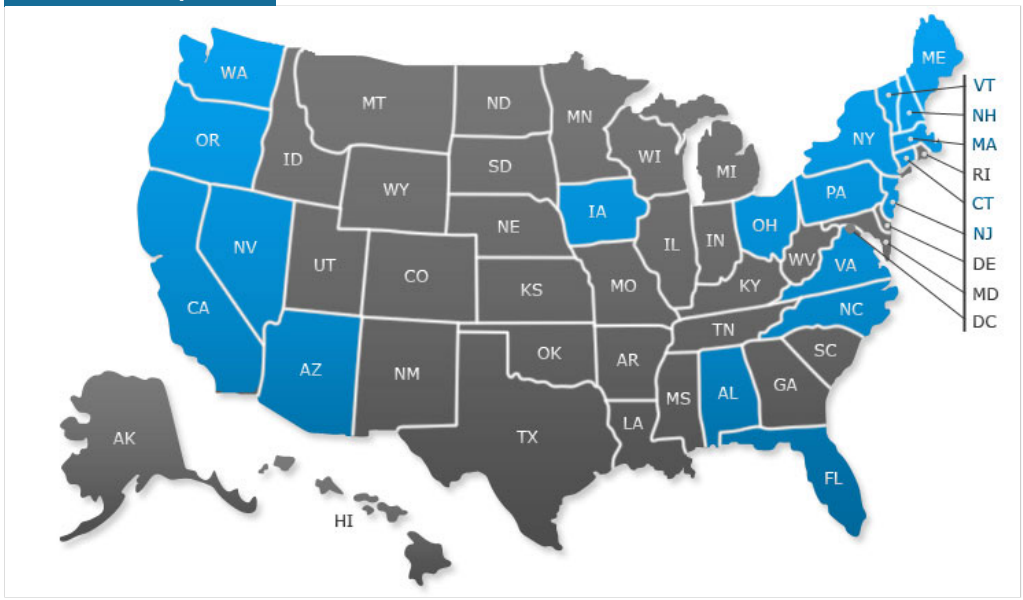
About This Map

Broadly defined, cloud computing (or "Software as a Service") refers to a category of software that's delivered over the Internet via a Web browser (like Internet Explorer) rather than installed directly onto the user's computer. The cloud offers certain advantages in terms of minimal upfront costs, flexibility and mobility, and ease of use.

Because cloud computing places data--including client data--on remote servers outside of the lawyer's direct control, it has given rise to some concerns regarding its acceptability under applicable ethics rules.

Learn more about cloud computing in our brief overview.

Cloud Ethics Opinions



Opinion Summaries

Jurisdiction	Permitted?	Standard?	Specific Requirements or Recommendations
ALABAMA Opinion 2010-02	Yes	Reasonable Care	• Know how provider handles storage/security of data. • Reasonably ensure confidentiality agreement is followed. • Stay abreast of best practice regarding data safeguards.

ARIZONA** Opinion 09-04	Yes	Reasonable Care	• "Reasonable security precautions," including password protection, encryption, etc. • Develop or consult someone with competence in online computer security. • Periodically review security measures.
CALIFORNIA Opinion 2010-179	Yes	Reasonable Care	• Evaluate the nature of the technology, available securit precautions, and limitations third-party access. • Consult an expert if lawyer's technology expertise is lacki • Weigh the sensitivity of the data, the impact of disclosur on the client, the urgency o the situation, and the client instructions.
CONNECTICUT Informal Opinion 2013-07	Yes	Reasonable Care	• Lawyers ownership and acce to the data must not be hindered. • Security policies and process should segregate the lawyer data to prevent unauthorize access to the data, including by the cloud service provide
FLORIDA Opinion 12-3	Yes	Reasonable Care	• Ensure provider has enforceable obligation to preserve confidentiality and security, and will provide notice if served with process • Investigate provider's securi measures • Guard against reasonably foreseeable attempts to infiltrate data.
IOWA Opinion 11-01	Yes	Reasonable Care	• Ensure unfettered access to your data when it is needed including removing it upon termination of the service. • Determine the degree of protection afforded to the da residing within the cloud service.
MAINE Opinion 207	Yes	Reasonable Care	• Ensure firm technology in general meets professional responsibility constraints. • Review provider's terms of service and/or service level agreements. • Review provider's technolog specifically focusing on secu and backup.
MASSACHUSETTS Opinion 12-03	Yes	Reasonable Care	• Review (and periodically revisit) terms of service, restrictions on access to dat data portability, and vendor' security practices. • Follow clients' express instructions regarding use o cloud technology to store or transmit data.

			• For particularly sensitive clie information, obtain client approval before storing/transmitting via the internet.
NEW HAMPSHIRE Opinion #2012-13/4	Yes	Reasonable Care	• Have a basic understanding technology and stay abreast changes, including privacy la and regulations. • Consider obtaining client's informed consent when stor highly confidential informati • Delete data from the cloud a return it to the client at the conclusion of representation when the file must no longe be preserved. • Make a reasonable effort to ensure cloud providers understand and act in a manner compatible with a lawyer's professional responsibilities.
NEW JERSEY** Opinion 701	Yes	Reasonable Care	• Vendor must have an enforceable obligation to preserve confidentiality and security. • Use available technology to guard against foreseeable attempts to infiltrate data..
NEW YORK Opinion 842	Yes	Reasonable Care	• Vendor must have an enforceable obligation to preserve confidentiality and security, and should notify lawyer if served with process for client data. • Use available technology to guard against foreseeable attempts to infiltrate data. • Investigate vendor security practices and periodically review to be sure they rema up-to-date. • Investigate any potential security breaches or lapses l vendor to ensure client data was not compromised.
NEVADA Opinion 33	Yes	Reasonable Care	• Chose a vendor that can be reasonably relied upon to ke client information confidenti • Instruct and require the vendor to keep client information confidential.
NORTH CAROLINA 2011 Formal Ethics Opinion 6	Yes	Reasonable Care	• Review terms and policies, a if necessary re-negotiate, to ensure they're consistent w ethical obligations. • Evaluate vendor's security measures and backup strategy. • Ensure data can be retrieve vendor shuts down or lawye wishes to cancel service.
			• Competently select appropri vendor.

