American Bar Association
42nd Annual Forum on Franchising

Ethics: Keeping Up With Ever Evolving Technology, They Didn't Teach That in Law School

Regina B. Amolsch
Plave Koch PLC
Reston, Virginia

and

Leslie Smith
Foley & Lardner LLP
Miami, Florida

October 16 – 18, 2019
Denver, CO

Table of Contents

I. INTRODUCTION 1

II. THE MODEL RULES OF PROFESSIONAL CONDUCT AND THE REQUIREMENT OF TECHNOLOGY COMPETENCE AND DUTY OF CONFIDENTIALITY 2

A. Model Rules On Technology Competence And Confidentiality Relating To Digital Data And Communications 2

1. Model Rule 1.1: Competence 4

2. Model Rule 1.4: Client Communication 5

3. Model Rule 1.6: Confidentiality Of Information 6

4. Model Rules 1.15 and 1.16: Safekeeping Property And Terminating Representation 8

5. Model Rules 5.1 and 5.2: Responsibilities Of Partners And Subordinate Lawyers 9

6. Model Rule 5.3: Responsibilities Regarding Nonlawyer Assistance 10

B. State Rules Of Professional Conduct Addressing Technology Competence 12

1. Continuing Legal Education 12

2. Use of Nonlawyers To Maintain Competence 13

3. Other Variations And Qualifiers 13

III. MAINTAINING DATA SECURITY 15

A. Types Of Data Security Risks 15

B. Regulatory Considerations 17

C. Data Security Policies 18

D. The Role Of Encryption 19

E. Third Party Vendors: Are They Secure? 20

IV. MAINTAINTING CONFIDENTIALITY WHEN USING TECHNOLOGY 21

A. Overview Of Assessing Risks To Confidentiality In Digital Landscape 21

B. Minimizing Risks When Using Data Connections 22

1. Email 22
2. Voicemail 24
3. Text Messaging And Instant Messaging 24
4. Shared Sites 25
C. Minimizing Risks When Using Common Devices 26
1. Portable Devices And Media 26
2. Discarded Hardware 26
3. Public WiFi Access 27
4. Public Computers 27
5. Client And Guest Access To Law Firm's Computers 29
D. Minimizing Risks Associated With Cloud Computing 29
1. "Reasonable Care" Standard And Selecting Service Providers 29
2. Cloud Computing In Its Various Forms 29
3. Communicating With Clients About Your And Their Cloud Computing Practices 34
V. MANAGING AND MINIMIZING RISKS WITH ELECTRONIC DOCUMENTS 36
A. Electronic Document Production And E-Discovery 36
B. Managing Redactions 37
C. Managing Metadata 38
D. Role Of Artificial Intelligence 39
E. Electronic Document Retention And Destruction 40
VI. SOCIAL MEDIA 41
VII. CONCLUSION 43
ATTACHMENT A - Sample Checklist Of Factors And Considerations For "Reasonable Care" Standard And Selecting Service Providers
Biographies

I. INTRODUCTION

General Omar N. Bradley once said: "If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner." Attorneys should take notice of this cautionary advice. The evolving technology landscape will affect law firms in many ways: managing firm personnel and resources, electronically storing and sharing client data, communicating with clients and other parties, engaging in electronic discovery (including preservation of potential evidence, production and review of electronically stored information), conducting due diligence for transactions, preparing contracts and negotiating on behalf of clients, and preparing and making online regulatory submissions, among others. Emerging technologies that will likely also impact the practice of law include blockchain, data analytics, knowledge management, and artificial intelligence (AI).

The ubiquity of technology in modern life and the commercial world has made it inevitable that lawyers use technology in the practice of law to one extent or another. As such, even without explicit instructions in the applicable ethics rules, lawyers must be aware of technology and how it interacts with their work in order to comply with their ethical obligations to provide competent representation and to protect client information. Addressing this reality, in 2012, the American Bar Association approved changes to ABA's Model Rules of Professional Responsibility (the "Model Rules"),[1] including additional text to make clear that a lawyer's duty of competence requires keeping up to date with relevant technology in the practice of law.[2] Since that time, a majority of states have adopted a duty of technology competence (the changes in state ethics rules are explored further in Section II.B below).

So what does technical competence really mean for practicing attorneys, and what actions are needed to comply with the duty of technical competence? As explored in this paper, the ABA and state ethics authorities have purposely declined to require specific technologies or safeguards. Instead, they have articulated standards for evaluating competence as technologies and circumstances evolve. Because protecting client information and property is a core ethical duty, and that information is now routinely created, stored and transmitted in digital form, it is easy to see the critical intersection of technology and a lawyer's duties of competence and confidentiality. In fact, many of the recent changes in the Model Rules and state ethics rules, and much of the guidance provided in recent state ethics opinions on a lawyer's use of technology, have focused on "cloud computing." Those rules and opinions make clear that a lawyer must understand the risks and benefits of cloud computing technology to use cloud computing technologies and platforms in a manner that competently facilitates the representation and appropriately protects the client's information.

Additionally, some recent state opinions and other authority, including court rules and practices, have implicated the duty of technology competence in litigation involving electronic discovery. The old adage "what you don't know, won't hurt you," does not apply in electronic discovery. A 2015 California opinion, which is discussed further in Part II.C of this paper, illustrates that a litigating attorney's lack of understanding (and failure to associate with others possessing the necessary knowledge) of electronically stored information and electronic

---

[1] 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").

[2] *Id.*, r. 1.1.

discovery methods can have potentially disastrous effects for the client and violate ethical standards.

Lawyers will also face additional dynamics that will impact how they incorporate technology in to their practices, such as the potential to increase efficiency in conducting certain legal tasks and decrease expenses associated with preparing, storing and transmitting records, offering digital resources to clients, and accessing internet-based research tools.

In light of all of these considerations, the particular knowledge, technology and protocols required to render "competent" representation will vary based on the lawyer's field of practice and a variety of other factors. In this paper, we will analyze the foundational ethics rules in this realm, recent changes and developments in the Model Rules and state ethics rules and opinions, and strategies for how to meet those ethical and legal obligations.

II. THE MODEL RULES OF PROFESSIONAL CONDUCT AND THE REQUIREMENT OF TECHNOLOGY COMPETENCE AND DUTY OF CONFIDENTIALITY

To lay the foundation, this paper first discusses the ethical rules that most directly and consequentially address a lawyer's obligations in using technology in their practices. Fifty-five jurisdictions have adopted some version of the Model Rules—all 50 states, the District of Columbia, Guam, Puerto Rico, the Mariana Islands, and the Virgin Islands (recognizing that the states may have variations in their rules and may not adopt any or all Comments).[3] California is the most recent state to adopt new Rules of Professional Conduct patterned after the Model Rules.[4] With that in mind, this paper focuses on the applicability of the ABA's Model Rules as the primary reference in connection with the ethical duty of technology competence. The following two sections discuss the evolution of this issue under the ABA Model Rules and the recent developments in the corresponding state ethics rules as well as a few variations enacted in some states.

A. Model Rules On Technology Competence And Confidentiality Relating To Digital Data And Communications

In connection with the use and understanding of technology, the most relevant Model Rules are: 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; 4.4—Respect for Rights of Third Parties; 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

[3] ABA, Alphabetical List of Jurisdictions Adopting Model Rules, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/alpha_list_state_adopting_model_rules/ (last visited July 23, 2019).

[4] CA ST RPC Rules (as amended by Admin. Order 2018-05-09 (Cal. 2018), effective November 1, 2018) *available at* http://www.calbar.ca.gov/Attorneys/Conduct-Discipline/Rules/Rules-of-Professional-Conduct. *See also* Michael E. McCabe, Jr., *Seeking National Uniformity, California (Finally) Adopts New Ethics Rules*, May 11, 2018, https://www.ipethicslaw.com/seeking-national-uniformity-california-finally-adopts-new-ethics-rules/.

to which the client is entitled; and reasonably ensure that lawyers, legal assistants and service providers are familiar with and acting in a manner consistent with the Model Rules.

The ABA has a long history in revising the model ethical standards to reflect the changing landscape and circumstances that affect modern legal practice. In the past twenty-odd years, advancements in technology, particularly the use of the internet, digital communications, and the potential threats in cyberspace, have been important considerations for the ABA.[5] The ABA's Ethics 2000 Commission added two comments to Model Rule 1.6. titled "Confidentiality of Information." The Commission added Comment 15 to reiterate 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 as the use of digital and online technologies grows, so does the potential for inadvertent and unauthorized disclosure of client information. The Commission also added Comment 16 to admonish lawyers to be wary of the harm that might flow from such a disclosure and to consider whether circumstances call for enhanced security precautions.[6] It is noteworthy that the ABA has consistently and purposely 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.

The ABA's more recent significant activity in this area began in 2010, when the ABA Commission on Ethics 20/20[7] (the "Commission")—specifically through the Working Group on the Implications of New Technologies (the "Working Group")—evaluated the then-existing ethical rules and concluded that it was time for a periodic reexamination of the prevailing ethical framework governing a lawyer's duties and obligations in light of changing technology.[8] The Commission's Working Group was particularly interested in the evolving model ethical standards governing a lawyer's use of "cloud computing" and issues regarding the privacy and security of client data when stored electronically on third-party servers.[9] As defined by the National Institute

---

[5] 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*. *See* report in 14 ABA/BNA Lawyer's Manual on Professional Conduct, no. 15, August 19, 1998, at 394. 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. Then in 1999, it issued the ABA Formal Opinion No. 99-413, with the opinion that encryption of email was not generally an ethical requirement, given the reasonable expectation of privacy inherent in the use of email, but cautioning that there might be extraordinary cases involving particularly sensitive information that might require extraordinary security precautions. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999). Similarly, in 2000, the ABA 2000 Ethics Commission stopped short of requiring the use of encrypted email. *See 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).

[6] MODEL RULES, r.1.6, cmt. 16 (2000).

[7] ABA Comm. on Ethics 20/20, https.//www.americanbar.org/groups/professional_responsibility/committee_commissions/standingcommitteeonprofessionalism2/resources/ethics2020homepage/ (last visited June 17, 2019).

[8] *See* 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.

[9] *Id.*

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."[10] In simpler terms, however, if lawyers electronically store client data anywhere other than on a hard drive or on a server located in their offices or homes, the data is being stored "in the cloud." This includes data electronically stored on computers as well as on tablets and smartphones. Additionally, even if lawyers do not 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, including email and texts.

Cloud computing solutions have also proliferated. Well known examples include data storage services and applications (such as Google Drive, IBM Cloud, Amazon Cloud, tresori, Microsoft Cloud, Dropbox, Crashplan); 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 Clio, Time Matters Cloud, NetDocuments, and MyCase).

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 providing competent legal representation, cloud computing and other related uses of technology.[11] The ABA House of Delegates adopted the proposed Amendments to the Model Rules of Professional Conduct in August 2012 (the "2012 Amendments"). Below is a discussion of Rules that are directly relevant to the ethical issues relating to technology, including additions and other changes that were made to the Rules, either directly in the text of the Rules or in the Comments as part of the 2012 Amendments.

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."[12] 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

[10] Peter Mell & Timothy Grance, Nat'l. Inst. of Standards & Tech., *The NIST Definition of Cloud Computing*, 2 Spec. Publ'n. (Sept. 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[11] 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.

[12] MODEL RULES, r. 1.1.

question."[13] Comment 1 makes clear, therefore, that the duty of competence is broad enough to encompass just about every aspect of the practice of law.

