Technology in the Law Practice: Avoiding Ethical Pitfalls in the Digital Age (Ethics)

Danielle Hall, Executive Director,
Kansas Lawyers Assistance Program

Friday, April 29th
3:00 – 3:50 p.m.

TECHNOLOGY IN THE LAW PRACTICE:

AVOIDING ETHICAL PITFALLS

Technology has become an important part of a modern law practice or legal department. Lawyers use technology to do everything from sending communication, storing documents, and even processing payments. Lawyers, however, should not only be able to recognize when to use technology to provide legal services efficiently, but also understand how to use that technology responsibly and ethically. The first ethical duty of a lawyer is to practice competently, which includes understanding and managing technology in the law office while ensuring client confidences. During this seminar, we will discuss how to leverage some of the benefits and risks associated with using technology, as well as your ethical obligations when using technology in your practice.

Danielle M. Hall
Executive Director
Kansas Lawyers
Assistance Program

INTRODUCTION

One of the basic concepts of our Rules of Professional Responsibility is protecting client confidences. KRPC 1.6 explicitly states, "A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation…" Protecting client confidences is an obligation we have traditionally applied—and still do—in the "brick and mortar" setting of a physical office, traditionally storing files in a locked cabinet, behind locked doors.[1] We still talk to our clients privately in person and on the phone and in letters. The landscape of client communication, however, has changed dramatically over the last ten years. For instance, items such as email, text messaging, and client portals have all changed how we deliver information to clients.

Just over the last two years, the COVID-19 pandemic has also drastically impacted the landscape in which lawyers and law firms practice law. For forward-thinking, technologically inclined practitioners, the COVID-19 pandemic confirmed that implementing tools to facilitate remote work for employees and communication with clients is the way to go. For many others, the pandemic exposed critical areas where advancements are necessary. Law firms have transitioned towards remote practices and greater flexibility in practice model structures. Virtual meetings platforms—such as Zoom, Microsoft Teams, and WebEx—have become the norm in the law practice for everything from appearing for court to client meetings. Many ethics and legal tech commentators, including myself, anticipate that several of the changes made to the way law is practiced during the pandemic may be here to stay for the long term. While the landscape may have changed, our obligations have not.

As lawyers begin introducing new technologies to their practice—shifting to more virtual environments—they must do so with the Rules of Professional Conduct in mind. In addition to new confidentiality concerns, technology competence is an issue lawyers should be aware of—think lawyer cat. Just twenty years ago, as ethics commentator Andrew Perlman points out, lawyers were not expected to know how to protect confidential information from cybersecurity

[1] Tracy Vigness Kolb, *Technology Competence: The New Ethical Mandate for North Dakota Lawyers and the Practice of Law*, at 2, (2016).

threats, use the Internet for marketing and investigations, employ cloud-based services to manage a practice and interact with clients, implement automated document assembly and expert systems to reduce costs, or engage in electronic discovery.[2] Heck, just two years ago we were not expected to know how to use Zoom as our primary method of communication, despite its several years of existence.

Because of the digital age we now live and work in, our ethics rules need to reflect this change, giving us both guidance and flexibility to practice in the modern era. As a result, both the ABA and several of the states have started offering guidance. In fact, some guidance can be found in our existing Rules of Professional Conduct, while others can be found in recently released ethics advisory opinions. As such, there is no time like the present to begin improving your technology skill and become more familiar with the applicable rules.

ETHICS AND TECHNOLOGY

The American Bar Association Commission on Ethics 20/20

The American Bar Association (ABA) Commission on Ethics 20/20 was created in 2009 by then-ABA president Carolyn Lamm to perform a thorough review of the ABA Model Rules of Professional Conduct and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments. The group's challenge over the next several years is to study these issues and, with 20/20 vision, propose policy recommendations that will allow lawyers to better serve their clients, the courts, and the public. [3]

In August of 2012, the Commission proposed several amendments to the ABA Model Rules of Professional Conduct. These proposals were then adopted by the ABA House of Delegates. The following amended rules contain amended language that encompasses aspects of the use of technology by the legal profession.

---

[2] Andrew Perlman, *The Twenty-first Century Lawyer's Evolving Duty of Competence*, The Professional Lawyer, Vol. 22, No. 4 (2014).

[3] ABA Commission on Ethics 20/20, information available at: http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20/about_us.html.

Amendment Regarding a Lawyer's Duty of Competence (Model Rule 1.1)[4]

Because technology use in law firms and legal departments is now universal, the Commission proposed and the House adopted an amendment to Comment [8] of Model Rule 1.1 to remind lawyers that being competent includes not only staying abreast of changes in the law and its practice, but also includes having a basic understanding of the benefits and risks of relevant technology.[5] The amendment makes clear that a lawyer or law firm should be versed in the implications of technology used in the course of representation, including knowing any limitations of their personal understanding and hiring the right professionals to help make informed choices.[6]

Amendment to the Rule on Confidentiality of Information (Model Rule 1.6)[7]

The 2012 adopted amendments clarify that lawyers should take reasonable precautions to protect client confidences from inadvertent or unauthorized access or disclosure and identify the factors that lawyers should consider when determining whether they have taken reasonable precautions. To help lawyers better understand how to protect client confidences in the digital age, the Commission proposed, and the House adopted black letter paragraph (c) to Model Rule 1.6.[8] This paragraph clarifies lawyers have a duty to take reasonable precautions to protect client confidences, not only from inadvertent or unauthorized disclosure, but from inadvertent or unauthorized access. In discussing the duties under Rule 1.6, the Commission made clear that they understand lawyers can't guarantee electronic security any more than they can guarantee the physical security of documents stored in a file cabinet or offsite storage facility. Just like fires and floods, computer systems can suffer catastrophic events and they can also be hacked. This rule, however, does not impose a duty on lawyers to achieve the unattainable.[9] What constitutes

---

[4] ABA Commission on Ethics 20/20 Revised Draft Resolution for Comment – Technology and Confidentiality, at 4 (February 2012) (available at: http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120221_ethics_20_20_revised_draft_resolution_and_report_technology_and_confidentiality_posting_final.authcheckdam.pdf) (hereinafter *Ethics 20/20 Draft Resolution for Comment Re Technology*).