OHIO Informal Advisory Opinion 2013-03	Yes	Reasonable Care	• Preserve confidentiality and safeguard client property. • Provide reasonable supervisi of cloud vendor. • Communicate with the clien as appropriate.
OREGON Opinion 2011-188	Yes	Reasonable Care	• Ensure service agreement requires vendor to preserve confidentiality and security. • Require notice in the event that lawyer's data is accesse by a non-authorized party. • Ensure adequate backup. • Re-evaluate precautionary steps periodically in light of advances in technology.
PENNSYLVANIA Opinion 2011-200	Yes	Reasonable Care	• Exercise reasonable care to ensure materials stored in t cloud remain confidential. • Employ reasonable safeguar to protect data from breach, data loss, and other risk. • See full opinion for 15 point of possible safeguards.
VERMONT Opinion 2010-6	Yes	Reasonable Care	• Take reasonable precautions ensure client data is secure and accessible. • Consider whether certain ty of data (e.g. wills) must be retained in original paper format. • Discuss appropriateness of cloud storage with client if d is especially sensitive (e.g. trade secrets).
VIRGINIA Legal Ethics Opinion 1872	Yes	Reasonable Care	• Exercise care in selection of the vendor. • Have a reasonable expectati the vendor will keep data confidential and inaccessible • Instruct the vendor to preserve the confidentiality information.
WASHINGTON** Advisory Opinion 2215	Yes	Reasonable Care	• Conduct a due diligence investigation of any potentia provider. • Stay abreast of changes in technology. • Review providers security procedures periodically.
WISCONSIN Opinion EF-15-01	Yes	Reasonable Care	• Consider the sensitivity of th data, the impact of the disclosure, the client's circumstances and instructi • Consult an expert if lawyer's technology expertise is lacki • Understand/know the experience and reputation o the service provider and the terms of their agreement.

* Note that in most opinions, the specific steps or factors listed are intended as non-binding recommendations or suggestions. Bes

practices may evolve depending on the sensitivity of the data or changes in the technology.

** These opinions address issues which aren't directly labled cloud computing or software as a service, but which share similar technology (e.g.. online backup and file storage).

Disclaimer

See an error? Are we missing an opinion? Let us know.

Cloud Ethics Opinions Around the U.S.

Cloud Ethics Opinions

There's a compelling business case for cloud computing, but can lawyers use it ethically? We've compiled these comparison charts to help you make the right decision for your practice.

What is Cloud Computing?

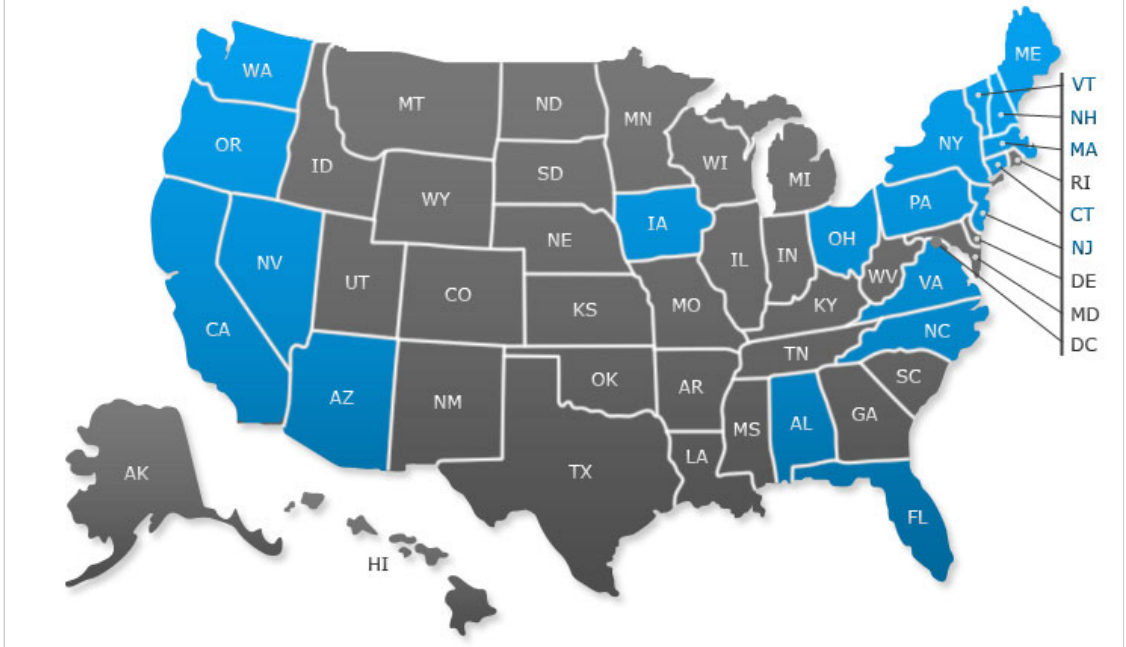
About This Map

Broadly defined, cloud computing (or "Software as a Service") refers to a category of software that's delivered over the Internet via a Web browser (like Internet Explorer) rather than installed directly onto the user's computer. The cloud offers certain advantages in terms of minimal upfront costs, flexibility and mobility, and ease of use.

Because cloud computing places data--including client data--on remote servers outside of the lawyer's direct control, it has given rise to some concerns regarding its acceptability under applicable ethics rules.

Learn more about cloud computing in our brief overview.

Cloud Ethics Opinions



Quick Reference

Jurisdiction	Summary of Opinion
	The Alabama Disciplinary Commission examined cloud computing specifically within the context of storing and producing client files. In that context, the Commission recognized certain benefits of cloud computing, including "the lawyer's increased access to client data" and the possibility that it may also "allow clients greater access to their own files over the internet." That said, the