The Commission found that, given the "bewildering pace of technological change," it was 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 practice, includ[ing] understanding relevant technology's benefits and risks."[14] 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[15] to Rule 1.1. to state:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.[16]

Thus, although the 2012 Amendment created no new ethical obligation, the Commission noted 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."[17] 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. <u>Model Rule 1.4: Client Communication</u>

Another Model Rule relating to cloud computing and communications with clients is Model Rule 1.4. 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 assistance not permitted by the Rules of Professional Conduct or other law.

---

[13] *Id.* r. 1.1 cmt. 1.

[14] ABA Comm. on Ethics 20/20, Introduction and Overview 8 (Aug. 2012), https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20121112_ethics_20_20_overarching_report_final_with_disclaimer.pdf (hereinafter "ABA 20/20 Introduction").

[15] 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.

[16] MODEL RULES, r. 1.1 cmt. 8 (emphasis added).

[17] ABA 20/20 Introduction, *supra* n. 14, at 8.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.[18]

Although the direct language of Rule 1.4 itself does not address a lawyer's choice to use (or refrain from using) a particular type of technology or technology-enabled service (which may include a cloud computing solution, database, machine learning technology and other forms of artificial intelligence, etc.), this Rule does require lawyers to inform their clients of any actual or potential security breach resulting in the actual or potential loss of confidential information.[19]

Unfortunately, it has become rather commonplace to receive news of the ever growing number of electronic data breaches and other cyber threats. With this reality, additional questions may arise 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 Part III.D.

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."[20] 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."[21] 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.

First, the ABA added a new section, paragraph (C), to 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."[22]

Second, Comment 18[23] to Rule 1.6 was expanded to emphasize the reasonableness standard and to provide guidance on the relevant factors when analyzing the ethical implications

---

[18] Model Rules, r. 1.4.

[19] For purposes of discussing the Model Rules, this paper does not address 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.

[20] *Id.* r. 1.6.

[21] ABA 20/20 Introduction, *supra* n. 14, at 8.

[22] Model Rules, r. 1.6(C) (emphasis added).

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

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].[24]

Third, the 2012 Amendments added one sentence to Comment 19 to Rule 1.6. Comment 19 addresses the preservation of confidentiality when transmitting confidential data.[25] Although not directed only at electronic communications and internet based services, this comment bears directly on lawyers' uses of online and digital technologies. 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

[24] Model Rules, r. 1.6 cmt. 18.

[25] Prior to the 2012 Amendment Comment 19 was numbered Comment 17.

state or federal laws that govern data privacy, is beyond the scope of these Rules.[26]

As all of Comment 19 is relevant to use of technology and a lawyer's competence in using the available technology, it is interesting to note that Comment 19 itself was not new in the 2012 Amendments. Additionally, it is noteworthy that the Commission did not choose to revise this comment to provide more specific examples regarding cloud computing, electronic communications methods or related security measures or tools. Instead, Comment 19 remained unchanged in explaining that how the ethical standard is carried out in practice is circumstance dependent. The only change to Comment 19 was to add the last sentence that makes clear 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

Model Rules 1.15 and 1.16 both discuss technology competence and how it (or the lack of it) may impact ethical obligations to clients.

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

> (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 the lawyer and shall be preserved for a period of [five years] after termination of the representation.[27]

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.[28]

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. However, state ethics opinions, which are discussed in Part III.C below, do offer some guidance.

---

[26] Model Rules, r. 1.6 cmt. 19.

[27] *Id.* r. 1.15.

[28] *Id.* r. 1.1.

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:
> (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.[29]

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.[30]

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 the application of these ethical mandates to implementing and using cloud computing solutions. Again, state ethics opinions, discussed in Part III.C. *infra*, do offer some guidance.

[29] *Id.* r. 5.1.

[30] *Id.* r. 5.2.

6. Model Rule 5.3: Responsibilities Regarding Nonlawyer Assistance

Model Rule 5.3 regarding a lawyer's responsibilities with respect to non-lawyers is also relevant as virtually all lawyers use the assistance of non-lawyers, such as legal assistants, paralegals, litigation consultants, technology vendors and others. 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 technology 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 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.[31]

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***").[32] All other changes made by the Commission were in the comments that significantly include the addition of new Comments 3 and 4. Comment 3 reads:

> 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 … 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

[31] MODEL RULES, r. 5.3.

[32] ABA 20/20 Introduction, *supra* n. 14, at 12.

> (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.[33]

Much of Comment 3 to Model Rule 5.3 has direct application to online and cloud-based technology services used in a legal practice. As an initial matter, Comment 3 specifically includes 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," although it simultaneously recognizes that this supervisory obligation is circumstance dependent. An exhaustive list of circumstances and factors to consider is not realistic for many reasons. However, 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.[34]

Comment 4 was also added in its entirety in the 2012 Amendments:

> [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.[35]

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.[36] Two, lawyers must give "appropriate instructions" to those outside servicers when retaining their services.[37]

---

[33] MODEL RULES, r. 5.3 cmt. 3.

[34] *Id.*

[35] *Id.* r. 5.3 cmt. 4.

[36] ABA 20/20 Introduction, *supra* n. 14 at 12.

[37] *Id.*

B. State Rules Of Professional Conduct Addressing Technology Competence

As noted in Section II.A, virtually all states and jurisdictions have adopted some version of the Model Rules. Each of these states adopted their respective version of the Model Rules before the ABA's 2012 Amendment to the Model Rules. Since the 2012 Amendment, approximately 36 states have adopted, in whole or in part, the changes made in the 2012 Amendments in connection with the duty of competence as it relates to technology (which appears in Comment 6 of the Model Rules) and other aspects of the 2012 Amendments relating to technology, confidentiality and responsibilities regarding nonlawyer assistance.[38]

Some states have adopted the 2012 Amendment regarding technology competence (and related issues) verbatim, while other states have adopted modified versions. In general, the variations do not reflect significant departures from the Model Rule, but rather reflect adjustments in each state's approach to provide more specifics and, in some cases, to reflect a less stringent approach. Below we discuss a few of the notable variations.

1. Continuing Legal Education

In September 2016, Florida became the first state to require continuing legal education specific to technology competence, when it adopted amendments to its ethics rules clarifying that the ethical duty of competence includes technology competence.[39] As part of the amendment, Florida Rule 6.10.3(b) was revised to require that an attorney complete at least 3 hours of continuing legal education in approved technology programs per three-year period.[40]

Similarly, in 2018 North Carolina implemented a new annual requirement, beginning in 2019, that all licensed attorneys must complete one hour of continuing legal education that is devoted to "technology training."[41] The North Carolina Rules amendments went on to define "technology training" and give examples of the types of programs that may be eligible for accreditation. According to the North Carolina rule, "technology training" means a program that is devoted to education on information technology (IT) or cybersecurity, for which the primary objective is to increase professional competence and proficiency as a lawyer.[42] The rule goes on to provide examples, which include education as to information tools, procedures and methodology to perform tasks specifically suited to the practice of law or to increase the efficiency

[38] The *Law Sites* blog provides useful summaries and links to the state professional rules of conduct and orders implementing changes relating to technology competence. *See* https://www.lawsitesblog.com/tech-competence (last visited July 21, 2019). According to the blog, the states that have adopted some or all of the 2012 Amendments are: Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Massachusetts, Minnesota, Missouri, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

[39] *In re Amendments to Rules Regulating The Fla. Bar 4-1.1, 6-10.3*, 200 So. 3d 1225 (Fla. 2016) [hereinafter "Fla. Amendments"].

[40] FL ST BAR Rule 6-10.3(b). The CLE requirements are a total of 33 hours during a 3 year period.

[41] 27 N.C. Admin. Code 1D.1518(a)(2). *See also* North Carolina State Bar, *Technology Training CLE Required Effective in 2019* (Nov. 27, 2018), https://www.nccle.org/about-us/news-publications/2018/11/technology-training-cle-required-effective-in-2019/ (last visited July 23, 2019).

[42] 27 N.C. Admin. Code 1D.1501(c)(17).

of performing tasks necessary to legal practice, social media evidence, e-discovery; electronic filing of legal documents, digital forensics for legal matters; and practice management software.[43]

2. Use Of Nonlawyers To Maintain Competence

The 2016 Florida amendments to its ethics rules included other changes regarding technology competence, which were largely based on the 2012 Amendments.[44] Below is the amended version of Florida Rule 4-1.1-Competence, comment regarding "Maintaining competence":

> Maintaining competence. To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education, *including an understanding of the benefits and risks associated with the use of technology*, and comply with all continuing legal education requirements to which the lawyer is subject.[45]

Although the italicized words reflect only slight variations from the Model Rule change in 2012, the comment to Florida Rule 4-1.1 regarding "Legal knowledge and skill" contains a noteworthy change. That comment makes explicit that lawyers may use non-lawyers to acquire the required level of technical competence:

> Competent representation may also involve the association or retention of a non-lawyer advisor of established technological competence in the field in question. Competent representation also involves safeguarding confidential information relating to the representation, including, but not limited to, electronic transmissions and communications.[46]

3. Other Variations And Qualifiers

As noted above, some states have adopted language varying from the duty of competence the Model Rules impose. For the most part, the seeming effect of these variations is to make the duty either (potentially) less stringent or more specific in scope than the ABA's 2012 Amendments. Examples of states with these types of variations include Indiana, Colorado, North Carolina, New Hampshire and New York. Certain aspects of these state variations are described below.

In modifying the "Maintaining Competence" comments to the state versions of Rules 1.1 and 1.01, respectively, Indiana and North Carolina slightly modified their language to clarify that the obligation relates to the technology that is relevant to the lawyer's practice. Below is the text applicable in both states' comments to their rule on Competence.

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with the technology *relevant to the lawyer's practice*, engage in continuing study and

---

[43] *Id.*

[44] Fla. Amendments, *supra* n. 39.

[45] *Id.*, r.4-1.1, at 5.

[46] *Id.*, r.4-1.1, at 4.

> education and comply with all continuing legal education requirements to which the lawyer is subject.[47]

Similarly, New Hampshire opted for a variation on Model Rule 1.1, Comment on "Maintaining Competence" that reflects its intent to have a flexible and practical application of technology competence. In the revision, the New Hampshire Supreme Court adopted the state ethics committee comment:

> The New Hampshire Rule continues the prior New Hampshire Rule, expanding on the Model Rule to serve both as a guide and objective standard. The Model Rule standards of legal knowledge, skill, thoroughness, and preparation reasonably necessary are rejected as being too general.
>
> ABA comment [8] … requires that a "lawyer should keep abreast of . . . the benefits and risks associated with relevant technology." This broad requirement may be read to assume more time and resources than will typically be available to many lawyers. Realistically, a lawyer should keep reasonably abreast of readily determinable benefits and risks associated with applications of technology used by the lawyer, and benefits and risks of technology lawyers similarly situated are using.[48]

The New York State Bar Association also adopted and published comments "to provide guidance for attorneys in complying with the Rules." The New York State Bar Association's version of Comment 8 is different and less comprehensive than the ABA's 2012 Amendment. Rather than the more broad statement that the ABA adopted, the New York State Bar Association's comments state that a lawyer should: "…keep abreast of the benefits and risks associated with technology the lawyer *uses to provide services to clients or to store or transmit confidential information*."[49]

Similarly, Colorado's amendment to its comments to Rule 1.1 varies from the Model Rule to read: "… a lawyer should keep abreast of change in the law and its practice, *and changes in communications and other relevant technologies* …"[50] With this modification, the Colorado comment appears to emphasize competence in understanding and using technological communications and how that may affect the obligations to protect client confidences and information.