[5] Catherin Saunders Reach, *Ethics 20/20, Security, and Cloud Computing*, ABA TECHSHOW, at 4 (2015).

[6] *Id.*

[7] *Ethics 20/20 Draft Resolution for Comment Re Technology*, at 8.

[8] Saunders Reach, *supra* note 5, at 4.

[9] *Id* at 5.

reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.[10] In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.[11] Importantly, mere inadvertent or unauthorized disclosure of, or unauthorized access to this information does not, by itself, constitute a violation of the rule.

Amendment to the Rule on Responsibilities Regarding Non-Lawyers Assistance (Model Rule 5.3)[12]

The adopted amendments to Model Rule 5.3, added commentary regarding outsourcing. Comment [3] now provides that a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's obligations. Outsourcing refers generally to the practice of taking a specific task or function previously performed within a firm or entity and, for reasons including cost and efficiency, having it performed by an outside service provider. [13] Examples of outsourced legal work include, "investigative services, offsite online data storage or online practice management tools (e.g. 'cloud computing services') …"[14]

The Kansas Ethics 20/20 Commission

In February 2013, the Kansas Ethics 20/20 Commission was appointed and directed by the Kansas Supreme Court to undertake a review of the model rule changes adopted by the ABA in 2012. The Kansas Commission reviewed the adopted amendments and proposed a series of rule changes based upon this review. [15] In the Memorandum to the Supreme Court from the Commission, it stated as a summary of the amendments:

---

[10] Aba Formal Opinion 477, at 4 (2017). The full opinion is available at http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf.

[11] *Id.*

[12] ABA Commission on Ethics 20/20: Revised Draft Resolution for Comment – Outsourcing, at 2 (February 2012) (available at: http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120221_ethics_20_20_revised_draft_resolution_and_report_outsourcing_posting_final.authcheckdam.pdf) (hereinafter *Ethics 20/20 Draft Resolution for Comment Re Outsourcing*).

[13] ABA Commission on Ethics 20/20 Resolution and report, 105 C, at 4 (Aug. 2012).

[14] *Id.*

[15] Information regarding the Commission and the rule changes can be found at: http://www.kscourts.org/pdf_inc/ethics-20_20-recommended-changes.pdf.

1. **ESI.** To keep up with changing times, a number of the amendments address electronic data, electronically-stored information ("ESI"), and electronic communications, including advertising via blogs and websites. The rules also add a requirement that lawyers keep abreast of changes in technology.
2. **Outsourcing.** With the increase in outsourcing of legal services, the need to maintain confidentiality and adequate supervision are addressed in several rules.
3. **Confidentiality.** A renewed focus on confidentiality allows the limited disclosure of information to identify conflicts in relationship to firm mergers and lateral hires, and expands on the need to avoid the inadvertent disclosure of client confidential information…[16]

The amendments proposed by the Kansas Commission were adopted by the Kansas Supreme Court in January of 2014 and were effective March 1, 2014. Amendments of note—which relate to technology—can be found in KRPC 1.1, 1.6, and 5.3.[17]

KRPC 1.1 Competence

> Comment [8]. To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)

KRPC 1.6 Confidentiality of Information

> 1.6(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

[16] Kansas Ethics 20/20 Commission Memorandum Re Ethics 20/20 Commission Report, at 1 (June 2013) (available at: http://www.kscourts.org/pdf_inc/ethics-20_20-commission-report.pdf)
[17] *Id.*

> Comment [26]. 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.

It then goes on to read:

> 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].

KRPC 5.3 Law Firms and Associations: Responsibilities Regarding Nonlawyer Assistance

> Comment [3]. A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to

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

What Does Technology Competence Even Mean?

KRPC 1.1, Comment [8] makes clear, a lawyer or law firm should be well versed in the implications of technology used in the course of representation, including knowing any limitations of their personal understanding and hiring the right professionals to help make informed choices.[18] It requires every lawyer:

- keep abreast of changes to technology used in legal practice;
- develop an awareness of technology, its functionality, and available offerings;
- gain a grasp of the risks and benefits associated with using technology; and
- attain reasonable level of skill in a chosen technology.[19]

[18] *Id.*

[19] Ivy Grey, *Exploring the Ethical Duty of Technology Competence*, Law Technology Today (March 2017). Available at http://www.lawtechnologytoday.org/2017/03/technology-competence-part-i/.

To date, 40 states—in addition to Kansas— have formally adopted Model Rule 1.1, Comment [8]. As more and more states continue to adopt this standard, lawyers cannot continue to ignore the focus on technology competence. In fact, the amended commentary to the rule will preclude a lawyer from pleading ignorance to new technologies or the risk associated with technology.[20]

A lawyer's fundamental duty has always been to provide competent representation to his or her client. Historically, the concept of a "competent" lawyer primarily focused on a lawyer's knowledge of a substantive area of the law coupled with his or her experience and ability to represent a client in a particular engagement.[21] This view, however, has become outdated with regard to technology, and the amendments to the rules were necessary to reflect the importance of technology in the delivery of legal and law related services.[22]

Per the rules, lawyers should have a basic understanding of the technology they employ, in addition to acknowledging the risks associated with the use of that technology and what can be implemented to mitigate those risks. It is important to remember, however, that competence does not mean perfection or expertise, instead it requires the baseline understanding of, and reasonable proficiency in, the technology being used.[23] And, just as with any other practice area or skill, a lawyer's duty of technology competence can be achieved through continuing study and education or through association with others who are well versed in the area.[24]