ALABAMA Opinion 2010-02	Commission recognized the "confidentiality issues that arise with the use of 'cloud computing,'" specifically that "[c]lient confidences and secrets are no longer under the direct control of the lawyer or his law firm." After reviewing other opinions from both Arizona and Nevada, the Commission eventually concluded "that a lawyer may use "cloud computing" or third-party providers to store client data provided that the attorney exercises reasonable care in doing so." The Commission defined reasonable care as requiring the lawyer to: • Learn how the provider would handle the storage and security of the data; • Reasonably ensure that the provider abides by a confidentiality agreement in handling the data; • Stay abreast of appropriate safeguards that should be employed by both the lawyer and the third-party. In the event that a breach of confidentiality occurs, "the focus of the inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider." Finally, with regard to client files generally, the Commission emphasized that the the format the lawyer uses to store client documents must allow the lawyer "to reproduce the documents in their original paper format," and that the lawyer "must abide by the client's decision in whether to produce the file in its electronic format ... or in its original paper format."
ARIZONA Opinion 09-04	The State Bar of Arizona's Ethics Committee reviewed a query from an Arizona lawyer interested in using "an encrypted online file storage and retrieval system for clients in which all documents are converted to password-protected PDF format and stored in online folders with unique, randomly-generated alpha-numeric names and passwords." In an earlier 2005 opinion, Arizona's Committee had already approved electronic storage of client files where the lawyer or law firm takes "competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence." The opinion stated that there were a "panoply of electronic and other measures ... available to assist an attorney" in this regard, and that specific reasonable precautions included "firewalls, password protection schemes, encryption, anti-virus measures, etc." The opinion concluded that the "proposed online client file system appears to meet the requirements" outlined by the rules and the earlier ethics opinion, but did stress that "technology advances may make certain protective measures obsolete over time" and therefore "lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information."
CALIFORNIA Opinion 2010-179	Recognizing that a technology-by-technology analysis "would likely become obsolete" in a short amount of time, the State Bar of California's Standing Committee on Professional Responsibility and Conduct instead issued an opinion that "sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology." The Committee stated that "transmission of information through a third party reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information," but that the "manner in which an attorney acts to safeguard confidential information is governed by the duty of competence." Examining the issue of competence, the Committee declares that "the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney's handling of such information does not result in a waiver of any privileges or protections." The Committee next examines several factors that an attorney should consider before using a given type of technology. These include: • The nature of the technology in relation to more traditional counterparts (i.e. e-mail versus mail). • Reasonable precautions possible to improve the security of a given technology. • Limitations on who can monitor the use of technology and disclose activity.

	• The lawyer's own level of technological competence, and whether it's necessary to consult with an expert. • Legal ramifications to third parties for intercepting or otherwise interfering with electronic information. • The sensitivity of the data. • Impact of possible disclosure on the client. • Urgency of the situation. • Client instructions. Summing up the opinion, the Committee states that a lawyer must take the appropriate steps to ensure that technology use "does not subject confidential client information to an undue risk of unauthorized disclosure" and must "monitor the efficacy of such steps" on an ongoing basis.
CONNECTICUT Informal Opinion 2013-07	Addressing the question of "whether it is permissible under the Rules of Professional Responsibility for a lawyer to use cloud computing in the practice of law," the Connecticut Bar Association's Professional Ethics Committee found that "Lawyers who use cloud computing have a duty to understand its potential impact on their obligations under applicable law and under the Rules of Professional Responsibility." The opinion noted that "Lawyers' remote storage of data is not a new phenomenon; lawyers have been using off-site storage providers for many years, and the issues remain the same whether tangible records are stored in a 'brick-and-mortar' warehouse or intangible data is stored on third party servers." Recognizing the new ABA Model Rule 1.1 comment that lawyers should "keep abreast of changes in the law and practice, including the benefits and risks associated associated with relevant technology, the Committee concluded that "[i]n order to determine whether use of a particular technology or hiring a particular service provider is consistent or compliant with the lawyer's professional obligations, a lawyer must engage in due diligence." The Committee discussed several rules to be considered when engaged in this due diligence. They include: • Rule 1.6(a) - the prohibition against revealing confidential information of a client • Rule 1.15 - which requires that property of clients and third persons which the lawyer receives should be 'appropriately safeguarded.' • Rule 5.3 - which addresses a lawyer's duties regarding nonlawyers employed or retained by / associated with a lawyer This reference to Rule 5.3 seems to be the most important consideration for the Committee. In concluding its opinion, the Committee states that "the lawyer outsourcing cloud computing tasks...must exercise reasonable efforts to select a cloud service provider who...is able to limit authorized access to the data, ensure that the data is preserved...reasonably available to the lawyer, and reasonably safe from unauthorized intrusion."
FLORIDA Opinion 12-3	The Professional Ethics Committee of the Florida Bar examined the issues surrounding lawyers' use of cloud computing because it "raises ethics concerns of confidentiality, competence, and proper supervision of nonlawyers." After identifying that confidentiality was the primary concern, the Committee stated that lawyers have an obligation "To maintain as confidential all information that relates to a client's representation, regardless of the source," and that obligation extends to ensuring the "confidentiality of information … maintained by nonlawyers under the lawyer's supervision, including nonlawyers that are third parties used by the lawyer in the provision of legal services." Added to a lawyers obligation to remain current on developments in technology that affect the practice of law, the Committee concludes that lawyers using cloud technology "have an ethical obligation to understand the technology they are using and how it potentially impacts confidentiality of information relating to client matters, so that the lawyers may take appropriate steps to comply with their ethical obligations." After a review of comparable ethics opinions from other state and local bars, the Committee determined that it agreed with their general finding: cloud

	computing is permissible "as long as the lawyer adequately addresses the potential risks associated with it." The Committee goes on to favorably cite the New York State Bar Ethics Opinion 842 with regard to specific due diligence steps, and likewise notes Iowa's Ethics Opinion 11-01 which lists appropriate considerations including using secure passwords, encrypting where possible, and more. Finally, the Committee adds an additional note that lawyers should "consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information."
IOWA Opinion 11-01	The Iowa State Bar Association's Ethics Committee evaluated the broad question of whether a lawyer or law firm may use cloud computing or Software as a Service (SaaS). The Committee chose to take a "reasonable and flexible approach to guide a lawyer's use of ever-changing technology" that "places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly." The opinion stressed that lawyers wishing to use SaaS "must ensure that there is unfettered access to the data when it is needed" and that lawyers must also "determine the nature and degree of protection that will be afforded the data while residing elsewhere." In describing these two key requirements, the opinion explores a number of questions that lawyers may need to ask before using such a service, including questions about the legitimacy of the provider, the location where data will be stored, the ability to remove data from the service, and so forth. In terms of data protection, the opinion stresses the need to perform due diligence regarding password protection, access to data, and the ability to encrypt data used in such a service. The opinion concludes by noting that performing due diligence "can be complex and requires specialized knowledge and skill," but allows that lawyers may discharge their ethical duties "by relying on the due diligence services of independent companies, bar associations or other similar organizations or through its own qualified employees."
MAINE Opinion 207	In earlier Opinion 194, the Maine State Bar Association's Professional Ethics Commission conducted a limited review of confidential firm data held electronically and potentially handled by third-party vendors and technicians. Though not directly addressing the cloud, the opinion covered enough common issues that it was previously included in this comparison chart. In January 2013, the Commission revisited the matter to "remove any uncertainty … by squarely and formally addressing the issue" of cloud computing and storage. Overall, the Commission determined that use of such technology was permissible if "safeguards are in place to ensure that the attorney's use of this technology does not result in the violation of any of the attorney's obligations under the various Maine Rules of Professional Conduct." As part of its review, the Commission noted that a number of rules were implicated by the use of cloud technology including 1.1, 1.3, 1.4, 1.6, 1.15, 1.16, 1.17, and 5.3. Yet at the same time, the Commission notes that the "overriding ethical constraints on counsel" have not changed with the evolution of technology; rather, the steps lawyers must take to satisfy those constraints have changed. The Commission notes several internal policies and procedures that lawyers should consider to satisfy their obligations generally under the Rules, including backing up firm data, protecting the firm's network with a firewall, limiting information provided to third parties, and much more. The full list of suggested policies runs to 10 items and draws heavily on Pennsylvania Formal Opinion 2011-200. In addition to these general suggestions regarding firm's technology, the Commission suggests that firm's should also carefully review the terms of service or SLA with providers and ensure adequate recognition of the lawyers' professional responsibilities. In addition, lawyers should ensure data will be accessible if the service is terminated and that data will be destroyed at the request of the firm. Finally, lawyers should review the provider's security and backup policies.