---

[47] IN ST RPC r. 1.1, cmt. 6 (amended by Order Amending Indiana Rules for Professional Conduct, Cause No. 94S000-1701-MS-5 (Ind. 2017), effective January 1, 2018); 27 N.C. Admin. Code Rule 1.01, cmt. 8 (emphasis added).

[48] NH R RPC r. 1.1 (amended by Order, Section XI. Rules of Professional Conduct – ABA 20/20 Initiative (N.H. 2015), effective January 1, 2016, *available at* https://www.courts.state.nh.us/supreme/orders/11-10-15-Order.pdf).

[49] New York State Bar Association, Committee on Attorney Professionalism Resources, effective April 1, 2019, https://www.nysba.org/CustomTemplates/SecondaryStandard.aspx?id=53800 (last visited July 23, 2019). These comments are not part of the New York Rules of Professional Conduct because the New York Appellate Division has not adopted any of the comments to the rules. *See also* Robert Ambrogi, *Two More States Adopt Duty of Technology Competence*, Nov. 11, 2015, https://www.lawsitesblog.com/2015/11/two-more-states-adopt-duty-of-technology-competence.html.

[50] CO ST RPC Rule 1.1, cmt. 8 (emphasis added).

The state variations from the ABA Model Rule 1.6 and its duty of competence are not all in the direction of being more specific as to the scope of the obligation. West Virginia, for example, opted to change "should" to "must" so that the amended comment to Rule 1.1 reads: "a lawyer *must* keep abreast of … the benefits and risks associated with relevant technology…"[51] In doing so, West Virginia underscored the strength of this ethical obligation.

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[52]; links to state ethics opinions[53]; and summaries of states' adoption of the Comments to the Model Rule and the effects of the Comments and comparison of Model Rules and state rules.[54]

III. MAINTAINING DATA SECURITY

A. Types Of Data Security Risks

Whether practicing within a large law firm or legal department or as a solo practitioner, all lawyers need to be aware of the internal and external security risks confronting their data. Internal risks occur when an internal threat actor, such as an employee or contractor, access, leak, or steal confidential data. External risks arise when hackers gain access to a firm's information through common breach techniques, notably malware and email phishing. According to the ABA's 2018 Legal Technology Survey,[55] 23% of law firms experienced a cyberattack or data breach in 2017. The likelihood of experiencing a breach increased with a firm's size, from a low of 14% for solo practitioners to a high of 50% for firms with over 100 lawyers.[56]

Firms should take every step to stay up-to-date on emerging risks as technology continues to evolve. In recent years, a new form of cyberattack called "cryptojacking" has evolved.[57] Cryptojacking occurs when a hacker hijacks laptops and cellphones, and turns these items into

---

[51] WV R RPC Rule 1.1, cmt. 8 (emphasis added).

[52] ABA, Alphabetical List of Jurisdictions Adopting Model Rules, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/alpha_list_state_adopting_model_rules/ (last visited June 20, 2019).

[53] ABA, Links to Other Legal Ethics and Professional Responsibility Pages, https://www.americanbar.org/groups/professional_responsibility/resources/links_of_interest/ (last visited June 20, 2019).

[54] ABA, CPR Policy Implementation Committee, State Adoption of the ABA Model Rules of Professional Conduct and Comments, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/adoption_mrpc_comments.authcheckdam.pdf (last visited June 20, 2019); ABA, CPR Policy Implementation Committee, Variations of the ABA Model Rules of Professional Conduct, Rule 1.1 Competence, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/mrpc_1_1.pdf (last visited July 23, 2019).

[55] ABA, 2018 LEGAL TECHNOLOGY SURVEY REPORT, VOL. I: TECHNOLOGY BASICS AND SECURITY (2018) (ebook).

[56] *Id.*

[57] Vivian Hood, *Law Firms and Cyber Attacks – What's a Law Firm to Do? Part One* Nat. L. R. (Jul. 17, 2018), also *available at* https://www.natlawreview.com/article/law-firms-and-cyber-attacks-what-s-law-firm-to-do-part-one.

unsuspecting cryptocurrency harvesting devices.[58] Emerging technologies, such as cryptocurrency, mean new opportunities for hackers.[59] Law firms should continuously stay abreast of such new and evolving threats.

Although external breaches targeting law firms are more highly publicized,[60] internal risks are not uncommon.[61] As one data privacy industry expert observed, insiders pose a greater data security risk than outsiders because of their access to sensitive information and their knowledge as to how that information is protected.[62] Typically, the insider involved in an internal security breach falls within one of two categories, malicious or careless.[63]

The malicious insider is often a disgruntled employee who intentionally steals or leaks data out of spite or greed.[64] Law firms can protect themselves by installing data-centric security technologies that prevent employees from copying, moving or deleting data without receiving permission or approval to do so.[65] These technology solutions can also redact sensitive information from email transmission and will automatically alert the system administrator if an employee attempts to do so.[66]

On the other hand, a carless employee exposes confidential data by accident. By illustration, an employee may click on a phishing link in an email that he believes to be legitimate.[67] This mistake allows the hacker to install malware onto the device and infiltrate the firm's network. Firms should take affirmative steps to develop security awareness campaigns and implement employee-training programs on cybersecurity.[68]

---

[58] *Id.*

[59] *Id.*

[60] *See, e.g.*, Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal,* Wall St J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504; Dan Steiner, *Hackers Are Aggressively Targeting Law Firms' Data* (Aug. 3, 2017), https://www.cio.com.

[61] *See* Debra Cassens Weiss, Suit Claims Ex-Partner Installed Software Allowing Continued Access to Law Firm Files, ABA J. (Feb. 13, 2012), *available at* http://www.abajournal.com/news/article/suit_claims_ex-partner_installed_software_allowing_continued_access_to_law_.

[62] Joseph Steinberg, *Insider v. Outsider Data Security Threats: What's the Greater Risk?* (Apr.6, 2018), *available at* https://digitalguardian.com/blog/insider-outsider-data-security-threats.

[63] Jan van Vliet, *Why Employees Are The Biggest Threat To Company Data* (Oct.19, 2018), *available at* https://www.information-age.com/employees-threat-123475710/.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Id.*

B. Regulatory Considerations

Regulations addressing the protection of client sensitive data and information that law firms maintain abound. The most widely recognized is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which places restrictions on the receipt, transmission and use of an individual's health information.[69] An analogous regulation is the Health Information Technology for Economic and Clinical Health Act (HITECH) that requires law firms with access to "protected health information" to safeguard it from disclosure.[70] Both HIPPA and HITECH impose civil penalties for noncompliance as well as notification requirements for data breaches.

Under HIPAA, when law firms conduct work that involves "protected health information" (PHI) for covered entities, they are generally considered as "business associate"—a classification that triggers a wide array of compliance measures and serious civil monetary penalties.[71] PHI includes medical history, laboratory results and insurance information.[72] Law firms should develop and implement thorough HIPAA and HITECH a compliance plan to detect, contain, prevent, and correct security violations.[73]

HIPAA and HITECH are merely two examples of regulatory constraints that law firms might encounter. Noncompliance with federal regulations have serious consequences.[74] Attorneys may face disciplinary action and law firms expose themselves to unnecessary liability.[75] It is therefore imperative that law firms train their review team (or review technology) to spot categories of protected information (for example, Social Security numbers).[76] In the context of court documents, Federal Rule of Civil Procedure 5.2 grants courts with the authority to order that a filing be made under seal to protect sensitive information.[77]

At the state level, a number of laws are on the books that address the manner in which an individual's privacy must be protected. Many fall under the broad heading of affording protection to "personal identification information" (PII),[78] but the information that falls under that term and

---

[69] Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in sections of 29 and 42 U.S.C.).

[70] Pub. L. No. 111-5, 123 Stat. 223 (codified at 42 U.S.C. Sections 300jj et seq., Sections 17901 et seq).

[71] Joe Kelly, *What HIPAA Compliance Means for Lawyers as Business Consultants* (April 17, 2015), *available at* https://www.lawtechnologytoday.org/2015/04/lawyers-as-business-consultants-under-hipaa-how-t)o-stay-compliant/.

[72] *Id.*

[73] *Id.*

[74] Andrea Donovan Napp, *The Intersection of Data Privacy and E-Discovery*, ABA Sec. Lit. 23 (Dec. 17, 2014), also *available* at http://apps.americanbar.org/litigation/committees/businesstorts/articles/fall2014-1214-between-a-rock-and-a-hard-place-intersection-of-data-privacy-and-e-discovery.html.

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] While definitions of PII vary, PII is generally defined any data that could potentially be used to identify a particular person. *See, e.g.,* 2 CFR § 200.79 (defining PII as "information that can be used to distinguish or trace an individual's

can vary widely. Massachusetts, for example, requires companies to encrypt customers' PII that is stored on portable devices, such as iPads and laptops.[79] In Nevada, companies must encrypt customers' PII that is sent over the Internet to recipients outside of the business's secure network.[80] To date, California has adopted the most rigorous data privacy laws in the country.[81] The California Consumer Privacy Act broadly defines PII with reference to an expansive list of characteristics, behaviors, as well as inferences drawn from the information. This includes family information, geolocation, and sleep habits. The bill provides consumers with the right to request specific information collected about them.[82] Companies need to have the ability to quickly search, compile and produce these reports to consumers.

C. Data Security Policies

Given the ever-increasing threat of data breaches, establishing an effective security program is no longer optional. A comprehensive security program should address who has primary responsibility for data security, as well as defining the roles others in the organization will play in the event of a breach. Smaller firms may not warrant the expense of a full time information officer, but every firm should appoint one individual who will be bear responsibility for coordinating and overseeing security and who can implement the security program. Delegating security programs solely to an IT department omits the critical input lawyers and their legal staff should provide. IT departments can establish measures to prevent data breaches, but the role of identifying the information and data requiring protection falls squarely on the lawyers and the legal staff who handle it. Working collaboratively, lawyers, staff and members of an IT department can design a security program that addresses how to detect, respond to, and recover from data breaches. Such programs should include the adoption of key technology related policies such as data management and retention, email use, internet use, remote access, social media use, personal technology use and employee privacy. Although security programs that address the prevention side of data breaches are critical, incident response is just as important to a security program's success.[83] Finally, without security awareness, a security program is just another document sitting on a shelf or in an Outlook folder. Unless members of the law firm or legal department are trained to understand and recognize cyber threats, even the most well designed security program is doomed to fail.[84]

---

identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.").

[79] *See* 201 Mass. Code Regs. §§ 17.01–17.05 (2013)

[80] *See* Nev. Rev. Stat. § 603A.215 (2017).

[81] Juliana De Groot*, What is the California Consumer Privacy Act?* July 15, 2019, https://digitalguardian.com/blog/what-california-data-privacy-protection-act.

[82] *Id.*

[83] In fact, the ABA has extended a lawyer's duties under Model Rule 1.4 to keep client's "reasonably informed" of a matter to a lawyer's duties following a data breach. *See* ABA Formal Opinion 18-483 (October 18, 2018), discussed in Section IV(D)(3) of this paper.