While there are plenty of critics of the amended comment to Rule 1.1—saying that the amendment is vague or that the ABA might as well say water is wet—one must keep in mind the area of technology is an ever-changing landscape. The chief reporter of the ABA commission on Ethics 20/20, Andrew Perlman, explained that the standard had to be nebulous, because "a competent lawyer's skill set needs to evolve along with technology itself," and "the specific skills

[20] Steven Puiszis, *A Lawyers Duty of Technological Competence*, American Bar Association 2017 Professional Responsibility Conference, at 3, available at https://www.americanbar.org/content/dam/aba/events/professional_responsibility/2017%20Meetings/Conference/conference_materials/session4_information_governance/puiszis_lawyers_duty_technological_competence.authcheckdam.pdf.
[21] *Id* at 1.
[22] Perlman, *supra* 2, at 25.
[23] Grey, *supra* note 19, at 1
[24] KRPC 1.1, Comment 2

lawyers will need in the decades ahead are difficult to imagine."[25]

When we consider what is means to stay abreast of the benefits and risks associated with the use of technology, it is clear that the "list" of what a lawyer should know is one that is not static. A good place to start, however, is by asking yourself if you really know how to use the technology that is already implemented in your office. For instance, let's take Microsoft Word. Do you know how to automatically number paragraphs, insert and fix footers, create a table of contents, convert the document to a PDF, apply and modify styles, and remove metadata?

Lawyer and ethics commentator, Steven Puiszis, has listed several broad areas in which lawyers should be expected to demonstrate technological competency. They are:

- Cybersecurity, or safeguarding electronically stored client information;
- Electronic Discovery, including the preservation review and production of electronic information;
- Leveraging technology to deliver legal services, such as automated document assembly, electronic court scheduling and file share technologies;
- Understanding how technology is used by clients to offer services or manufacture products;
- Technology used to present information and/or evidence in the courtroom; and
- Internet-based investigations through simple Internet searches and other research tools available online.[26]

As I have already mentioned, this list is certainly not one that is exhaustive, as a lawyer's duty of competence must evolve as the technologies we use to provide legal services evolve. Additionally, I would argue that in addition to this list, it is important for lawyers to know how the use of technology works with our other Rules of Professional Conduct, and not just the basic idea of technology competence.

[25] Perlman, *supra* note 2, at 25.
[26] Puiszis, *supra* note 20, at 2.

Using Technology Responsibly

The use of technology presents special ethical challenges, particularly in the areas of competence and confidentiality. Lawyers also have common law duties to protect client information and may have contractual and regulatory duties. The duties to safeguard information relating to clients are minimum standards with which lawyers are required to comply. Lawyers should aim for even stronger safeguards as a matter of sound professional practice and client service.

Together, the changes to KRPC 1.1, 1.6 and 5.3 require lawyers using technology to take competent and reasonable measures to safeguard client data. This duty extends to all use of technology, including computers, networks, smartphones, mobile devices, technology outsourcing, and cloud computing.

The requirement for lawyers is reasonable security, not absolute security. For example, New Jersey Ethics Opinion 701 states:

> …[r]easonable care,' however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible…" Recognizing this concept, the Ethics 20/20 amendments to the Comment to Model Rule 1.6 include "…[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.[27]

Ethics requirements establish minimum standards, and while lawyers are concerned about security, confidentiality, and control when it comes to technology, their reported behavior in the regarding precautionary measures when using technology, however, simply do not reflect their level of concern. For instance, in the *2020 ABA Technology Report* respondents were asked if encryption was used when sending confidential information or document via email to a client.

[27] A copy of New Jersey Ethics Opinion 701 can be found at https://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf.

Only 39% of respondents reported using the precautionary measure [28] Similarly, only 39% report using two-factor authentication and 29% report using remote device management and wiping.[29] The reason why precautionary measures are so important is because there are certain risks involved when using certain technology. The risks identified by the ABA Ethics Commission 20/20 included:

- Inadequate physical protection for devices or not having methods for deleting data remotely in the event a device is lost or stolen.
- Weak passwords.
- Failure to purge data from devices before they are replaced.
- Lack of appropriate safeguards against malware.
- Infrequent backups of data.
- Using computer operating systems that do not contain the latest security protections
- Inappropriately configured software and networking settings to minimize security risks.
- Not encrypting sensitive information or identifying (and when appropriate, eliminating) metadata from electronic documents before sending them.
- Using Wi-Fi hotspots in public places as a means of transmitting confidential information.
- Unauthorized access to confidential client information by a vendor's employees or by outside parties via the internet.
- The storage of information on servers in countries with fewer legal protections for electronically stored information.
- A vendor's failure to back up data adequately.
- Unclear policies regarding ownership of stored data.

[28] John G. Loughnane, *ABA TECHREPORT: Cybersecurity* (2020). Available at: https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/
[29] *Id.*

- The ability to access the data using easily accessible software in the event that the lawyer terminates the relationship with the cloud computing provider or the provider changes businesses or goes out of business.
- The provider's procedures for responding to (or when appropriate, resisting) government requests for access to information.
- Policies for notifying customers of security breaches.
- Policies for data destruction when a lawyer no longer wants the relevant data available or transferring the data if a client switches law firms.
- The extent to which lawyers need to obtain client consent before using cloud computing services to store or transmit the client's confidential information.[30]

Most of the risks addressed by the Commission involve the unauthorized disclosure of client information, and as there are more and more reports of data breaches in the headlines, those risks become more recognizable. For instance, according to data security software company the Digital Guardian, at least 80 percent of the nation's 100 largest law firms have been affected in some way by a data breach. [31] However, please acknowledge that solos and small firms are not exempt. In fact, as early as February of 2014, a solo firm in North Carolina fell victim to a virus know as Crypto Locker, which held all his firm's data for ransom.[32]

The data breach of Panamanian law firm Mossak Fonseca, has been one of the most reported law firm data breach to date. This breach is more commonly referred to as the Panama Papers, and involved the breach of 11.5 million documents.[33] The documents included emails, PDF and Word documents, and database entries.