	The Commission goes on to provide some specific guidance regarding how a lawyer may evaluate the provider's technology and terms, including determining ownership of data, the provider's ability to withstand infiltration attempts, and so on. While the opinion includes several lengthy lists of suggested policies and steps to meet ethical obligations, the Commission is clear that the "dynamic nature of the technology make it impossible to list criteria that apply to all situations for all time" and thus adopts the view articulated by the North Carolina Ethics Committee that lawyers must stay educated "on computer technology as it changes and as it is challenged by and reacts to additional indirect factors such as third party hackers or technical failures."
MASSACHUSETTS Opinion 12-03	In this opinion, the Massachusetts Bar Association examined cloud computing in the context of a lawyer who wished to synchronize his files, including confidential client files, between multiple computers using a solution like Google Docs. The MBA recognized that other options were available and drafted the opinion to generally address storage of data in "Internet based storage solutions." Reviewing past opinions that dealt with electronic data and the duty to preserve confidentiality, the MBA Committee concluded that the "the use of an Internet based storage provider to store confidential client information would not violate Massachusetts Rule of Professional Conduct 1.6(a) in ordinary circumstances *as long as* Lawyer undertakes reasonable efforts to ensure that the provider's data privacy policies, practices and procedures are compatible with Lawyer's professional obligations." [Emphasis in the original.] The MBA Committee goes on to list several examples of "reasonable efforts," including examining the provider's written policies and procedures regarding confidential data, ensuring that those terms prohibit unauthorized access to data, ensuring that the lawyer will have reasonable access to and control over the data, examining the provider's security practices (e.g. encryption, password protection) and service history, and periodically revisiting these topics to ensure continued acceptability. The Committee also stresses that a lawyer "remains bound to follow an express instruction from his client that the client's confidential information not be stored or transmitted by means of the Internet" and also that a lawyer "should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so." Finally, the Committee concludes by stating that ultimate responsibility for determining whether to use a cloud computing solution resides with the lawyer, who must make the determination "based on the criteria set forth in this opinion, the information that he is reasonably able to obtain regarding the relative security of the various alternatives that are available, and his own sound professional judgment."
NEW HAMPSHIRE Opinion 2012-13/4	Recognizing that technology has become pervasive in the practice, and that cloud computing in particular "is already a part of many devices" including smartphones and web-based email, New Hampshire sets out to explore the "effect on the lawyer's professional responsibilities." The opinion focuses on four specific rules: Rule 1.1 Competence, Rule 1.6 Confidentiality, Rule 1.15 Safekeeping Property, and Rule 5.3 Responsibilities Regarding Nonlawyer Assistants. Beginning with Rule 1.1, the opinion notes that recent changes to the comments of ABA Model Rule 1.1 specifically reference the need to "keep abreast of changes in the law and its practice, including the benefits or risks associated with relevant technology." As a result, the opinion stresses that a competent lawyer wishing to use the cloud must understand and guard against the risks inherent to it, and must stay abreast of changes in the technology, privacy laws, and applicable regulations. On Rule 1.6, the opinion again looks at recent changes to the ABA Model Rules, particularly the factors relating to the reasonableness of a lawyers efforts to keep information confidential. As the relative sensitivity of the information is among those factors, and because not all information is alike, New Hampshire states that "consent of the client to use cloud computing may be necessary" where information is highly sensitive. On Rule 1.15, the opinion discusses the need to safeguard the client's property-

	-including the client file. Where the contents of that file are stored in the cloud, the lawyer must "take reasonable steps to ensure that the electronic data stored in the cloud is secure and available while representing a client," and that the data can be deleted from the cloud and returned to the client "after representation is concluded or when the lawyer decides to no longer preserve the file." Finally on Rule 5.3, New Hampshire identifies cloud computing as a form of outsourcing and notes that this requires the lawyer to "make reasonable efforts to ensure that the provider understands and is capable of complying with its obligation to act in a matter compatible with the lawyer's own professional responsibilities." The opinion goes on to stress that this applies as well to any intermediaries the attorney may employee in selecting a provider - e.g. technology consultants or support staff. While New Hampshire is clear that its opinion addresses a lawyer's obligations and not the technical requirements of the cloud providers, it does conclude with a list of issues which an attorney must address before using the cloud. These include checking the provider's reputation, assessing their security measures, and reviewing the terms of service among other factors.
NEW JERSEY Opinion 701	The opinion from New Jersey's Advisory Committee on Professional Ethics does not focus on cloud-computing specifically, but on the more general topic of storing client files in digital format (e.g. PDF). The committee notes that per an earlier opinion (Opinion 692), certain types of documents are considered "property of the client" and therefore "cannot be preserved...merely by digitizing them in electronic form." The Committee states, however, that "there is nothing in the RPCs that mandates a particular medium of archiving" for other common document types typically included in the client file, such as correspondence, pleadings, memoranda and briefs. Indeed, the Committee states that the lawyer's "paramount consideration is the ability to represent the client competently, and given the advances of technology, a lawyer's ability to discharge those duties may very well be enhanced by having client documents available in electronic form." The Committee goes on to state that putting client documents online through a secure website "has the potential of enhancing communications between lawyer and client, and promotes the values embraced in RPC 1.4." The Committee does acknowledge that electronic document storage presents some risk of unauthorized access, and emphasizes that a lawyer's obligation to maintain client confidentiality "requires that the attorney take reasonable affirmative steps to guard against the risk of inadvertent disclosure." Reasonable care in this case "does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access." When a lawyer entrusts confidential data to an outside party, however, the "touchstone" for reasonable care requires that "(1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data."
NEW YORK Opinion 842	The New York State Bar Association's Committee on Professional Ethics examined the question of whether a lawyer could store client's confidential information online without violating professional responsibility rules, and if so, what steps the lawyer should take to ensure the data remains secure. The Committee stresses that a lawyer's duty to maintain client confidentiality includes an affirmative duty to exercise reasonable care in protecting confidential data. This includes exercising reasonable care to prevent inadvertent disclosure by attorney's staff, but does not mean "that the lawyer guarantees that the information is secure from *any* unauthorized access." The Committee notes that "the exercise of reasonable care may differ from one case to the next" based on the sensitivity of the data. Using online data storage to backup (i.e. preserve) client data is deemed ethically permissible where the lawyer has exercised reasonable care "to ensure that the system is secure and that client confidentiality will be maintained." The Committee suggests that this might include ensuring that the vendor has an enforceable obligation to preserve confidentiality and security and will notify the lawyer if served with process requiring production of client data, investigating the vendor's security and backup procedures, and using available technology to