[84] The ABA adopted a resolution at its 2014 Annual Meeting on cybersecurity that ""encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected." Resolution 109, American Bar Association, Cybersecurity Legal Task Force, Section of Science & Technology Law, Report to the House of Delegates, August 2013 (available at

D. The Role Of Encryption

Encryption is one of the basic safeguards for data protection. The process of encryption converts data to an unrecoginizable or "encrypted" form that can only be viewed by authorized persons.[85] Data that resides in storage can be encrypted as well as data that is being transmitted over wired and wireless networks. Data encryption can range from "full-drive encryption" that protects all data housed on a server, desktop, laptop or a portable device to "file drive encryption" that extends only to an individual file.[86] For handheld devices, such as smartphones, encryption in most current models of these devices is automatically enabled with PIN, passcodes and swipe patterns.

One of the ABA's most recent opinions underscores that lawyers should use only email for *routine* communications.[87] For matters that are highly sensitive, lawyers should consider more secure mediums such as encryption.[88] The availability of email encryption[89] has led many state bar associations to issue ethics opinions stating that email encryption may be required to discharge a lawyer's duty of confidentiality.[90] Such opinions are consistent with ABA Formal Opinion 477, Securing Communication of Protected Client Information.[91] That opinion discusses a lawyer's duty to utilize encryption and other safeguards to protect email and electronic communications not only as a result of the increase in cyber threats but also in recognition of the developing technology and evolving safeguards. Significantly, the opinion notes that whether encrypted email should be used is a fact-based analysis. As a result, although the ABA concludes that "the use of un-encrypted routine email generally remains an acceptable method of lawyer-client communication," the opinion states that "particularly strong protective measures, like encryption, are warranted in some circumstances."[92]

When encrypted email is unavailable, lawyers can protect confidential information to a lesser extent by putting it in an encrypted attachment rather than in the text of the email. Current versions of Microsoft Office, Adobe Acrobat, and WinZip encrypt a document by setting a password. Passwords should then be shared through a separate and secure email

---

https://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions/2014_hod_annual_meeting_109.authcheckdam.pdf).

[85] *Common Types of Encryption: What Lawyers Need to Know*, https://www.lawtechnology.org/2018/07/common-types-of-encryption/ (Jul. 18, 2018).

[86] *Id.*

[87] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 5 (2017).

[88] *Id.*

[89] Google's 2014 announcement making encryption available for its email services observed that unencrypted email was akin to sending a postcard while encrypted email was akin to adding an envelope. David G. Ries, Techreport 2017: 2017 Security, ABA (Dec. 1, 2017), available at https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/

[90] *See, e.g.,* Tex. Disciplinary Rules on Prof'l Resp. & Conduct, Formal Op. 648 (2015).

[91] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 5 (2017).

[92] *Id.*

communication. Although not as robust as encryption, and less so with a weak password, this method is more secure than no encryption at all.

E. Third Party Vendors: Are They Secure?

In today's world, no law firm will ever fully be able to benefit from advancements in technology without turning to third party vendors. Many law firms use third party vendors for electronic billing or payroll services, as well as for cloud computing to process and share data. While the benefits provided by these strategic partnerships are invaluable and necessary, the risks to firm security as a result of utilizing third party vendors can be detrimental. Once a vendor has access to the firm's network, they also have access to all of its electronically stored confidential information. If the vendor's network is not secure or is vulnerable to some sort of breach, the firm's data is in direct risk and the firm will be completely responsible for whatever happens to the leaked data. Pursuant to Model Rule 1.6 and 5.3, lawyers have an ongoing obligation to protect the confidentiality of client data and information, as well as to supervise the conduct of non-lawyers employed or retained by the firm. Due to the unique risks associated with third party vendors, merely selecting the wrong vendor can directly jeopardize Model Rule compliance.[93]

The consequences of improper vendor selection have been put on trial. In 2017, a Virginia federal magistrate judge ruled that a plaintiff insurance company inadvertently disclosed confidential material "when an employee intentionally uploaded the case file" to an unprotected file-sharing site.[94] This oversight led to the complete waiver of the plaintiff's attorney-client privilege and work product protection for its counsel. Further, the judge stated that plaintiff's counsel should have realized that the unsecure site could lead to the exposure of confidential information and thus should have taken steps to remedy the breach. The failure to do so was considered an ethics violation and resulted in sanctions. The judge also specifically ordered the plaintiff's counsel to pay the parties' costs associated with the court's ruling.[95]

Although these risks are concerning, law firms should not do away with cloud computing or electronic billing altogether. An October 2016 Illinois State Bar Advisory Opinion determined that a lawyer's "use of an outside provider…is not, in and of itself, a violation of Rule 1.6."[96] A 2006 Nevada opinion concurs.[97] However, both opinions go on to state that, in order for a firm to be Model Rule compliant, it is imperative that they conduct an adequate due diligence when selecting a third party provider.[98] Yet, it is difficult for any bar association to definitively state specific requirements as to what exactly is "an adequate due diligence" because technology changes so rapidly.[99] Various state bar association advisory opinions are therefore the only

[93] MODEL RULES, r. 1.6; MODEL RULES, r. 5.3.

[94] *Harleysville Ins. Co. v. Holding Funeral Home, Inc.,* No. 15-CV-00057, 2017 WL 4368617 (W.D. Va., Oct. 2, 2017).

[95] Joan C. Rogers, Putting Case File on File-Sharing Site Waived Privilege, Work Product Protection, Bloomberg Law (Feb. 22, 2017).

[96] ISBA Op. 16-06 (2016).

[97] St. Bar of Nevada Comm'n. on Ethics and Prof'l., Formal Op. N. 33 (2006). pp. 2-3.

[98] ISBA Op. 16-06 (2016).

[99] *Id.*

source detailing what reasonable inquiries and practices lawyers should take when selecting a third party provider. The following is a list of practices that the Illinois advisory opinion has noted:

- Reviewing cloud computing industry standards and familiarizing oneself with the appropriate safeguards that should be employed;
- Investigating whether the provider has implemented reasonable security precautions to protect client data from inadvertent disclosures, including but not limited to the use of firewalls, password protections, and encryption;
- Investigating the provider's reputation and history;
- Inquiring as to whether the provider has experienced any breaches of security and if so, investigating those breaches;
- Requiring an agreement to reasonably ensure that the provider will abide by the lawyer's duties of confidentiality and will immediately notify the lawyer of any breaches or outside requests for client information;
- Requiring that all data is appropriately backed up completely under the lawyers' control so that the lawyer will have a method for retrieval of the data; and
- Requiring provisions for the reasonable retrieval of information if the agreement is terminated or if the provider goes out of business.[100]

State bar advisory opinions also provide that the lawyer has further ethical obligations even after selecting the most secure provider. In order to comply fully with Rules 1.6 and 5.3, lawyers must perpetually be monitoring advancements in technology to a reasonable extent. An advancement could render a firm's current protective measures or third party vendor selections obsolete. Accordingly, the lawyer should "conduct periodic reviews and regularly monitor existing practices to determine if the client information is adequately secured and protected."[101]

IV. MAINTAINTING CONFIDENTIALITY WHEN USING TECHNOLOGY

A. Overview Of Assessing Risks To Confidentiality In Digital Landscape

The ABA Model Rules of Professional Conduct underscore that lawyers carry an ethical duty to safeguard confidential information.[102] Although there is no hard and fast rule on the use of technology, Comment 19 to Model Rule 1.6 further explains that the obligation of confidentiality requires lawyers to take "reasonable precautions" when electronically communicating with clients.[103] According to the ABA, "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the

[100] *Id.*

[101] *See* AZ Ethics Op. 09-04 (2009); WSBA Advisory Op. 2215 (2012).

[102] MODEL RULES, r. 1.6.

[103] *Id.* at comment 3.

representation of a client.[104]" What exactly constitutes reasonable efforts? The answer is not straightforward. The Model Rules do not mandate specific security measures, such as firewalls and password requirements.[105] Rather, the Model Rules take a holistic approach to define "reasonable effort" as a series of factors.[106] When assessing "reasonableness," factors to consider include:

> (1) the sensitivity of the information;
> (2) the likelihood of disclosure if additional safeguards are not employed;
> (3) the cost of employing additional safeguards, the difficulty of implementing the safeguards; and
> (4) the extent to which the safeguards adversely affect the lawyer's ability to represent clients.[107]

In the wake of cyberattacks and digital breaches, lawyers may need to discuss security safeguards with clients.[108] When handling very sensitive client information, lawyers should possibly utilize enhanced security measures and obtain a client's informed consent.[109]

B. Minimizing Risks When Using Data Connections

1. Email

Electronic mail ("email") is among the most commonly used forms of lawyer-client communication, outpacing the more traditional form of "snail mail." Naturally, many clients prefer the use of email due to its quick and inexpensive nature. However, with the convenience of emails derives the risk of mistakes. With this in mind, lawyers must take proper steps to protect clients' confidential information from an array of risks associated with email, many of which are easily preventable. Notably, email communication presents the risk of sending confidential information to the wrong recipient or attaching the wrong document. With such proliferation of email usage, lawyers must carefully consider what measures are most appropriate to safeguard the confidentiality of client information.

a. Email Cyberattacks

Two of the most common attacks that hackers perform are spear phishing and ransomware. Spear phishing occurs when a hacker sends a fraudulent email from a trusted account, or account manufactured to appear as a trusted account, with the intent to induce the individual to reveal confidential information. The fraudulent email typically contains a link or attachment that carries a virus or malware. Once the targeted individual clicks on the link or

---

[104] MODEL RULES, r. 1.6(c).

[105] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 5 (2017).

[106] *Id.*

[107] *Id.*

[108] *See* ABA Formal Opinion 18-483 (October 18, 2018), discussed in Section IV (D)(3), *infra.*

[109] *Id.* at 5.

attachment, he or she exposes the firm's network to unauthorized access of confidential and privileged information.

At the core of spear phishing is a hacker's intent to gain access to confidential information. For instance, a California lawyer became a victim of a serious case of spear phishing in 2015.[110] Upon receiving an email with an address ending in "usps.gov," and believing it to be a legitimate notification from the U.S. Postal Service of a package delivery status, the lawyer clicked on the attachment provided in the email. Shortly afterwards, the lawyer attempted to access his law firm's account through the bank's on-line access. After receiving a phone call from an individual who presented himself as a bank employee and prompted the lawyer to provide his bank account PIN, the lawyer discovered that $289,000 had been transferred to an offshore account.[111]

In contrast to spear phishing, a ransomware attack occurs when a hacker encrypts data on a targeted computer system and demands that the targeted individual(s) pay a ransom to decrypt it. Often times, ransomware attacks arise from fraudulent PDF attachments transmitted by email. Once an individual opens the PDF, the malware freezes the system and encrypts all of its data. Unlike spear phishing, hackers that employ ransomware are not typically seeking confidential information. Rather, ransomware attackers seek a financial gain by disturbing lawyers' access to confidential information.