The hack on Mossak Fonseca was certainly not complex in nature. In fact, it was so simple that some experts say a teenager with no hacking knowledge other than basic googling skills

[30] ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies, For Comment: Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology, at 3-6 (2010).
[31] Ellen Rose, *Most Big Firms have had Some Hacking: Business of Law*, Bloomberg (March 10, 2015) (available at: https://www.bloomberg.com/news/articles/2015-03-11/most-big-firms-have-had-some-form-of-hacking-business-of-law).
[32] WSOCTV, *Computer Virus Locking Important Files Targets Local Business* (Feb. 6, 2014) (available at: http://www.wsoctv.com/news/local/computer-virus-locking-important-files-targets-loc/113739524).
[33] Luke Harding, *What are the Panama Papers? A Guide to History's biggest Data Leak*, The Guardian (April 5, 2016) (available at: https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers).

could have done it.[34] The attackers point of entry was through older versions of popular open-source web server software WordPress. Security experts think it is likely that an attacker gained access to the Mossak Fonseca WordPress website via a vulnerability in WordPress.[35] This vulnerability had long since been updated prior to the attack, but Mossak Fonseca simply had not updated the software on their web server. From there the attackers were able to infiltrate their entire firm database. And while the stories surrounding the Mossak Fonseca breach are made for TV—they were breached by hacktivist that exposed criminal activity at the firm—the reality is that many firms are vulnerable to cybersecurity incidents and breach potentially exposing client information.

Law firms and legal departments are considered by attackers to be "one stop shops," because they have high value information that is well organized. Hackers target money, personally identifiable information that can be converted to money, client business strategy, intellectual property and technology, and information about deals and litigation. [36] Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.[37]

Because personal identifiable information is so valuable in the digital age we live in, lawyers must take precautions to protect their client's information and uphold their duty of confidentiality. Lawyers must be reasonable with the technology they use, and they must be competent in its use to ensure that those client confidences are not broken.

PRACTICAL APPLICATION OF THE ETHIC RULE TO TECHNOLOGY USE

Cloud Technology, Online Data Storage and Third-Party Vendors

File hosting services, such as Dropbox, Box, and Google Drive, all store files via cloud computing. Broadly defined, cloud computing (or "Software as a Service") refers to a class of

[34] Jason Bloomberg, *Cybersecurity Lessons Learned from Panama Papers Breach*, Forbes (April 21, 2016)
[35] *Id.*
[36] Sharon Nelson, *Egregious Data Breaches, Leaks and Hacks*, ABA TECHSHOW, (March 17, 2016).
[37] ABA Formal Opinion 477, at 2.

software that's delivered over the Internet via a Web browser—like Safari, Chrome, and Edge—rather than installed directly on the user's computer.[38] Lawyers and law firms see the cloud as a fast and scalable way to use advanced legal technology tools without the need for substantial upfront capital investment in hardware, software, and support services.[39]

Most lawyers have used the cloud for years, even if not in a law practice setting. If you use any online email products, you are using cloud computing. Also, if you have ever used Google Docs, Office 365, or even accessed a bank account online you are using cloud computing. As lawyers become accustom to the ease of using cloud computing for their personal uses, they come to expect that same ease in a professional setting. Additionally, in the last few years, the use of the cloud has become far more commonplace as cloud service providers recognize the value of the legal marketplace. Everything from case management software, discovery software, and document assembly has been developed now that the use of the cloud is becoming more prevalent in the legal profession. Every year at the ABA TECHSHOW, vendors flock to the exhibit hall to show off their technology—almost all of them run on the cloud.

Even though most of us use or have used some sort of cloud computing in our personal lives, cloud computing continues to be a major topic for the legal profession, despites its uptick in usage. One of the defining—and for lawyers, the most alarming—characteristics of the software is that the data is stored over the internet on a server owned by a third party, rather than on the user's computer.[40] For example, when you use a web-mail service like Gmail, your actual emails reside on a remote server hosted by Google and not on your own hard drive or server.[41] Because of this characteristic, lawyers often want to know if cloud based software is ethical to use, and if it is secure.

Many states have weighed directly in on answering the question regarding cloud computing and ethics. Those states that touch on the principles of cloud computing generally agree that lawyers should maintain reasonable care in the evaluation of services of a cloud or

[38] What is Cloud Computing? IBM (available at: https://www.ibm.com/cloud-computing/what-is-cloud-computing).
[39] Kennedy, *ABA TECHREPORT: Cloud Computing*, at 2 (2016) (available at https://www.americanbar.org/content/dam/aba/publications/techreport/2016/cloud/cloud-computing.authcheckdam.pdf)
[40] Saunders Reach, *supra* note 5, at 3.
[41] *Id.*

third-party provider. About 20 jurisdictions have ethics opinions about the use of the cloud. All say that lawyers can use the technology, however, you should investigate the products, the methods used, and keep up with any changes the provider may make. While Kansas is not among the 20 jurisdictions to offer an opinion, the rules relating to technology should give guidance on this issue, since their original intent was to address technology. The ABA Legal Technology Resource Center maintains a list of cloud ethics opinions with a summary and links to the opinions at:

https://www.americanbar.org/content/dam/aba/images/legal_technology_resources/CloudEthicsOpinions2019/cloudethicsopinions2019.pdf

When asked about the security of cloud-based software, I often describe it being similar to the difference between holding your money in your back pocket vs. putting it in the bank. Let's say you have a 100-dollar bill. You could walk around town with that 100-dollar bill in your pocket, where you could get pick-pocketed, it could fall out of your pocket, or you simply could misplace the pair of pants it was in. The alternative is that you could put the 100 dollars in the bank. I think we can all agree that the bank is the safer place to put the money, but why?