	guard against reasonably foreseeable attempts to infiltrate it. The Committee also writes that lawyers "should periodically reconfirm that the vendor's security measures remain effective in light of advances in technology." If the vendor's methods are insufficient or if the lawyer learns of any breaches effecting the vendor, the lawyer must investigate to be sure his or her clients' data wasn't compromised and if necessary discontinue use of the vendor's service. Lawyers should also stay abreast of general developments in technology insofar as they impact the transmission or storage of electronic files.
NEVADA Opinion 33	The State Bar of Nevada's Standing Committee on Ethics and Professional Responsibility examined whether a lawyer violated their professional responsibility rules "by storing confidential client information and/or communications, without client consent, in an electronic format on a server or other device that is not exclusively in the lawyer's control." The Committee provided that a lawyer "must act competently to safeguard against inadvertent or unauthorized disclosure of confidential client information" by taking "reasonable precautions." The Committee likened the storage of data online to the storage of paper documents in a third-party warehouse, and stated that this was permissible "so long as the attorney observes the usual obligations applicable to such arrangements." This would include, for example, choosing a vendor that "can be reasonably relied upon to maintain the confidentiality" of client data. The opinion also noted that client consent isn't necessary, but that a client "may give informed consent to a means of protection that might otherwise be considered insufficient."
NORTH CAROLINA 2011 Formal Ethics Opinion 6	The North Carolina State Bar's Ethics Committee examined two broad questions in its opinion on cloud computing: first, may a lawyer use cloud computing or software as a service, and second, what measures should a lawyer consider when evaluating a vendor or seeking to reduce the risks associated with the cloud? On the first subject, the Committee's answer is straightforward: yes, lawyers may use the cloud, "provided steps are taken to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property." In taking these steps, the lawyer should apply "the same diligence and competency to manag[ing] the risks of SaaS that the lawyer is required to apply when representing clients." On the broader question of the appropriate measures a lawyer should take, the Committee begins by stating hat it "does not set forth specific security requirements because mandatory security measures would create a false sense of security in an environment where the risks are continually changing." Rather, the Committee urges lawyers to exercise due diligence and educate themselves regularly about the subject. The Committee does recommend several security measures, however, which includes reviewing applicable terms and policies, and if necessary, negotiating terms regarding how confidential data will be handled. The Committee also suggests that the lawyer have a method of retrieving data if they leave the service or the vendor goes out of business, that the lawyer review the vendor's backup strategy, and finally that the lawyer evaluate the vendor's overall security measures.
	The OSBA Informal Advisory Opinion examines a question of "whether [a] law firm may use a third-party vendor to store client data 'in the cloud.'" While acknowledging that previous opinions and rules have traditionally examined "older data storage methods," the Professional Committee writes that the "issues and ethical duties regarding cloud storage are analogous to the ones that apply when lawyers opt to use a vendor to store their paper files offsite rather than in their own offices." Thus, the Committee opts to take a "practical" approach by "applying existing principles to new technological advances while refraining from mandating specific practices." More specifically, the Committee notes that rules about specific security measures would be superseded quickly by technological advances. The Committee addresses the matter in four areas. First, it states that lawyers

OHIO Informal Advisory Opinion 2013-03	must "exercise 'due diligence as to the qualifications and reputation of those to whom services are outsourced,' and also as to whether the outside vendor will itself provide the requested services competently and diligently." The Committee specifically suggests a Service Level Agreement and offers some guidance on the types of questions that vendors should be asked. Next, the Committee looks at confidentiality and states that lawyers have a "duty…to maintain the confidentiality of all client data relating to the representation, irrespective of the form of that data, and to carry out that duty with due regard for the form that the data is in." To preserve the confidentiality, a lawyer must exercise competence "(1) in selecting an appropriate vendor, (2) in staying abreast of technology issues that have an impact on client data storage and (3) in considering whether any special circumstances call for extra protection for particularly sensitive client information or for refraining from using the cloud to store such particularly sensitive data." The Committee notes that terms of service that provide or suggest that the vendor has an ownership interest in the data "would violate the duty to keep client property 'identified as such'." Third, the Committee looks at supervision of cloud vendors and states that putting data in the cloud "is almost by definition a service that lawyers will out-source," thus "lawyers who contract with a cloud-storage vendor must make reasonable efforts to ensure that the vendor's conduct is compatible with the lawyer's own professional obligations." On the fourth and final issue, the Committee states that lawyers should use judgment to determine if the circumstances require consultation with the client regarding the use of cloud computing. That might arise where the data is of a particularly sensitive nature.
OREGON Opinion 2011-188	The Oregon Committee found that a lawyer "may store client materials on a third-party server as long as Lawyer complies with the duties of competence and confidentiality to reasonably keep the client's information secure within a given situation." That compliance requires "reasonable steps" to ensure that the storage company will secure the client data and preserve its confidentiality. The Committee stated that in some circumstances it may be sufficient for the vendor to be compliant with "industry standards relating to confidentiality and security," but only where those standards "meet the minimum requirements imposed on the Lawyer by the Oregon RPCs. As examples of these requirements, the Committee suggests that lawyers should ensure that "the service agreement requires the vendor to preserve the confidentiality and security of the materials," and that the vendor notify the lawyer if there's any non authorized third-party access to the lawyer's files. The opinion also suggests that lawyers should "investigate how the vendor backs up and stores its data and metadata." Finally, the Committee notes that the reasonableness of the lawyer's protective measures will be judged based on the technology available at the time of disclosure. In other words, the "vendor's protective measures may become less secure or obsolete over time" and therefore the lawyer must reevaluate the measures periodically.
	The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility begins its opinion by recognizing that advances in technology, including the cloud, offer opportunities to "reduce costs, improve efficiency and provide better client service." There's also a genuine risk of data breach, particularly given a recent FBI warning that law firms are "being specifically targeted by hackers who have designs on accessing the firms' databases." Noting that an earlier informal opinion (2010-060) had found that a lawyer 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," the Committee dedicates most of this formal opinion to addressing the nature of those "reasonable" efforts. The Committee provides a 15 point list of possible steps a firm "may" take in exercising reasonable care with cloud computing. Several of these steps are routine elements of preserving client confidentiality (e.g. "[r]efusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission"), but others focus on specific technology issues:

PENNSYLVANIA Opinion 2011-200	• Backing up firm data and maintaining onsite copies; • Using encryption to protect confidential data, including backups; • Developing a plan to address security breaches, including possible notifications to clients; • Evaluating the vendor regarding data ownership, security precautions, the location of data centers, data portability, and more; • Providing training to firm staff that will use the cloud tool, including instruction on password best practices; • Having an backup internet connection. Pennsylvania attorneys should review the *full list* published in the opinion. The opinion goes on to stress that "some data may be too important to risk inclusion in cloud services," and also notes that most states have data breach notification laws that lawyers should be familiar with and adhere to in the event that a data breach occurs. The opinion also addresses the question of web-based email, which the Pennsylvania Committee lists as a type of cloud computing. It suggests that attorneys take reasonable precautions "to minimize the risk of unauthorized access to sensitive client information" when using webmail, possibly including specific steps like "encryption and strong password protection"--especially when the data is of a particularly sensitive nature.
VERMONT Opinion 2010-6	The Vermont Bar Association's Professional Responsibility Section addressed the "propriety of use by attorneys and law firms of Software as a Service ("SaaS") which is also known as Cloud Computing." In its analysis, it looked at storing client data in the cloud, possible data types that should not be stored online, as well as specific Cloud uses such as web-based email, calendaring, and remote document synchronization. A significant portion of the Section's analysis is focused on reviewing other recent cloud computing ethics opinions from other jurisdictions, including North Carolina, California, and New York. Drawing upon these opinions and its own analysis, the Section "agrees with the consensus view" that lawyers are obligated to provide "competent representation" while "maintaining confidentiality of client information, and protecting client property in their possession." In choosing whether to use new technologies, including the cloud, lawyers must exercise their due diligence. The Section provides a list of steps a lawyer may take, though it stresses that is not providing a formal "checklist of factors a lawyer must examine." This loose list of factors includes reviewing the vendor's security, checking for limitations on access to or protection of data, reviewing terms of service, examining vendor confidentiality policies, weighing the sensitivity of data placed in the cloud, reviewing other regulatory obligations, and requiring notice if a third party accesses or requests access to data. In addition to those factors, the Section adds that a lawyer may consider giving notice to the client when using the cloud to store client's data, and may want to look to expert third parties to review the vendor's security and access systems. Finally, the Section stresses that lawyers should take "reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present."
VIRGINIA Legal Ethics Opinion 1872	Virginia Legal Ethics Opinion 1872 examines a variety of ethical issues associated with virtual law offices, including the use of cloud computing. This summary focuses specifically on the elements of the opinion dealing with cloud computing, but readers are encouraged to view the full text of the opinion to understand the context. The opinion begins by stating that lawyers "must always act competently to protect the confidentiality of client information, regardless of how that information is stored/transmitted," but notes that the task may be more challenging when the information is being "transmitted and/or stored electronically through third-party software and storage providers." The opinion notes that the duty is not to "absolutely guarantee that a brief of confidentiality cannot occur," only to "act with reasonable care to protect information relating to the representation of a client."

	Specifically, lawyers are instructed to carefully select vendors, instruct the vendor to preserve confidentiality, and to have a reasonable expectation that the vendor will in fact keep data confidential and inaccessible. To do that, lawyers must "examine the third party provider's use of technology and terms of service" and, if they're unable to make an assessment on their own, "consult with someone qualified to make that determination."
WASHINGTON Advisory Opinion 2215	In Advisory Opinion 2215, the Washington State Bar Association's Rules of Professional Conduct Committee examined lawyers' ethical obligations relating "to the use of online data storage managed by third party vendors to store confidential client documents." The opinion focused specifically on data storage rather than the broader category of cloud computing, but addressed many issues common to both platforms. In its analysis, the Committee noted that such an arrangement places "confidential client information … outside of the direct control of the lawyer" and thus raises some concern. In particular, the Committee notes lawyers' obligations to preserve confidentiality under RPC 1.6 and to protect client property under RPC 1.15A. Acknowledging that specific guidelines regarding security are impossible "because the technology is changing too rapidly," and also noting that it's "impractical to expect every lawyer who uses such services to be able to understand the technology sufficiently in order to evaluate a particular service provider's systems," the Committee nonetheless suggested that a lawyer must conduct a due diligence investigation of the provider and "cannot rely on lack of technological sophistication to excuse the failure to do so." The Committee offered several steps to conduct such a due diligence investigation, including familiarizing oneself with the risks of online data storage, evaluating the provider's history, comparing terms with other providers, ensuring notice of any non-authorized access to lawyer's data, and generally ensuring that data is secured and backed up. Finally, the Committee also noted that under RPC 1.1 a lawyer has a duty to stay abreast of changes in the law and its practice, and that necessarily includes staying informed about the risks associated with the technology the lawyer employs in his or her practice. As technology evolves, the lawyer must also "monitor and regularly review the security measures of the provider" he or she uses for online data storage.
WISCONSIN Opinion EF-15-01	Wisconsin Formal Ethics Opinion EF-15-01 (Ethical Obligations of Attorneys Using Cloud Computing), issued by the State Bar of Wisconsin's Professional Ethics Committee, notes that increased lawyer accessibility to cloud-based platforms and services comes with a direct loss of control over client information but that lawyers can use cloud computing services if the lawyer uses reasonable efforts to adequately address the potential risks associated with it. "To be reasonable," the opinion states, "the lawyer's efforts must be commensurate with the risks presented." The opinion acknowledges that lawyers cannot guard against every conceivable danger when using cloud-based services, but lists numerous factors to consider when assessing the risk of using cloud-based services in their practices: • The information's sensitivity • The client's instructions and circumstances • The possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party • The attorney's ability to assess the technology's level of security • The likelihood of disclosure if additional safeguards are not employed • The cost of employing additional safeguards • The difficulty of implementing the safeguards • The extent to which the safeguards adversely affect the lawyer's ability to represent clients • The need for increased accessibility and the urgency of the situation • The experience and reputation of the service provider • The terms of the agreement with the service provider • The legal and ethical environments of the jurisdictions in which the services

will be performed, particularly with regard to confidentiality

The opinion also states that in determining what efforts are reasonable to address the cloud-computing risk, lawyers should understand a number of computer security concepts:

- Firewalls
- Virus and spyware programs
- Operating system updates
- Strong passwords and multifactor identification
- Encryption for stored information
- Dangers of using public wi-fi
- Risks of file-sharing sites
- Options for using a virtual private network (VPN)
- The importance of regularly backing up data

Disclaimer

Attachment C:

Sample Checklist of Factors and Considerations for

"Reasonable Care" Standard and Selecting Service Providers

1. Develop an Understanding of Cybersecurity Benefits and Risks - Internal and External

- Have a basic understanding of technology and stay abreast of changes, including in privacy laws and regulations and data security.

- Consider data at various phases of representation (in use, in transit, and in storage) to help identify where potential risks may lie and appropriate measures at the different phases to mitigate risks.

- Risks may come from many sources—the dangers arise not just from attacks launched by cyberspace bad guys, but also malicious acts by disgruntled employees (or former employees if access is not promptly terminated), and innocent mistakes by personnel (such as opening attachments with viruses, malware, spyware and other nefarious tools used by cybercriminals).

- Risks include unauthorized access/theft; destruction or loss of documents and information; and down-time and unavailability/accessibility.

- What is your (or your staff's) ability to assess the level of security that will be provided through a particular technology, or the abilities of a proposed service provider, or the reasonableness of the provider's standard contractual service terms? Technology is fast moving and is, well, technical. Talk with a consultant or hire an IT professional with cybersecurity knowledge and experience to develop a firm plan.

2. Due Diligence and Assessments

- Evaluating Needs—Why do you need cloud computing: data storage only; client demands; decreased cost; space considerations; work flexibility and mobility? Determine scope of data and amount of storage space needed.

- Confidentiality and Security Evaluation and Measures—there is a broad range of services with differing levels of security and vulnerabilities.

- Assess sensitivity of data—Evaluate propriety of electronic storage only (hard copy originals may be necessary, e.g., wills), and levels of security that may be required to protect firm financial information, attorney-client privileged communications, confidential client information, and "highly-confidential" client information, like trade secrets. Different levels of protection may be appropriate for different types of data.

    - For a particular technology or service, assess the likelihood of unauthorized disclosure if additional safeguards are not used.

- Assess costs of implementing various cloud computing processes, in whole or in part, as well as practical ability of firm attorneys and staff to maintain security protocols.
    - Difficulty/ease in implementing the additional safeguards
    - Would additional safeguards interfere with effective representation—in what manner?
        - Speed of access and retrieval—and what speed is needed for effective representation?
        - Ability to access and share data with authorized third parties
- Encryption—Determine whether the firm will have the ability to encrypt data as stored, in transit, or while in use, or if all or portions of the data can be encrypted (control of encryption key).
- Has the client instructed or requested that you use particular service providers or security measures?
    - How do these providers or tools measure up to the providers and standards that you otherwise use?
    - If concerns as to their security, is there are possibility that using those services may create vulnerabilities in your system?

- Availability, access, and portability
    - What are the potential downtimes in accessibility? At this time 99.9% uptime is common, but some service providers offer uptimes approaching 99.999% (according to Wisconsin Formal Ethics Opinion EF-15-01 (Mar. 23, 2015), see page 12).
    - What are data retention terms and measures?
    - Evaluate plans to recover data at any time to transfer to new vendor (data format, time to transfer, what happens to data at termination of contract, if the contract is unpaid, or if the vendor goes out of business).
    - What back-up measures should be used? Determine whether vendor has redundant and off-site back-up systems and power sources to protect data (from physical and cybersecurity threats).
    - Consider if you have data so critical to the representation that maintaining a hard copy back-up is appropriate.

- Selection of Service Provider—Make a reasonable effort to ensure cloud providers understand and act in a manner compatible with professional responsibilities and client demands. Healthcare and financial institutions demand greater levels of security because of the legal obligations to protect personal health information and

financial information. Factors to consider include:

- Evaluate range of services available and needed (data storage only, software application hosting, mission-critical systems) and identify vendors who can provide all required services.

- Experience and reputation of the service provider—Determine vendor's track record (data breach experience and response to prior breaches; interruption of service; customer references; length of time in business; financial security; frequency and thoroughness of security audits; certification that vendor meets industry standards).

- Standards and protocols used by the service provider

    - Does it follow industry cybersecurity standards? Can you ensure that these standards are followed in reality?

    - Consider whether the provider has received certification by a recognized third party that the vendor's cybersecurity policies and practices meet industry standards.

- Terms of its Service Agreement—It is essential that you carefully review the service agreements with any proposed service provider (these are often called "Service Level Agreements"). See below under "Agreement with Providers."

- Subcontractors

    - Does the service provider use subcontractors, or have the right under the services agreement to use subcontractors to provide services to you?

    - If so, what assurances are there regarding trustworthiness, reliability, and abilities of the subcontractors?

    - If they use subcontractors in some or all phases of services, then your security may be only as good as the weakest link.

- Location of service provider and services

    - Determine where the service providers and data will be transmitted, processed and stored (multiple national or international locations; single source; option to elect location).

    - Do these jurisdictions have laws and authorities that respect and enforce data ownership and security rights? Regardless of laws on the books, how prevalent are cybercrimes?

- Agreement with Service Providers—It is critical that the service agreements with any proposed service provider be carefully reviewed. As a practical matter, many law firms and lawyers may not be in a position to negotiate significant (or possibly any) changes in these agreements. But, one aspect of determining if the provider and service are appropriate for use with client data, is to at least have an understanding

of the provider's terms of service. Some specific terms are discussed below.