Lawyers can take some simple steps to prevent phishing and ransomware attacks. Among those are remembering to always verify the sender of an email. Although the source of an email may appear to be a legitimate sender, if in doubt, lawyers should try to verify the sending identity from an independent source or call the number referenced in the email to verify the sender's identity.[112]

In addition, lawyers should be on the lookout for abnormalities in the emails they receive, be it from an unexpected sender, or one that contains language seeking "urgent" or "immediate" response, or contains misspellings and grammatical errors.[113] In addition, lawyers may consider adding a special IT tool that automatically scans and verifies the safety of links and attachments. Such tools can be effective, but they are not foolproof and lawyers should always couple these tools with technology education.[114]

b. The "Accidental" Email

A common feature that contributes to the misuse of emails is the "remember" feature on many email applications that automatically fills in the recipient's name as a user types. For example, the "remember" feature once caused a lawyer to accidently disclose highly confidential information—regarding an ongoing negotiation between the firm's client and the government—to

---

[110] Debra Cassens Weiss, *Lawyer Who Clicked on Attachment Loses $289K In Hacker Scam*, ABA.J. (Feb. 19, 2015), *available at* http://www.abajournal.com/news/article/lawyer_who_clicked_on_attachment_loses_nearly_289k_in_hacker_scam.

[111] *Id.*

[112] Karen Erger, *Too Many Phish in the Sea*, Ill. Bar J.L. (April 2015), *available at* https://www.isba.org/ibj/2015/04/toomanyphishsea.

[113] *Id.*

[114] *Id.*

a New York Times reporter instead of the lawyer's co-counsel who had the same last name.[115] Thus, lawyers that do not take proper precautions when sending an email may accidently divulge confidential client information to opposing counsel or a third party.

Lawyers can best minimize the risk of inadvertent disclosure of confidential information by carefully reviewing the directed recipient(s) of their correspondence, and not sending highly sensitive client information and financial documents through email. One can avoid sending an email to the wrong person by typing out the recipient's email address rather than relying on the automation feature. Some lawyers may consider utilizing email servers that provide a "pop-up box" feature that asks a sender who has selected the "Reply All" button if he or she actually intends to reply to all listed recipients.

2. Voicemail

Voicemail presents many of the same risks associated with email. In fact, several law firms have integrated their messaging system to combine both voicemail and email into one system.[116] Some firms have even switched over to a VoIP system—a program that carries phone conversations over the Internet instead of traditional phone lines.[117] With the introduction of a VoIP system in the firm setting, issues that involve voicemail messages correlate to those that involve email.

Firms that still operate with a more traditional phone system may either transcribe voicemail messages to email, or have a voicemail messages backup process in place. Like emails, voicemail messages may live forever. Thus, lawyers should take great precaution when leaving a voicemail. Most effectively, lawyers should refrain from leaving voicemails that contain confidential information.

3. Text Messaging And Instant Messaging

Lawyers communicate with clients through text messages, and often times, text messages are rushed. Some lawyers even communicate through instant messaging (IM). Thus, many of the considerations that apply to emails additionally apply to text messages. Like many emails, text messages are unencrypted.[118] Lawyers that heavily rely on text messages to communicate with clients risk the possibility of exposing confidential information to hackers.

It is imperative for lawyers to think twice before sending clients' confidential information through a text message. Lawyers should refrain from discussing substantive client matters through text messages or IM. However, in an evolving world that requires technological adaption, many clients demand to stay informed, and often, through instantaneous methods. Therefore, lawyers who choose to communicate with their clients through text message should use their

---

[115] *See* Debra Cassens Weiss, *Did Lawyer's E-Mail Goof Land $1B Settlement on NYT's Front Page?*, ABA J. (Feb. 6, 2008), *available at* http://www.abajournal.com/news/article/lawyers_e_mail_goof_lands_on_nyts_front_page.

[116] *Id.*

[117] *Id.*

[118] *Id.*

judgment to assess the situation and determine if sending a text message is reasonably necessary.

4. Shared Sites

File-sharing services provide lawyers with the ability to store information on remote servers and access it through the Internet. This process is one type of "cloud computing." When lawyers utilize the file-sharing service to preserve and transfer documents, they must rely on such service's security measures to protect confidential information. According to the ABA's 2018 Technology Survey Report, the availability and usage of online storage remains high.[119] In 2018, 54.6% of surveyed lawyers reported that online storage is available at their firms. Despite the rate at which lawyers continue to rely on cloud computing software, the survey reveals that the most common concern remains the risk to clients' confidentiality and data security.[120]

File sharing is increasingly important in the practice of law. Although law firms are keenly aware of the IT risks they pose, the need for sharing files continues unabated. Demand from clients and other law firms for the convenience that shared sites offer means they will continue to be utilized. To combat the risks associated with the use of such sites, law firms should consider using enterprise file sharing services such as Citrix ShareFile, as opposed to consumer file sharing services such as Dropbox.[121] The former often allow lawyers to set controls in terms of how and when files may be viewed, while the latter typically do not.

One cautionary tale regarding the use of shared sites is found in *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*[122] In *Harleysville,* an investigator for the plaintiff insurance company uploaded privileged documents into a cloud-based file sharing account that was not protected by a password. When the defendant subpoenaed the third party to produce documents, one of the documents produced contained a link to the shared file.[123] Opposing counsel found the hyperlink, accessed the account and downloaded and read the documents. The court denied Harleysville's motion to disqualify opposing counsel and held that Harleysville waived both the attorney-client privilege and the work product doctrine. Applying Virginia state law to the privilege doctrine, the court considered the "reasonableness of the precautions to prevent inadvertent disclosures," the "time taken to rectify the error" and the "extent of the disclosure," and found that the attorney-client privilege was waived. As the court observed, the plaintiff's disclosure was "vast" and likened it to "the cyber world equivalent of leaving its claims file on a bench in the public square and telling its counsel where they could find it." Likewise, the court held that the plaintiff also waived work-product doctrine protection under Federal Rule of Evidence 502. Notably, the court also advised that under public policy, businesses who choose to use evolving technology bear the

---

[119] Dennis Kennedy, *Techreport 2018: 2018 Cloud Computing*, ABA J. (Jan. 14, 2019), *available at* https://www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cloud/

[120] *Id*.

[121] *Id.*

[122] *See, e.g., Harleysville Ins. Co. v. Holding Funeral Home, Inc. No. 15-CV-00057, 2017 WL 4368617 (W.D. Va., Oct. 2, 2017)*, discussed in Section IV(B)(4).

[123] *Id.*

responsibility to know how to use it and to ensure confidential information cannot be accessed by anyone not entitled to view it.[124]

C. Minimizing Risks When Using Common Devices

1. Portable Devices And Media

Portable devices and media present special threats to client confidentiality. A risk that is particularly prevalent with portable devices is the possibility of theft. According to a report released by Kensington, a laptop is stolen every 53 seconds, and over 70 million cell phones are lost each year.[125] Therefore, lawyers must take greater precaution to protect their laptops, tablets, and cellphones that may potentially carry sensitive client information. In the realm of portable devices and media, this may include multi-factor authentication (MFA), encryption, and stronger passwords.

MFA is a security system that involves two or more methods of authentication from separate categories of credentials to confirm the user's identity.[126] By implementing MFA, law firms can add an extra layer of security to protect clients against the risks associated with portable device theft and data breach. Moreover, law firms should consider encrypting portable devices, monitor mobile applications and downloads on firm-issued devices, and ensure that confidential information on these devices are not stored in secondary locations.

In addition, lawyers should refrain from creating and storing documents on portable devices beyond the firm's network. By doing so, lawyers can decrease the likelihood that hackers will infiltrate their clients' confidential information. Additionally, portable devices should be turned off when not in use as those devices in "sleep" or "hibernation" mode can easily be accessed.

2. Discarded Hardware

Lawyers must practice due diligence in the disposal of sensitive client information. In 2014, an Indiana lawyer received two years of suspension without automatic reinstatement, partly because of his improper disposal of sensitive client documents.[127] The lawyer disposed several paper files containing sensitive client information, such as Social Security numbers and financial records, in a local trash bin.[128] A newspaper reporter brought Lehman's conduct to light when the reporter went through the trash and discovered confidential information pertaining to several of Lehman's cases. The Indiana bar concluded that Lehman's lack of care in regards to disposal of

---

[124] *Id*. at p. 13.

[125] Steve Olenski, *Is The Data On Your Business' Digital Devices Safe?,* Forbes (Dec 8, 2017), https://www.forbes.com/sites/steveolenski/2017/12/08/is-the-data-on-your-business-digital-devices-safe/#45b765b84c6a.

[126] *See* https://www.americanbar.org/groups/law_practice/publications/law_practice_magazine/2019/january-february/JF2019HotButtons/.

[127] *Matter of Lehman*, 3 N.E. 3d 536 (Ind. 2014).

[128] *Id.*

client information, coupled with numerous offenses, evidenced lack of competence and diligence.[129]

In the age of technology, the problem presented in Lehman's case is exponentially greater. Information stored on hardware is much more difficult to destroy than physical documents. Particularly, deleting electronic information from a hard drive does not necessarily mean that such information is destroyed in the same manner a paper can be destroyed. Law firms should implement "scrubbing" software that truly destroy residual computer files and a "shredding" procedure that provides for the proper physical destruction of outdated hardware.[130]

3. Public WiFi Access

Lawyers are often on the go and therefore tasked with conducting business outside the four walls of the office. This usually requires internet access. With the global extension of public WiFi access, lawyers must deal with the ethical implications of linking digital devices to a public domain. By connecting to a WiFi hotspot, lawyers run the risk of hackers potentially intercepting and decoding packets of confidential information that transfer through the wireless connection.

Many states now advise lawyers to limit the use of WiFi hotspots in the course of conducting business. For example, in California, the Standing Committee on Professional Responsibility and Conduct determined that a lawyer might potentially violate their duty of confidentiality when using public wireless networks for client work.[131] The committee's formal opinion addressed an issue pertaining to a lawyer who used his firm-provided laptop at a local coffee shop to conduct legal research and email his client. In reaching its decision, the Committee emphasized the lack of security features provided in most public wireless access locations.[132]

Firms should provide a secure virtual private network (VPN) for lawyers to utilize secure internet access outside the office. In doing so, firms should take reasonable steps to safeguard the confidentiality of client information. Furthermore, law firms should educate lawyers about the risk associated with downloading, saving, and sending confidential client information when utilizing public WiFi connections.[133]

4. Public Computers

Lawyers may rely on public computers, particularly during the course of travel. Many airports, hotels, and coworking spaces provide computers for public use. Law firms cannot adequately monitor public computer usage, and therefore lawyers who opt to conduct work on a publicly-accessible computer are exposed to several technical risks. Public computers are often

---

[129] *Id.* at 2-3.

[130] Dan Pinnington, *Avoiding Cybercrime Dangers: Scrub Confidential Client Information on Discarded Equipment*, Lawyers Mutual (May 19, 2015), https://www.lawyersmutualnc.com/blog/avoiding-cybercrime-dangers-scrub-confidential-client-information-on-discarded-equipment.

[131] COPRAC, Formal Op. 179 (2010).

[132] *Id.* at 7.

[133] *See* Jaliz Maldonado, *Law Firm Cybersecurity: Ethical Issues in Wireless Networks*, Nat'l L. Rev. (Feb. 7, 2019), *available at* https://www.natlawreview.com/article/law-firm-cybersecurity-ethical-issues-wireless-networks.

programmed to store a user's keystroke through a special "key logging" software.[134] Such a feature can lead to password and authentication security concerns.[135] Ultimately, an unauthorized user can leverage the key logging feature to access a client's confidential information.[136]

To avoid this scenario, lawyers should limit the use of public computers for business purposes.[137] When using a public computer is necessary, lawyers should refrain from conducting sensitive tasks that may compromise their duty of confidentiality. At the end of any session involving a public computer, lawyers should make certain to log off and close the browser.