There is obviously a sense of security in the bank. This is because they have a vault to keep my money in. This vault is locked and may need a key or password, only certain people have access to it, and the bank could have security guards on staff. Think about cloud based systems being the bank with your data. The good programs often need passwords for security reasons, the data is often encrypted, limited people have access to your data and often the location of the server is remote and secure. Now, I am not saying that every system out there is fool-proof and has top-notch security—you should definitely be particular about who holds your data as you will see below—but that is why you as the lawyer have to do your due diligence in researching the security of your provider.

One of the most popular cloud file storage and sharing services is Dropbox, with more than 600 million users according to SaaS Scout Research Group.[42] Dropbox continues to be the most

[42] https://saasscout.com/statistics/dropbox-statistics/#:~:text=Dropbox%20has%20over%20600%20million,of%20content%20uploaded%20to%20Dropbox

used cloud technology in the legal in the profession, as reported by the *2020 ABA Technology Report*. Dropbox was at the top of the list with 67% of respondents reporting that they use the service. [43] In fact, five times as many respondents used Dropbox as the most popular legal-specific cloud tool. However, is the software secure? That is to be debated.

On the Dropbox homepage, it says that it uses "256-bit AES encryption" (the strongest normal standard today) and two-step verification. Encryption and two-step verification are both security aspects that you should search for in a product. Additionally, your Dropbox data is stored on Amazon's S3 storage service, which means that it is securely encrypted, but Dropbox retains the encryption keys and could theoretically access it. Dropbox's privacy policy states that certain employees have this power for use when data is legally required to be disclosed. Because the file data arrives at Dropbox in unencrypted form—which is the point of contention for many—the file could be accessed and reproduced in original format by Dropbox to comply with a court order. This is a prime example of why you should pay attention to privacy policies and user agreements.

If you want to address this security risk, one alternative would be to add encryption to some or all your files before placing them in your Dropbox drive on your computer. Carefully consider which of your files need to be encrypted. If you are looking at using Dropbox to back up your personal bank records and tax returns, should those be encrypted? If your client has given you the recipe for something, should it be encrypted before you move it to Dropbox for storage? It is highly unlikely that all documents stored on Dropbox require encryption.

Another example of why reading user agreements is important, is that Dropbox also contains language in the agreement which states that they may "*transfer, store and process your data in another location other than the customer's country."* If you work with banks, insurance companies, or healthcare organizations, you are most likely forbidden from offshore data storage.[44]

---

[43] Kennedy, ABA TECHREPORT: 2020 Cloud Computing, available at: https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cloudcomputing/

[44] Accellis Technology Group*, Ethical Considerations of Using Dropbox for Your Firm*, at 5 (available at: https://accellis.com/wp-content/uploads/Ethical-Considerations-of-Using-Dropbox-in-Your-Law-Firm-21.pdf).

One last thing to be aware of with using Dropbox, is that if you need to house documents in a system that is compliant with HIPAA regulations, then you will want to upgrade to Dropbox Business. Neither the free or Pro accounts guarantee compliance with HIPAA, but the Business plan does. This is just another example of why it is important to pay attention to the details, compare plans, and look at your service agreements. The bottom line is that terms and conditions change over time (often silently); companies flop; people get sued and lose; and what was once a no-brainer decision yesterday, may be a mistake today. [45]

Every ethics opinion published to date regarding cloud technology asserts that a lawyer must be reasonable, which includes doing your due diligence when it comes to deciding what products to use. Additionally, KRPC 5.3 Comment [3] states, "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." This would of course include the duty of confidentiality. Therefore, it's important to carefully examine all technology before buying, whether it's SaaS or traditional. Be sure to ask any vendor some questions before committing your data to their hands. Vendors that aren't willing or able to answer questions should be treated with caution. Even after a lawyer examines various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess to confirm that the lawyer's actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.[46]

Email Encryption

Encryption has become a hot topic as it relates to data breaches, remote work environments due to the COVID-19 Pandemic, and lawyer responsibilities. Under our rules, should lawyers use encryption when sending information through email? Should we have our information on mobile devices encrypted? We all know that confidentiality is the foundation to client communications, but do we think about this when sending a routine email? There are many

[45] *Id*. at 12.
[46] ABA Formal Opinion 477, at 10.

security issues associated with email, ranging from the simple to the complex, such as hitting the "reply all" instead of reply, or being a victim of a phishing email. When the information you are sending via email is confidential in nature, adding a level of encryption can reduce the risk of those security issues, and help you maintain your duty of confidentiality.

In 2011, the ABA issued formal opinion 11-459 to address sending communications via email to clients. The opinion states:

> Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client. [47]

I will note that this opinion mentions nothing about encrypting emails, but remember the opinion was written in 2011, since then several software services have been developed—some specifically for law offices—that allow you to encrypt your communications via email. The key line to recognize from the above excerpt is the reference to reasonable care. This is a common thread among the use of technology within the profession. So, does reasonable care include encrypting confidential information sent via email to clients? An answer to this question may be found in the State Bar of Texas Opinion No. 648. [48]

The State Bar of Texas Opinion No. 648 was one of the first opinions to tackle the confidentiality issues of email, addressing whether a lawyer has the duty to encrypt their emails. The opinion states:

> Having read reports about email accounts being hacked and the National Security Agency obtaining email communications without a search warrant, the lawyers

[47] ABA Formal Opinion 11-459, at 4 (2011). The full opinion can be found at http://www.americanbar.org/content/dam/aba/publications/YourABA/11_459.authcheckdam.pdf.
[48] The State Bar of Texas Ethics Opinion 648 can be found at: https://www.texasbar.com/AM/Template.cfm?Section=Past_Issues&Template=/CM/ContentDisplay.cfm&ContentID=30523.