- Ownership and Security and Data—an Essential Contract Term
    - It is critical that the service terms contain an explicit agreement that the service provider has no ownership or other interest in the data, and that the lawyer (and/or client) maintains ownership of all data and records.
    - Confirm the provider's obligations for confidential treatment of data (automatic or requires designation). Confirm the extent of the vendor's right, if any, to access or use data; the vendor's use of subcontractors or other cloud providers; employees' and subcontractors' nondisclosure agreements).
- Notifications
    - Does the contract require that the provider give notice of breaches of data security and third party requests (including a warrant or subpoena) for data or access?
    - Establish how the firm will be notified in the event of any changes in physical or cybersecurity protocols.
- Audit rights—Does the service agreement provide you with a right to conduct an audit or otherwise access their system to assess compliance?
- Back-up
    - What are the provider's obligations to use back-up systems?
    - How often does data back-up occur?
- Indemnification—Will the provider indemnify you and be responsible for the costs and damages associated with a service failure or data breach? These may include costs to replace data, reinstitute security and plug breaches, notice to others impacted by breach and consequential damages. Although this is not a requirement under the ethics rules, it is a practical protection for lawyers in the event there is a problem.
- Insurance—Ensure the vendor has insurance against physical or cybersecurity breaches.

3. <u>Ongoing Due Diligence—Monitoring and Policies</u>

- Periodically review security measures, terms of service, service agreements, restrictions on access to data, data portability, back-up policies, technology, and security practices.
- Guard against reasonably foreseeable attempts to infiltrate data with basic protections such as password protection, data encryption, and physical security systems in server areas.

- Employee policies and training

    - Provide periodic training of personnel as to your firm's internet and cybersecurity policies. Develop standards and procedures for employee cloud computing when away from office. Be aware of the dangers of unprotected Wi-Fi and other open access environments (coffee shops, hotels, airports). Consider what secure applications may be implemented on mobile devices.

    - Alert your personnel about evolving types of cyber-attacks to help keep your staff vigilant and informed. Advise employees to report concerns regarding breaches, viruses, or other suspicious activity.

    - Consider developing a "whitelist" of software and applications that lawyers and staff are permitted to use without further approval—at least for certain core functions and activities.

- Conduct periodic analysis and risk assessments to determine if there is any new vulnerability. Technology evolves quickly—both to preserve security and to destroy it—so it is important to make periodic reassessments of technology in use and potential new options.

Regina Amolsch

Regina is a partner with Plave Koch PLC, concentrating her practice in franchising, licensing, and distribution issues, as well as general corporate transactions.

Regina's provides advice and counseling on various commercial, licensing, franchise, corporate and business development matters across a diverse range of industries. Her experience includes structuring new franchise programs and restructuring existing franchise programs; dealership and distribution relationships; re-branding franchise systems; drafting and negotiating franchise, licensing, and distribution agreements, and related commercial contracts; international expansion; terminating and renewing franchise relationships; counseling clients with respect to compliance with state, federal, and international regulatory issues; and assisting in dispute resolution proceedings. She also assists with mergers and acquisitions of franchise companies and exemption-based franchising.

Though active in all area of franchising and licensing, Regina has developed particular interest and experience in the areas of medical franchising, technology, and e-commerce. In the medical and health care field, Regina assists clients expand using franchised and non-franchised licensing programs. She also advises on and prepares Internet-related policies and guidelines for franchise systems and counsels clients on domain name protection, cybersquatting and related issues.

Ms. Amolsch is an active speaker at industry seminars and professional training programs concerning franchising and intellectual property issues and has co-authored articles appearing in various franchise-related publications and seminar presentations.

Before entering law firm practice, Ms. Amolsch served in-house as the Assistant Counsel of Hooters of America, Inc., the national franchisor and operator of the "Hooters" restaurant chain. In that capacity, she directed and managed non-employment litigation and trademark activities; assisted in developing and implementing corporate, franchising, and employment practices and policies; conducted internal investigations of employment claims; and counseled unit managers on legal compliance and company policies and procedures.

Trishanda Treadwell

Trish Treadwell is a partner with Parker Hudson Rainer & Dobbs LLP's Litigation and Employment practice group. She represents clients in state and federal courts in a variety of commercial litigation contexts, primarily including franchise and employment disputes, but also including UCC and other banking litigation and general complex commercial litigation and arbitration.

Trish represents and advises franchise systems in the hotel and quick-service restaurant sectors among others. She has represented franchisors in actions to enforce franchise agreements against franchisees, in actions by third parties asserting vicarious liability against the franchise system, and in more complicated matters involving system-wide class actions and RICO claims. She provides counseling for franchisors with respect to their disclosure documents, franchise agreements, terminations, and other issues.

Trish is actively engaged in the franchise law community and especially within the ABA Forum

on Franchising, having spoken at a previous Forum Conference and authored and co-authored articles for both the Franchise Law Journal and The Franchise Lawyer. She is currently an Associate Editor for the Franchise Law Journal and an active participant in the Forum's Diversity Caucus. Along with co-presenter Robert Salkowski, she also recently presented the Annual Judicial Update at the 2015 International Franchise Association's Legal Symposium.

As part of Trish's employment law practice, she provides counseling, general advice, and litigation representation on a panoply of employment-related issues. Trish represents clients before the Equal Employment Opportunity Commission, the Georgia Department of Labor, and FINRA, as well as in state and federal courts. Representative engagements include claims for discrimination and retaliation based on age, gender, race, religion, and disability; breach of employment agreements; alleged violations of federal and state wage and hour and leave laws; and advice regarding employment handbooks, policies, trade secrets, non-competes and other restrictive covenants, and executive and employee agreements. The recent movements by the NLRB to try to designate franchisors as responsible for franchisees' employees have created an interesting intersection for employment and franchise law practices, and Trish is uniquely positioned to provide counseling and representation on that issue.

Trish graduated with honors from Atlanta-based Oglethorpe University with a Bachelor of Arts in English. She recently concluded her eighth and final year (for now) as a member of the Board of Trustees for the University, including service on the Board's Executive Committee and as chair of the Academic Affairs Committee. After a three-year stint teaching middle school and high school English, Trish attended and graduated with honors from Georgia State University College of Law, where she was Student Writing Associate Editor of the Law Review and president of the Student Bar Association. She also currently serves on her law school alma mater's Board in addition to service on the Board and Executive Committee of the non-profit Trees Atlanta and on the Advisory Council for the Atlanta Legal Aid Society. Trish also remains actively involved in local, state, and national bar associations, including as the new president of the national leadership organization, the Leadership Institute for Women of Color Attorneys.