Moreover, many consumers are unaware that older vehicle "infotainment systems," which permit access to navigation, music streaming, voice dialing/messaging, or other services may collect and store information from personal mobile devices connected to the system via Bluetooth or USB.[138] As a result, connecting your mobile device to a vehicle's infotainment system can expose confidential client information.[139] In 2017, the National Association of Automobile Dealers ("NADA") and the Future of Privacy Form ("FPF") published "Personal Data in Your Car" to inform consumers about personal data collected and stored by cars, as well as to provide a "privacy checklist" when selling or renting a car.[140] The NADA and FPF recommend that consumers delete information that may be stored on a vehicle's hard drive before selling a car or returning a rented or leased vehicle. In 2016, the FTC issued guidance on personal data and rental cars.[141] Based on the guidance provided by the FTC, NADA, and FPF (and others), when renting a car, lawyers should (1) avoid connecting their phone to rental car's system; (2) charge the phone via the cigarette lighter port rather than directly from the car's USB port; and (3) delete data from the dashboard before returning the rental vehicle.[142]

---

[134] Sharon D. Nelson & John W. Simek, *Hot Buttons On the Road Again: Secure Mobile Computing*, A.B.A. (Nov. 1, 2018), *available at* https:// www.americanbar.org/groups/law_practice/publications/law_practice_magazine/2018/ND2018/ND2018HotButtons/.

[135] *Id.*

[136] *Id.*

[137] *See id.*

[138] Steve Halloran, *Don't Let a Rental Car Compromise Your Privacy*, CarGurus® Blog (Mar. 21, 2018), *available* at https://blog.cargurus.com/2018/03/21/dont-let-a-rental-car-compromise-your-privacy. Note: newer cars that are equipped with Android Auto or Apple CarPlay may present a lower risk since those interfaces are designed simply to project the information on the connected phone (rather than storing the information). *See id*.

[139] *Id.* In addition to potential exposure of client confidential information, lawyers should be aware of the vast scope of other personal information that connected cars collect and store, including home, work, and other favorite places on navigation, as well as garage door programming.

[140] *See Personal Data in Your Car*, NADA (Nov. 2010), *available at https*://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf

[141] Lisa Weintraub Schifferle, *What is Your Phone Telling Your Rental Car?,* Consumer Information Blog (Aug. 30, 2016), *available at* https://www.consumer.ftc.gov/blog/2016/08/what-your-phone-telling-your-rental-car.

[142] *Id.* It is particularly important to follow the instructions on the vehicle's screen for data deletion as presently, there is no uniform method to delete/reset an infotainment system. Indeed, reset/deletion methods vary by make, model, and even trim. *Id* Recognizing the importance of this issue, the U.S. Senate Commerce, Science and Transportation Committee adopted unanimously an amendment on vehicle data access and personal data deletion as part of the Committee's autonomous vehicle legislation in 2017. That amendment would have required the Government

5. Client And Guest Access To Law Firm's Computers

Clients and guests at a law firm may need to connect to the internet during their visit. This poses a risk to the security of the law firm's network because an unauthorized user may expose the firm's network to cyberattacks, viruses, and breach.[143] Due to the sensitivity and confidentiality of information stored on a law firm's local area network (LAN), unauthorized individuals should not have access to the main network.[144] Instead, firms should provide clients and visitors with access to a separate "guest" wireless network.

D. Minimizing Risks Associated With Cloud Computing

1. "Reasonable Care" Standard And Selecting Service Providers

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. As further discussed in Section IV.D.2 below, all of these known 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 A 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, including factors to consider in selecting a service provider; (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, each factor may not be universally relevant and the checklists in Attachment A will serve as a guide rather than a one-size-fits-all approach.

2. Cloud Computing In Its Various Forms

At least twenty-two state bars across the country have issued opinions or examined ethical questions associated with a lawyer's use of cloud computing services in a variety of forms.[145]

Accountability Office to report back to Congress within 12 months after enactment on the feasibility of mandating a uniform and simple procedure for deleting personal data stored by motor vehicles for all vehicles sold in the United States each year. The amendment was not enacted into law, as the overall autonomous bill failed to pass before the end of the 115th Congress. *See* S.1885 — 115th Congress (2017-2018).

[143] Maldonado, *supra* note 133.

[144] *Id.*

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

Most of these opinions were issued between 2010 and 2016. Given the widespread acceptance of online communications and technology in the commercial world, it should not be surprising that the issuance of new state opinions on whether cloud computing may be used has slowed. Indeed, this practical reality was recognized in a Texas opinion issued in 2018 that explained: "Considering the present state of technology, its common usage to store confidential information, and the potential cost and time savings for clients, a lawyer may use cloud-based electronic data systems and document preparation software for client confidential information…."[146]

Each of these state opinions has concluded that it *can be* ethically permissible to utilize cloud-based data storage facilities and other cloud-based services. However, lawyers must 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. Each opinion, like the Commission with the 2012 Amendments, also generally declines to specify what exactly constitutes "reasonable efforts." Although no two are identical, the state ethics opinions generally analyze the very similar rules of professional conduct and provide helpful guidance.

One of the later opinions, and arguably the most comprehensive in reviewing existing state opinions and the 2012 Amendments, is Wisconsin Formal Ethics Opinion EF-15-01: The Ethical Obligations of Attorneys Using Cloud Computing, published March 23, 2015[147] (the "Wisconsin Opinion"). For this reason, this section of the paper focuses on the Wisconsin Opinion, along with additional points from select additional opinions.

Wisconsin Opinion. 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). The Opinion's focus on these rules creates an instructive "reasonable efforts" 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, "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*."[148]

When assessing the risk associated with utilizing cloud computing solutions, the Wisconsin Opinion advises lawyers to consider these (albeit non-exclusive) factors:

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

---

[146] Tx. Eth. Op. 680 (Sept. 1, 2018).

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

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

- the lawyer's ability to assess the level of security that will be provided through the technology intended for use in the practice;
- the likelihood of unauthorized disclosure using the technology if additional safeguards are not employed;
- the potential costs of employing additional safeguards;
- the difficulty of implementing additional safeguards;
- if additional safeguards are employed, the extent to which they would 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 agreement terms with the selected service provider; and
- the environment (legal and ethical) in the relevant jurisdiction(s) where the services are to be conducted, with particular importance with respect to confidentiality.[149]

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.[150]

At a minimum, lawyers should:

1. Possess "a base-level comprehension of the technology and the implications of its use"[151] 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;

[149] *Id.* at 1.

[150] *Id.* at 11.

[151] *Id*. 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).

3. Understand and be familiar with the "qualifications, reputation, and longevity"[152] of the cloud-service provider, just like they should know the same criteria of any other service provider;

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[153]

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.[154]

Other state opinions. Many of the state opinions have offered variations on the guidance above and examined additional specific issues or uses of technology. While far from a comprehensive description, we examine some additional factors and guidelines that a few other states have noted in their opinions for lawyers' consideration.

For example, 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.[155] 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 the following regarding SaaS (software as a service technology):

> 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

[152] *Id*.

[153] 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.

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

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

> diligence and competency to manage the risks of SaaS that the lawyer is required to apply when representing clients.[156]

The Ohio State Bar Association similarly reviewed its Rule 1.15 in looking at whether a law firm may use a third-party vendor to store client data in the cloud. In Informal Advisory Opinion 2013-03, the Bar concluded that the Rule permitted storing client information in the cloud if the chosen vendor had appropriate systems to protect the clients' data from "destruction, loss or unavailability." [157] The Bar also imposed 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.[158]

Washington State Bar Association Advisory Opinion 2215, issued in 2012, also reviewed online data storage in connection with its Rule 1.15.[159] 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."[160] The WSBA opinion, much like the Wisconsin Opinion and the ABA guidance, recognized the impossibility and impracticality of providing specific directions or guidelines for particular security measures that lawyers must use with service providers for cloud data storage and related services in order to satisfy the standard of adequate protection of client information and material.[161] 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:

> 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.
> 2. 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.
> 3. 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.
> 4. Ensure secure and tightly controlled access to the storage system maintained by the service provider.[162]

Similarly, 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 retrieving client property," if the lawyers take "reasonable precautions to ensure the property is

---

[156] *Id.*

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

[158] *Id.*

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

[160] *Id.* at 2.

[161] *Id.*

[162] *Id.*

secure and accessible."[163] Much of the "reasonable precautions" or due diligence that a lawyer should undertake is similar to those described in the Wisconsin Opinion. 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."[164] The Vermont Opinion went on to suggest additional considerations for lawyers, including (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.[165]

As set forth in several of these Ethics Opinions, the most important requirement is that an attorney stay abreast of technological developments to ensure that the security measures taken remain valid and current.

3. Communicating With Clients About Your And Their Cloud Computing Practices

In light of what can seem to be regularly occurring data breaches and cyber-attacks, the question arises as to whether, or in what circumstances, the legal ethical standards may require 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 client consultation or consent may not be required by the ethics rules in connection with storage of electronic client information in many situations, so long as reasonable steps have been taken to competently safeguard the confidentiality of the client information. 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 to determine if the circumstances call for consultation."[166] Similarly, a Pennsylvania opinion in 2011 stated that "it is not necessary to communicate every minute detail of a client's representation."[167] 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.

Some 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

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

[164] *Id. at 6.*

[165] *Id.*

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

[167] 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).

suggests giving notice to the client about the proposed method for storing client information.[168] 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.[169] 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."[170] Also, the Wisconsin Opinion offered a suggestion as to the manner in which attorneys may inform clients about their technology practices, writing that: "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."[171]

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.[172] Most recently, the ABA issued a formal opinion last year to address the scope of a lawyer's duty following a data breach.[173] Titled "Lawyers' Obligations After an Electronic Data Breach or Cyberattack," the opinion's introduction lays out the impetus for its issuance:

> Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers…Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.[174]

However, discharging one's ethical obligations after a data breach is not a one-size fits all proposition, and instead, "depends on the nature of the cyber incident, the ability of the lawyer to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations."[175]

---

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

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

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

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

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

[173] ABA Formal Opinion 18-483 (October 18, 2018).

[174] *Id*.

[175] *Id.* The opinion further notes that obtaining technical advice from a cyber-expert may be warranted in determining how to comply with the obligations of the Model Rule 1.4 after a cyber-incident. *Id.*

V. MANAGING AND MINIMIZING RISKS WITH ELECTRONIC DOCUMENTS

A. Electronic Document Production And E-Discovery

Electronic documents have replaced paper copies for some time now, but still not all lawyers are versed in the significant technological differences that have come from this shift. A single, accidental click by an uninformed user of electronic documents can easily lead to unwanted transmissions of data. In the worst case, the user could send or delete privileged items of vital importance, without realizing, and derail an entire case. It is therefore imperative that lawyers stay up to date on how to manage and minimize risks during electronic document production.

In more recent years, the guidance under state opinions has grown to cover electronic disclosure. For example, in a formal opinion, California addressed the question of what are the ethical duties of an attorney in handling the disclosure of electronically stored information ("ESI").[176] The hypothetical scenario laid out in the opinion can be easily imagined. An attorney is defending a client in a case brought by the client's primary competitor in a court requiring electronic disclosure. As part of the negotiated disclosure process, the attorneys agree to a joint search of the client's network using agreed upon search terms, with a clawback agreement that may allow the inadvertently produced ESI that contains privileged information. In this hypothetical, the attorney did not sufficiently understand the electronic discovery process or methods, the clients' information system, or the potential output of the search. Nor did he consult with an e-discovery consultant before agreeing to a court approved plan. Unfortunately for the attorney and client, the data disclosed in the e-discovery process included privileged content and highly valuable proprietary information of the client. Moreover, based on the attorney's participation in court approved e-disclosure process, the client was vulnerable to claims by its competitor that the resulting disclosures were not "inadvertent" and therefore the clawback was not applicable and the privileges were waived.