> are concerned about whether it is proper for them to continue using email to communicate confidential information.[49]

The opinion goes on to read:

> Under the Texas Disciplinary Rules of Professional Conduct, and considering the present state of technology and email usage, a lawyer may generally communicate confidential information by email. Some circumstances, may, however, cause a lawyer to have a duty to advise a client regarding risks incident to the sending or receiving of emails arising from those circumstances and to consider whether it is prudent to use encrypted email or another form of communication. [50]

The opinion also lists 6 examples of when lawyers should consider whether the confidentiality of the information will be protected if communicated by email, and whether it is prudent to use encrypted email or another form of communication. Here are those examples:

1. Communicating highly sensitive or confidential information via email or unencrypted email connections;
2. Sending an email to or from an account that the email sender or recipient shares with others;
3. Sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer;
4. Sending an email from a public computer or a borrowed computer or where the lawyer knows that emails the lawyer sends are being read on a public or borrowed computer or unsecure network;

[49] Ethics Committee for the State Bar of Texas, *Ethics Opinion No. 648*, Florida B.J. 78, at 480 (2015).
[50] *Id.*

5. Sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protect by a password; or
6. Sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, without a warrant.[51]

Because Rule 1.6 requires fact-based analysis to determine the reasonableness of the methods employed to maintain confidentiality, strong protective measures, like encryption are warranted in some circumstances.[52] Cyber-threats and the proliferation of electronic communications devices have changed the landscape, and it is not always reasonable to rely on the use of unencrypted email.[53] Lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the factors found in Comment [18] of the Model Rules, to determine what effort is reasonable.[54]

The good news is that there are services out there that help make this process easier for the lawyer. A popular service is Citrix ShareFile. ShareFile has an easy to use Outlook or Gmail plugin that allows you to encrypt an entire email or an attached document. The client is then taken to a sign in page to gain access to the document. There are also several other companies out there that offer this type of service for law firms as well, such as RPost, HushMail, Virtru, and Enlocked.

I will also mention that there are ways you can encrypt your emails when using Outlook. Instructions on how, can be found at https://support.office.com/en-us/article/Encrypt-e-mail-messages-84d7e382-5f76-4d71-8705-324489b710a2, however, you and the client must share your digital ID or public key certificate with each other before either party can open the encrypted communication. Gmail messages can also be encrypted straight from your Gmail account; those instructions can be found at:

[51] *Id.* at 481.
[52] ABA Formal Opinion 477, at 5.
[53] *Id.*
[54] *Id.* The factors for determining reasonableness in Kansas can be found in KRPC 1.6 Comment [26].

http://www.computerworld.com/article/2473585/encryption/easily-encrypt-gmail.html.

I have, however, found this process to be even more cumbersome than encrypting in Outlook. If you want something that is easy to use to encrypt you emails, I suggest investing in a product that has worked with law firms and understands your need for confidentiality.

One last alternative that is easy to do if you are attaching a document to an email is to simply encrypt the word or pdf document itself. This is a simple process, which requires you to set up a password to have access to the document. Both Microsoft Word and Adobe have simple ways you can do this. The most important thing to remember is to not send the password to the person in the email which contains the attachment or within a subsequent email.

- You can find instructions for password protecting a PDF at: https://helpx.adobe.com/acrobat/using/securing-pdfs-passwords.html.
- You can find instruction for password protecting a Word document at: https://support.office.com/en-us/article/Password-protect-a-document-8f4afc43-62f9-4a3a-bbe1-45477d99fa68.

Finally, when determining whether to employee technology like encryption, remember your duties under KRPC 1.4 with regards to communication. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved.[55] The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted.[56]

Passwords and Two-Factor Authentication

Password security is key when it comes to protecting yourself from potential security risks associated with the use of technology and data breaches, however, many still often reuse passwords or create small variations on a theme in their passwords across sites. A weak password used at a low security website, can allow hackers to gain a toehold and use the password more

[55] ABA Formal Opinion 477, at 10 (2017).
[56] *Id.*

easily gleaned there in attempt to gain access to the user's more sensitive information.[57] I am still amazed at the number of people who use passwords that are easily guessed. For instances, if you Google "top used passwords," all results will tell you the same thing. Passwords like 123456, 1234678, and yes, even "password" are still the most used passwords. Hopefully your password is not one that is on this list of shame.

When it comes to passwords, always be sure that you change your password from the default password setting that many products come with. Many frauds begin simply by entering simple default passwords to see what information can be obtained. Avoid using obvious passwords like your name, your firm name or other things that are easily guessed. Strong passwords (those that contain 12 or more characters with a combination of upper and lowercase letters, symbols and numbers) are best, but can be difficult to remember. Using sentences (ilovelawyers) or sentences with symbols and numbers replacing letters (!L0v3l@wyer$) is a good way to strengthen your password, while maintaining a password that you can remember.

I often get asked about password managers, and if they are safe to use. Given the extensive number of passwords that people must remember, most security experts agree that passwords managers are one of the best options when it comes to password management. A password manager is designed to help you store, organize, and encrypt your passwords for online accounts and several devices. It is definitely a better alternative to reusing the same two or three passwords, or just writing them down and keeping them at your desk or on your mobile device. Additionally, because complexity matters when it comes to passwords, most password managers can generate them for you. If you use a password manager I suggest that you turn on the two-factor authentication option if available. The most popular password managers offer this as an option.

Even if you don't use a password manager, many popular services support two-factor authentication and you should turn it on when it is available on your accounts. There are three different types of authentications factors that currently exist. These include:

[57] ABA ETHICSearch, *How Ethical is Your Password, Ethics Tip of the Month* (February, 2013).

- Something you know – such as a username and password.
- Something you have – such as a mobile phone or special USB key.
- Something you are – such as a fingerprint or another biometric identifier.[58]

Two-factor authentication combines two of these factors to add an extra layer of security. Many popular services such as Facebook, Twitter, iCloud, Amazon, PayPal, LinkedIn, Snapchat, WordPress, and Gmail offer two-factor authentication. In most instances, your phone will be primarily used. It will be used either to receive codes by SMS or to generate them using special apps like Google Authenticator. While we all know that a phone can be easily lost or stolen, the good news is that most of the companies offering two-factor authentication offer a way to recover your account should that happen.