This California opinion analyzes the attorney's conduct primarily under California's ethical duties of competence and confidentiality (California Rules 3-100 and 3-110).[177] According to the opinion, under the California professional code, the ethical duty of competence evolves as new technologies develop and become integrated with the practice of law. While the level of necessary proficiency will vary depending on the circumstances, the opinion makes clear that competence relating to litigation "… requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information…".[178] Additionally, this duty "requires an attorney to assess his or her own e-discovery skills and resources".[179] It further provides that a higher level of technical knowledge and ability may be required depending on the e-discovery issues involved in a particular matter, and the nature of the ESI. If an attorney does not have the necessary level of competence required for a particular matter involving e-discovery, then the attorney: "has three options: (1) acquire

[176] COPRAC Formal Op. 2015-193 (2015).

[177] CA ST RPC Rules 1.1 and 1.6 (formerly cited as CA ST RPC Rules 3-110 and 3-100).

[178] *Id.* at 1.

[179] *Id.* at 3.

sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation."[180]

The California opinion also provides guidance as to specific functions that attorneys handling e-discovery should be able to perform, either directly or by associating with competent co-counsel or retaining expert consultants, in order to meet their duty of competence. These include being able to:

- initially assess e-discovery needs and issues, if any;
- implement/cause to implement appropriate ESI preservation procedures;
- analyze and understand a client's ESI systems and storage;
- advise the client on available options for collection and preservation of ESI;
- identify custodians of potentially relevant ESI;
- engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan;
- perform data searches;
- collect responsive ESI in a manner that preserves the integrity of that ESI; and
- produce responsive non-privileged ESI in a recognized and appropriate manner.[181]

B. Managing Redactions

While keeping the general basics of electronic document printing and sending in mind, lawyers also need to understand how to effectively manage redactions so not as to accidentally share confidential and privileged information in violation of Model Rules 1.1 (competence) and 1.6 (confidentiality).[182] In 2007, the FTC found itself in trouble because of this very issue. In the electronic court filing of an antitrust suit brought against Whole Foods, the FTC redacted Whole Foods' confidential, proprietary information merely by applying black shading over the text.[183] When text is shaded as opposed to deleted, it is easy to simply move around the shading within an application such as Microsoft Word. Unfortunately, for the FTC and Whole Foods, the news media was able to take the publically filed, "redacted" documents and actually read and publish every word meant to be confidential.[184]

---

[180] *Id*. at 1.

[181] *Id.* at 3-4.

[182] MODEL RULES, r. 1.1; MODEL RULES, r. 5.3.

[183] *See* http://www.nbcnews.com/id/20269465/ns/business-us_business/t/oops-regulators-release-whole-foods-secrets/#.XTh_4o1Ya70.

[184] *Id.*

Over a decade later, lawyers are still making similar mistakes. Recently, in connection with the Special Counsel's investigation into the potential Russian interference of the 2016 presidential election, lawyers for Paul Manafort filed a brief using the same poor and ineffective black shading technique as the FTC in the Whole Foods case.[185]

In order to prevent such gaffes, firms must ensure that lawyers fully disclose and understand exactly how an electronic document was redacted. One of the safest methods for redactions is to use a pseudo-photocopy of the electronic document – called an image file – that does not allow for the searching of text within the document.[186] Specific software products that can automatically eliminate this problem are also available, such as CVISION Image Redaction Software, but lawyers should always exercise additional caution when utilizing third party vendors. Overall, the best way to prevent confidentiality breaches when managing redactions is simply to check with the firm's IT department or IT consultant in order to ensure that the redaction method is effective to prevent the redacted information from being viewed.[187]

C. Managing Metadata

Lawyers also have an affirmative duty to understand embedded data within electronic documents, called metadata, to determine whether it needs to be removed when sending or receiving files to avoid disclosure of confidential information, or whether it must be produced as often occurs during document production. Although the media often alludes to metadata as "hidden" or "secret" data,[188] its basic premise is not difficult to understand. Metadata is essentially information embedded in common software programs such as Microsoft Word or Adobe Acrobat. Metadata can include information about the document's author, how much time was spent revising the document, when it was revised, what revisions were made to it, and, in some instances, even information about the computer itself. In many cases, having this metadata information can be useful, as it helps with document management and collaborative document production. However, sharing this information with third parties, clients, or opposing counsel can potentially result in unauthorized disclosure of confidential, or even privileged, information.

Such an issue occurred in 2004 when lawyers suing a major car manufacturer filed a complaint containing metadata that inadvertently exposed the plaintiff's plan to later file suit against Bank of America.[189] This horror story prompted the ABA, in Formal Opinion 06-442, to explicitly extend the obligation of Model Rule 1.6(c) (lawyers must "take reasonable efforts to prevent the inadvertent or unauthorized disclosure of…information relating to the representation of a client") to the metadata transmitted in electronic documents.[190] At the state level there are a number of formal ethics opinions that address metadata, not only with respect to the duty to

---

[185] Jason Tashea, *How To Redact A PDF And Protect Your Clients*, ABA. J. (Jan. 10, 2019), http://www.abajournal.com/news/article/paul-manaforts-attorneys-failed-at-redacting-learn-how-to-do-it-right.

[186] Examples of image files include TIFF, JPEG, and GIF files.

[187] Tashea, *supra* note 185.

[188] *See* Evan Perez, *National Security Agency Halts Program*, CNN (Mar. 5, 2019), *available at* https://www.cnn.com/2019/03/05/politics/nsa-surveillance-program/index.html.

[189] Stephen Shankland, *Hidden Text Shows SCO Prepped Lawsuit Against BofA*, CNET (Mar. 18, 2004).

[190] ABA Formal Opinion 06-442 (Aug, 5, 2006).

protect against disclosure of metadata but also the potential implications for the receiving party.[191] There are various methods for managing metadata, but the safest way to eliminate it from documents altogether is to "scrub" the data away. Proprietary software programs exist that do this scrubbing automatically and, if selected properly, can greatly assist lawyers. Locked PDFs can also eliminate metadata from electronic transmissions. Conversely, when metadata is required to be produced, lawyers have a duty to ensure their production contains intact metadata and risk sanctions for their failure to do so.[192]

Sometimes, however, scrubbing metadata once is not enough and lawyers should use caution in recognizing when metadata returns to a previously scrubbed document. This occurs most frequently when a document is sent a second time. For example, if one lawyer sends a scrubbed complaint to another lawyer via email and the receiving lawyer forwards it on to yet another lawyer, the version sent to the last lawyer in the chain could contain metadata. In order to prevent this, it is imperative that the lawyer re-scrub documents received before sending them again. It is easy to accidentally slip and not realize that metadata has returned to a document. Therefore many state opinions, such as California Opinion 2007-174, suggest always checking with a firm's IT department or consultant if lawyers have any doubt as to whether or not their documents contain metadata.[193] Erring on the side of caution with metadata is the best way to remain compliant with the Model Rules.

D. Role Of Artificial Intelligence

As more and more artificial intelligence-type applications emerge, lawyers must remain extremely cautious in their utilization, whether their application is personal or professional. For example, within the personal realm, Amazon's Alexa or Google's Home Pod can be excellent assistants in scheduling meetings and more. However, all of these artificial intelligence assistants are equipped with multiple microphones that can record conversations. A couple in Oregon discovered this the hard way when their Alexa device recorded their conversation and sent it to a random person on their contact list.[194] Although instances like this are not common, the potential risk raises concerns of inadvertent disclosure in violation of the Model Rules. Some commentators recommend that lawyers who use artificial intelligence should unplug or disable microphones during client meetings or phone calls and "may seek to restrict their linkage to other sensitive

[191] *See, e.g.,* Tx. Disciplinary Rules on Prof'l Resp. & Conduct, Formal Op. 665 (2016); Alabama State Bar Office of General Counsel, Formal Opinion 2007-02; State Bar of Arizona Ethics Committee, Ethics Opinion 07-03; Colorado Bar Association Ethics Committee, Ethics Opinion 119; The Florida Bar Ethics Department, Ethics Opinion 06-02; Main Board of Overseers of the Bar Professional Ethics Commission, Opinion #196; Maryland State Bar Association Committee on Ethics, Ethics Docket No. 2007-09; New Hampshire Bar Association, Ethics Committee Opinion 2008-2009/4; New York State Bar Association - Committee on Professional Ethics, Opinion 749, 782; Association of the Bar of the City of New York - Committee on Professional and Judicial Ethics, Formal Opinion 2003-04.

[192] *See, e.g., Leidig v. BuzzFeed, Inc. Inc.*, No. 16CIV542VMGWG, 2017 WL 6512353, (S.D.N.Y. Dec. 19, 2017) (evidentiary sanctions imposed following plaintiffs' negligent and "amateurish" preservation efforts, including their failure to produce metadata).

[193] *See* COPRAC Formal Op. 2007-174.

[194] Eugene Kim, *Amazon Echo Secretly Recorded a Family's Conversation and Sent it to a Random Person on their Contact List*, CNBC (May 24, 2018), https://www.cnbc.com/2018/05/24/amazon-echo-recorded-conversation-sent-to-random-person-report.html.

databases."[195] In the professional realm, the use of e-discovery software has become more prevalent, especially the use of predictive coding. Yet whether a lawyer's use of AI is personal or professional in nature, in order to remain in compliance with Model Rule 1.6, it is important that lawyers not only remain cautious when using artificial intelligence but also keep abreast of new and evolving artificial intelligence technologies in order to remain competent.[196]

E. Electronic Document Retention And Destruction

The Model Rules covering electronic documents apply equally to open and closed matters. The lawyer therefore has an affirmative duty to take reasonable care in protecting inactive documents no longer needed in a case. Many firms fulfill this obligation by outsourcing document storage to a third party. As previously mentioned, in selecting a third party vendor the firm must first perform a careful and thorough due diligence. Maine Opinion 194 states that, in selecting a document storage vendor specifically, the lawyer "should take steps to ensure that the company providing…confidential data storage has a legally enforceable obligation to maintain the confidentiality of the client data involved."[197] Other states echo Maine's opinion.[198]

After considering how properly to store documents, a lawyer must next decide for how long to keep them. The ABA offers only a "reasonable time" threshold in its Informal Opinion 1384,[199] so the decision is ultimately up to the attorney. Other state ethics opinions have considered this issue, but they are inconsistent. For example, Missouri requires six years, Iowa requires ten, and other states still default to the "reasonable time" standard.[200] As a rule of thumb, five to ten years is a good reference point for how long the lawyer should intend to retain electronic documents.[201] However, any decisions on document retention should be made in concert with a review of state-specific ethics opinions. Most ethics opinions also require that the lawyer keep the client informed as to the retention and destruction of their documents.

In destroying electronic documents deemed unnecessary to retain, the lawyer must comport with the confidentiality requirements of Model Rules 1.6 and 1.9. Most states suggest that the firm conduct a thorough investigation before destroying electronic documents to ensure with a "reasonable likelihood that the important interests of the client" will not be harmed by the

---

[195] Brenda Dorsett and Barry Temkin, *Lawyers' Digital Assistants Raise Ethics, Privacy Concerns.* Law360 (May 23, 2019).

[196] *See The Future of eDisovery: The vital role of ERDRM*, *available at* https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-rfa-forensics-future-of-ediscovery.pdf.

[197] Me. Prof'l Ethics Comm'n, Op. No.194 (June 30, 2008).

[198] *See*, e.g., Ala. State Bar Ethics Op. 2010-02 (2010); Fla. Bar Ethics Op. 12-3 (2013).

[199] *See* ABA Informal Opinion 1384 (Mar. 14, 1977).

[200] Missouri Rule 4-1.22 [Effective July 1, 2016]; ISBA Op. 08-02 (2008).

[201] *See* OSBA Informal Ethics Opinion 00-02 (April 25, 2000); Neb. Op. 12-07 (2012); AZ. Op. 08-02 (discussing Arizona Opinion 91-01; five years is a safe "default option"); N.Y. Opinion 06-02 (June 28, 2006); WSBA, Guide to Best Practices for Client File Retention and Management, March 2010, *available at* http://www.wsba.org/~/media/Files/Resources_Services/Ethics/Guide%20to%20Best%20Practices%20for%20Records%20Manage ment%20310.ashx (seven to ten years).

destruction of the files.[202] A bankruptcy court, for example, required a law firm to notify clients about impending electronic document destruction by mail and by publishing a notice *in The Wall Street Journal*.[203] Once electronic documents are deemed destroyable, the lawyer must then select the best destruction method. Most states, like Massachusetts, Nevada, and Connecticut, require that disposal of electronic documents be done in a "secure manner."[204] So-called "cyberscrubbing," which is similar to the scrubbing used to remove metadata, is one such secure technique for destroying electronic documents. As discussed above, merely deleting a document from the computer will not permanently delete it altogether as it can still be retrieved with simple software. Prudent firms should always verify with their IT departments or consultants to ensure that electronic documents have actually been erased.

VI. SOCIAL MEDIA

Like it or not, social media is a fact of modern life and, in its various forms and applications, impacts individuals and businesses worldwide. As there is more than one definition of "social media," for purposes of discussing the ethical implications, we refer to the definition used by the District of Columbia in its ethics opinion on social media:

> Social media include any electronic platform through which people may communicate or interact in a public, semi-private, or private way. Through blogs, public and private chat rooms, listservs, other online locations, social networks, and websites such as Facebook, LinkedIn, Instagram, Twitter, Yelp, Angie's List, Avvo, and Lawyers.com, users of social media can share information, messages, e-mail, instant messages, photographs, video, voice, or videoconferencing content. This definition includes social networks, public and private chat rooms, listservs, and other online locations where attorneys communicate with the public, other attorneys, or clients. Varying degrees of privacy exist in these online communities as users may have the ability to limit who may see their posted content and who may post content to their pages. [205]

For attorneys, social media presents a number of ethical considerations, including attorney advertising limitations, the creation of an attorney-client relationship, issues of unauthorized practice of law, claims of expertise or specialization, and comments about judicial officials. These issues, while interesting, are beyond the scope of this paper. A less obvious consideration is how required technology competence, social media, and professional ethics rules may intersect in legal representations, including as part of due diligence activities, negotiations, investigations, and litigation.

Although the instructions in Comment 8 of Model Rule 1.1 to "… keep abreast of changes … including the benefits and risks associated with relevant technology …" do not specifically identify social media (or any particular technology at all), is it not difficult to make the connection. If an attorney does not have, or develop, an understanding how social media may be relevant to his or her clients, the attorney may miss the opportunity to capture information and evidence

---

[202] Tx. Eth. Op. 627 (Apr. 2013).

[203] *In Re Howrey LLP*, 2013 Bankr. LEXIS 1226, 2013 (Bankr, N.D. Cal. Jan.18, 2013).

[204] Nev. Rev. Stat. § 603A.200; Conn. Gen. Stat. § 42-471; Mass. Gen. Laws Ch. 93I, § 2.

[205] D.C. Bar Ethics Op. 371 (2016), at 1.

valuable to their clients-whether it be in pursuing claims for their clients or defending against third-party claims.[206] Indeed, at least seven jurisdictions (District of Columbia, Florida,[207] New Hampshire,[208] New York, [209] Pennsylvania,[210] Philadelphia[211], and West Virginia[212]) have specifically noted that, to varying degrees based on the types of representation, competence may require an understanding of social media in order to properly advise clients.[213] In Opinion 371, the District of Columbia wrote:

> Because the practice of law involves use or potential use of social media in many ways, competent representation under Rule 1.1 requires a lawyer to understand how social media work and how they can be used to represent a client zealously and diligently under Rule 1.3. Recognizing the pervasive use of social media in modern society, lawyers must at least consider whether and how social media may benefit or harm client matters in a variety of circumstances. We do not advise that every legal representation requires a lawyer to use social media. What is required is the ability to exercise informed professional judgment reasonably necessary to carry out the representation. Such understanding can be acquired and exercised with the assistance of other lawyers and staff.[214]

Similarly, but more directly related to litigation, the New Hampshire Bar Association Ethics Committee advised that lawyers "have a general duty to be aware of social media as a source of potentially useful information in litigation, to be competent to obtain that information directly or through an agent, and to know how to make effective use of that information in litigation."[215] The types of data and method of preserving and recording social media postings and information will vary, but the core issue is being aware of social media as a potential source of information and its potential impact on the representation.

And in the reverse context, attorneys should also be aware of ethical and legal obligations that can arise if social information or content is deleted under some circumstances. For example, a Virginia attorney was suspended for five years for misconduct that involved the attorney instructing his client to delete certain damaging photographs from a Facebook account after a document production request was issued, withholding the photographs from opposing counsel,

---

[206] Carole A. Levitt & Mark E. Rosch, *Social Media Evidence: Ignore It at Your Own Risk*, Law Practice Today (February 13, 2015) *available at* https://www.lawpracticetoday.org/article/social-media-evidence.

[207] Prof'l Ethics of The Fla. Bar, Op. 14-1 (2015).

[208] N.H. Bar Ass'n Ethics Comm., Advisory Op. 2012-13/5.

[209] New York Cty. Law. Ass'n, Ethics Op. 745 (2013).

[210] Pa. Bar Ass'n, Formal Op. 2014-300 (2014).

[211] Phila. Bar Ass'n, Op. 2014-5 (2014).

[212] W. Va. Office of Disciplinary Couns., L.E.O. No. 2015-02 (2015).

[213] *See also*, *Legal Ethics and Social Media, A Practitioner's Handbook*; Jan I. Jacobowitz and John G. Browning, *available at* https://law.ku.edu/sites/law.ku.edu/files/docs/media_law/2018/legal-ethics-chapter-3.pdf.

[214] DC Bar Ethics Op. 317, s*upra* note 205, *a*t 2.

[215] N.H. Bar Ass'n Ethics Comm., Advisory Op., s*upra* note 208, at 3.

and withholding from the court emails discussing the plan to delete the information from the Facebook page.[216] An in depth discussion of litigation holds and document retention is beyond the scope of this opinion, but the disciplinary action provides a cautionary tale regarding the potential consequences if lawyers do not recognize that social media content may be evidence and should be treated accordingly.

VII. CONCLUSION

Advances in technology have created valuable opportunities for attorneys and law firms of all sizes to provide high quality services using increasingly efficient and convenient communications. It is difficult for many lawyers now to conceive of completing complex transactions or litigating matters using only a typewriter and lengthy delivery methods. With the development of ever more powerful technologies and computing abilities, including artificial intelligence, blockchain, and complex predictive analytics, lawyers, individuals and business will continue have new tools at their disposal. With these advances and increased speed of information flow, the potential risks will also evolve. In order to competently (and hopefully with excellence) serve clients and fulfil ethical obligations to protect client information and property, it will be essential that attorneys also evolve in their understanding of the technologies that affect their practices and clients' interests. Fortunately, the relevant professional rules do not require a one-size fits all approach, and there are multiple reasonable and viable paths forward for lawyers.

[216] *In re Matter of Matthew B. Murray*, VSB Nos. 11-070-088405 and 11-070-088422 (July 9, 2013) *available at* https://www.vsb.org/docs/Murray-092513.pdf.

Attachment A:

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.

   - Evaluate 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 arise 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 and unvigilant 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 downtime and unavailability/accessibility.

   - Evaluate 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 suitability 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 online and digital 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 there are 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 data retention terms and measures are in effect (are they sufficient)?
    - 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. Ongoing Due Diligence—Monitoring and Policies

- 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.

AUTHOR BIOGRAPHIES

REGINA B. AMOLSCH

Regina Amolsch is a partner at Plave Koch PLC, a franchise boutique in Reston, Virginia. For over 20 years, Regina has counseled franchisors, licensors, and manufacturers on the transactional, regulatory and intellectual property issues important in franchise programs. Regina represents start-ups, early-stage franchisors and industry leaders in connection with the development and maintenance of their franchise and licensing programs and advises private equity investors on the acquisitions of franchise companies and exemption-based franchising. Regina has also developed particular interest and experience in medical franchising and has counseled numerous clients on the expanded use of franchised and non-franchised licensing programs. In addition to her franchising and licensing work, Regina also advises clients on general corporate transactions, trademark and privacy matters, and dispute resolution.

Before entering private practice, Regina served as Assistant Counsel at Hooters of America, Inc., the national franchisor and operator of the "Hooters" restaurant chain. As Assistant Counsel, 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.

Regina regularly speaks at industry seminars and professional training programs on franchising and intellectual property issues. Regina has received industry recognitions, including being named to *Who's Who Legal - Franchise* and *The Best Lawyers in America*© and has co-authored articles appearing in various franchise-related publications and seminar presentations. Regina is member of the ABA Forum on Franchising and the International Franchise Association, and currently serves on the IFA Legal Symposium Task Force.

LESLIE SMITH

Leslie Smith is a partner with Foley & Lardner LLP, and a member of the firm's Distribution & Franchise Practice Group, and Office Managing Partner of the firm's Miami, Florida office. Ms. Smith litigates a range of commercial matters at both the trial and appellate levels in both federal and state courts. Her franchising and distribution practice provides clients with counseling and litigation services, from initial negotiations through resolution, including mediation, arbitration and trial. She has represented franchisors in a variety of commercial disputes involving trademarks, trade secrets, covenants not to compete and vicarious liability claims. Ms. Smith was named to BTI Consulting Group's coveted Client Service All Star Team in 2017. This honor is bestowed upon individual attorneys who deliver outstanding client service according to corporate counsel interviewed at large organizations with $1 billion or more in revenue. Ms. Smith has been Peer Review Rated as AV® Preeminent™, the highest performance rating in Martindale-Hubbell's peer review rating system. Ms. Smith has been recognized in the trade press, most recently by her peers in the 2019 edition of *The International Who's Who of Franchise Lawyers*. *Chambers USA: America's Leading Lawyers for Business* also recognized her as one of the top franchise attorneys nationwide (2010 - 2019) and she was selected by her peers for inclusion in *The Best Lawyers in America*© since 2013. In addition, Ms. Smith was selected for inclusion in the 2014 - 2019 *Florida Super Lawyers*® lists, and the *South Florida Legal Guide* named her a Top Lawyer - Franchise in the 2015-2019 editions.

Ms. Smith earned her J.D., with honors, from the University of Florida, an M.A. from the London School of Economics, and a B.A., *cum laude*, from Southern Methodist University.