The Mobile Lawyer, Public Wi-Fi, and BOYD

With advancements in technology, comes advancements in the way we practice law—including where we practice. The practice of law is increasingly happening outside of the traditional law office setting. A lawyer's "office" is more mobile than it was even 10 years ago. Lawyers now work while they are at home or when traveling, or by simply checking an email while they are in line at a coffee shop. [59] Beyond their primary workspace, lawyers regularly perform legal work while outside of their office, and use everything from a desktop, laptop, tablet, or mobile phone to do it.

Part of the increase in mobility is, of course, due to cloud computing. The ability to access files, emails, and an abundance of information anytime and anywhere you need it has allowed lawyers to perform law-related tasks outside the traditional setting. This can, for obvious reasons, be both a curse and a blessing. While this modern business model may appear radically different from the traditional brick and mortar law office model of the yesteryears, the underlying

[58] Lucian Constantin, *5 Things you need to know about two-factor authentication*, PCWorld (March 31, 2016) (available at; http://www.pcworld.com/article/3050358/security/5-things-you-should-know-about-two-factor-authentication.html)
[59] Aaron Street, *ABA TECHREPORT: Mobile Technology*, at 1 (2016) (available at: http://www.americanbar.org/publications/techreport/2016/mobile.html).

principles of an ethical law practice remain the same. There is still a duty of confidentiality and competence when using mobile technology.

While this technology allows us to work more conveniently, it does come with some risks. Lawyers' increased use of mobile devices can lead to increased concerns that confidential client information will be lost, stolen, or inadvertently disclosed. Consider the possibilities: a lost iPhone full of attorney-client e-mails and texts; a wireless iPad communication session hacked, allowing the hacker full access to the information stored on the device; a malicious banking app on an Android phone allowing hackers to obtain attorney bank account information[60]

When using mobile devices, lawyers should keep in mind that these devices are easy to lose. Lawyers should consider password protecting and installing a wiping application feature. Many of these apps allow you to remotely find your device, as well as wipe information from the device or reset the device back to the factory settings like it was just out of the box. If a laptop is being used, rather than just using a password to access the device, consider encrypting the information contained on the laptop.

With the use of mobile devices, comes the use of the Internet to access information. According to the *2018 ABA Technology Report*, lawyers regularly use items such as their mobile devices for law related tasks.[61] The number of lawyers that report using public Wi-Fi without security a security measure, however, is a concern. 15% of respondents reported that they surf the net via public Wi-Fi with no security measure at all.[62] The open nature of a public WiFi network can allow for snooping by hackers, there could be other compromised machines on the network, or the hotspot itself could be malicious. Lawyers should obviously proceed with caution when using public Wi-Fi. You most certainly don't want to do any online banking or access any information sensitive in nature, because public Wi-Fi networks are often unencrypted, and therefore the network traffic is clearly visible to anyone within range.

---

[60] Jason Gonzalez and Linn Freedman, *Mobile Devices and Attorney Ethics: What are the Issues?*, The United States Law Week, 80 U.S.L.W. 747 (2011).
[61] Chad Burton*, ABA TECHREPORT: Virtual Law Practice*, at §2 (2018) (available at https://www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018VLP/)
[62] David Ries, *ABA TECHREPORT:Cybersecurity*, at § 11. (2018) (available at https://www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cybersecurity/)

California Formal Opinion 2010-179 (2010), addresses this issue of concern surrounding the use of public Wi-Fi. In the opinion, the scenario involves a lawyer who takes his work laptop to the local coffee shop and accessed a public wireless Internet connection to conduct legal research on a matter and email a client. He also takes the laptop computer home to conduct the research and email the client from his personal wireless system.[63] The opinion recognized that "due to the ever-evolving nature of technology and its integration in virtually every aspect of our daily lives, attorneys are faced with an ongoing responsibility of evaluating the level of security of technology that has increasingly become an indispensable tool in the practice of law." The opinion outlined factors in which a lawyer should consider when evaluating their duty of confidentiality and competence before using a specific technology, such as public Wi-Fi. Those factors were:

1. The lawyer's ability to assess the level of security afforded by the technology.
2. Legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person's electronic information.
3. The degree of sensitivity of the information.
4. Possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, including possible waiver of the privileges.
5. The urgency of the situation.
6. Client instructions and circumstances.[64]

Based upon these factors, the California Committee concluded that the lawyer risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on the client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions, and a personal firewall.[65] One way to solve the issues surrounding using public WiFi is to use a VPN (Virtual Personal Network). A VPN

[63] California Formal Opinion 2010-179, at 1 (2010).
[64] *Id.* at 3-6.
[65] *Id.* at 7.

allows you to connect to the Internet via server run by a VPN provider. All data traveling between your computer, phone, or tablet and the VPN server is securely encrypted.

In the California Formal Opinion, the Committee also concluded that if a personal home Wi-Fi system is configured with appropriate security features, then the lawyer would not violate his duties of confidentiality and competence by working from home.[66] One suggestion I have with regards to personal home Wi-Fi is that you want to make sure you are changing your default passwords on your wireless router, because hackers have managed to obtain access to those default passwords. If you don't change your password, then you may not be working from a connection that "has been configured with appropriate security features."

In the circumstance outlined above, the lawyer was using his work laptop to work remotely, however, what if had been his own personal mobile device or tablet, would that change things? It is reported that 74% of lawyers use a personal smartphone to check their email or do a simple legal task.[67] While many lawyers are using their own mobile devices for legal related work, it is worrisome that the offices they work for may not have clear BYOD guidelines and polices in place regarding the use of these personal devices.

Bring-Your-Own-Device or BYOD, is an approach that permits access to a company's computer network and email system through employee owned mobile devices.[68] It is estimated that more than half of all employees use their personal mobile technology for work.[69] While 90% of lawyers reported using remote access to check items such as their email in the *2018 ABA Technology Report*, only about 21% reported that their firm had a BYOD policy.[70]

---

[66] *Id.*
[67] Aaron Street, *ABA TECHREPORT: Mobile Technology*, at 1(2016) (available at https://www.americanbar.org/groups/law_practice/publications/techreport/)
[68] Steven M. Puiszis, *Can't live with them, Can't Live without them – ethical and risk management issues for law firms that develop a BYOD approach to mobile technology,* at 1 (2015) (available at: http://www.americanbar.org/content/dam/aba/events/professional_responsibility/2015/May/Conference/Materials/can't_live_with_them_cant_live_without_them.authcheckdam.pdf).
[69] Rachel King, *Forrester: 53% of Employees Use Their Own Devices for Work*, ZDNet (2012) (available at: http://www.zdnet.com/article/forrester-53-of-employees-use-their-own-devicesfor-work/#!).
[70] Ries, *supra* note 30, at §3.

Because the use of personal devices presents several risks, law firms should consider having clear BYOD policies if employees will be allowed to use their personal devices to access firm data. The policy should address:

- The risks associated with the use of mobile technology and security measures that need to be in place.
- What devices are permitted, and who is permitted to use them.
- The employee's responsibilities and the firm's responsibilities.
- The appropriate use of the mobile device, and be sure to clearly spell out that access to the firm's network is conditioned upon full and continuing compliance with the firm's data security policy.
- The right to access the firms' network will be immediately terminated if the policy is violated and upon the resignation, retirement or termination.
- If a violation of the policy occurs, what discipline can be imposed.[71]

Another thing to keep in mind is that laptop computers and items such as portable flash drives or external hard drives present risks as well. While the security controls may be different, and stronger than what is available on mobile devices, they still present the risk of being lost or stolen. Technical safeguards such as hard drive encryption, locking down the browser, the use of strong passwords, remote wiping, and other safety measures for laptops should be addressed with employees. Encrypting flash drives and hard drives should also be addressed.

Working Remotely/Virtually

ABA Opinion 498

When assessing the ethical obligations associated with the remote work environment or virtual practice, KRPC 1.1 Competence, 1.6 Confidentiality, and 5.3 Non-Lawyer Assistance are critical to determining one's obligations. KRPC 1.2 Diligence and 1.4 Communication are also relevant.

[71] Puiszis, *supra* note 45, at 38-40.

On March 10, 2021, the American Bar Association issued Formal Ethics Opinion 498 addressing the ethical obligations of lawyer practicing in a virtual practice. This opinion was in direct response to the number of lawyers making the switch to a remote practice as a result of the COVID-19 Pandemic. The opinions states,

> When practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies.[72]

The opinion also highlights a key comment to the Model Rule on competence, pointing out that in Comment [8], the rule states, "To maintain the requisite knowledge and skill [to be competent], a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…" As a result, should a lawyer practice virtually, he or she must be competent with their use of technology chosen to operate the virtual practice. Additionally, the opinion points to the Model Rule on confidentiality—which should be considered alongside Rule 1.1—stating that lawyers have the duty to, ""make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." These rules should be viewed in connection with one another given their bi-directional relationship. For example, if you are competent with chosen technology, you should be familiar with the risks and therefore will be able to access what precautions you need to protect the confidentiality and prevent inadvertent disclosure.

[72] American Bar Association Formal Opinion 498 at 2. (March 2021). The full opinion can be found here: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf

In a virtual practice, the opinion explicitly states that the lawyer should have plans in place to ensure responsibilities regarding communication and diligence. This duty is no different than in a brick and mortar practice. The way we fulfill this duty might just look a little different. The opinion highlights that Comment [1] to Rule 1.3 it makes clear that lawyers must also "pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor," and that Rule 1.4 requires that a lawyer, "…keep the client reasonably informed about the status of the matter; [and] promptly comply with reasonable requests for information. . . ."

Lastly, if the lawyer has any staff working for him or her in the virtual environment, supervision of the staff is still essential. Lawyers with managerial authority have ethical obligations, per Rule 5.3, to establish policies and procedures to ensure compliance with the ethics rules, and supervisory lawyers have a duty to make reasonable efforts to ensure that subordinate lawyers and nonlawyer assistants comply with the applicable Rules of Professional Conduct. These obligations do not change in the virtual environment. Instead, the way we meet these obligations just might look different than what we are used to seeing in the traditional brick and mortar office.

Staff Training

When it comes to your responsibilities as a lawyer, it is important that you remember to train to your staff in the areas of technology and security. Law firms can have advanced technological safeguards, but if the lawyers and staff in the firm don't know how to use the firm's technology, then those safeguards are worthless. As a result, technology and data security training is a key component.[73]

It is also important to remember that, KRPC 5.1 imposes supervisor obligations on partners or lawyers with managerial authority to ensure the firm has effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.[74]

[73] Puiszis, *supra* note 45, at 28-29.
[74] *See*, KRCP 1.5(a).

This requires lawyers with managerial authority to make reasonable efforts to establish internal policies and procedures.[75] Additionally, KRPC 5.3 takes a similar approach with non-lawyers who are employed, retained or associated with a lawyer or firm. The rule states, "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."[76] Nonlawyers who work for the firm should also understand the need to preserve confidentiality.[77]

When it comes to electronic communication, ABA Formal Opinion 477 suggests that lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communication with clients.[78] Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications.[79]

CONCLUSION

Together, the technology amendments to Rules 1.1 and 1.6 require law offices using technology to take competent and reasonable measures to safeguard client information. This duty extends to use of all technology, including desktop and laptop computers, mobile devices, network servers, cloud computing, and outsourcing. By applying common sense and remembering that the rules do not cease to apply simply because technology is involved, law offices can tackle the challenges of practicing law in the 21st Century with confidence.

[75] *See*, KRPC 1.5 [Cmt. 2].
[76] *See*, KRPC 5.3(b).
[77] Puiszis, *supra* note 59, at 28-29.
[78] ABA Formal Opinion 477, at 8 (2017).
[79] *Id.*