UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

68th Annual Taxation Conference

December 2-3, 2020
Live Webcast

Ethical Issues When Working Remotely (or did Alexa just waive privilege?)

Abbey B. Garber
Michelle M. Kwon

Authors Contact Information:
Abbey B. Garber
Thompson & Knight LLP
Dallas, Texas

Michelle M. Kwon
University of Tennessee
Knoxville, Tennessee

68th Annual Taxation Conference
Ethical Issues When Working Remotely (or did Alexa just waive privilege?)

A. INTRODUCTION

In a nationwide survey of lawyers conducted at the beginning of April, almost 90% of respondents reported that their offices were operating remotely in full or at least in part due to the COVID-19 pandemic.[1] By June, the percentage of firms surveyed who were working remotely in part or fully had dropped to 56%.[2] The 34% decrease in remote operations is likely the result, at least in part, of relaxed or expired state and local stay-at-home orders.[3] Despite this decrease, it is foreseeable that some number of lawyers will continue to work remotely, perhaps due to health concerns or to increasing responsibilities that ensued in the wake of the pandemic such as educating and caring for children and others at home. Even lawyers unburdened by those kinds of responsibilities might prefer to continue to work remotely due to the flexibility that remote working allows.[4] Many are predicting that the legal industry will continue to work remotely in some fashion even when the pandemic is over rather than reverting to the traditional brick-and-mortar practice of law.[5]

How does this "new normal" impact lawyers' ethical obligations to their clients? The easy answer is that the rules of professional conduct continue to apply despite the pandemic.[6] Nonetheless, it is worth reexamining several ethical duties that are implicated when practicing law remotely. This article considers the following ethical duties:

---

[1] Martin Cogburn, *How Law Firms are Responding to Covid-19-Remote Work*, https://www.mycase.com/blog/2020/04/survey-results-how-law-firms-are-responding-to-covid-19-remote-work/. The survey was conducted from April 8-10, 2020, and involved 819 respondents.

[2] Martin Cogburn, *How Law Firms are Adapting to New Normal of COVID-19 – State of Office and Challen*ges, https://www.mycase.com/blog/2020/07/new-survey-results-how-law-firms-are-adapting-to-new-normal-of-covid-19-state-of-office-challenges/.

[3] *Id*.

[4] *See*, *e.g.*, *2019 Millennial Attorney Survey, New Expectations, Evolving Beliefs and Shifting Career Goals*, https://cdn2.hubspot.net/hubfs/209075/MLA_MillenialSurvey_040519_forWeb-1.pdf?__hstc=51254006.713226280951a037a37ce402169ad1bc.1604758029585.1604758029585.1604758029585.1&__hssc=51254006.1.1604758029585&__hsfp=176983327. This Above the Law survey of over 1,200 respondents indicates that 75% of millennial lawyers would prefer a more flexible work schedule to more pay.

[5] *See*, *e.g.*, Law360, *New Normal of Legal Telework Likely to Outlast Pandemic* (July 24, 2020), https://www.law360.com/articles/1295207/new-normal-of-legal-telework-likely-to-outlast-pandemic; Bloomberg Law, *Analysis: The New Normal-Law Firms May Never be the Same* (May 7, 2020), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-the-new-normal-law-firms-may-never-be-the-same; David Lawson, *The Coronavirus Pandemic Could Mark the Dawn of the Virtual Office Revolution in the Legal Industry*, ABA Journal (Apr. 2, 2020), https://www.americanbar.org/groups/business_law/publications/blt/2020/04/virtual-office-revolution/.

[6] *See*, *e.g.*, ABA Formal Opinion 482 (2018) (the rules of professional conduct continue to apply despite a natural disaster). Numerous state bars have issued ethics opinions and other guidance in response to COVID-19. *See*, *e.g.*, PA Formal Opinion 2020-300, *Ethical Obligations for Lawyers Working Remotely* (Apr. 10, 2020), http://www.pabar.org/site/Portals/0/Ethics%20Opinions/Formal/F2020-300.pdf?ver=2020-04-21-111114-117; NYSBA, *Cybersecurity Alert: Tips for Working Securely While Working Remotely* (Mar. 12, 2020), https://nysba.org/app/uploads/2020/03/NYSBA-Cyber-Alert-031220.pdf.

- Competence and diligent representation (Rule 1.01)[7]
- Communication (Rule 1.03)
- Confidentiality (Rule 1.05)
- Remote supervision of junior lawyers and non-lawyers (Rules 5.01 and 5.03)

The discussion that follows may need to be tailored depending on the type and size of your law practice.[8] For example, large law firms presumably are better resourced as compared to solo practitioners and smaller firms, and thus, larger firms might be expected to implement more sophisticated security measures. There also may be special considerations for in-house legal departments and government lawyers. Moreover, the sensitivity of data that must be protected surely will vary depending on the type of practice. Also, keep in mind that a distinction should be made between what is minimally required to satisfy your ethical obligations as opposed to what are best practices.

B. RULE 1.01: COMPETENT AND DILIGENT REPRESENTATION

It goes without saying that lawyers must possess the requisite legal knowledge, skill, and training to fulfill their ethical obligations to their clients. This obligation is expressed in Rule 1.01(a), which provides in relevant part that "A lawyer shall not accept or continue employment in a legal matter which the lawyer knows or should know is beyond the lawyer's competence."[9] When COVID-19 hit the United States and quickly began spreading, countless lawyers had to pivot their practices. For some, it was keeping up with evolving court and agency closures. For many others, the pandemic has undoubtedly uncovered novel legal issues in areas such as employment law and health law, as well as a host of contracts issues. Still other lawyers have had to study and investigate laws that have been enacted in response to COVID-19 such as the Payroll Protection Program and the economic impact payments made by the Treasury Department to individuals earlier this year.[10] The comments to Rule 1.01 make clear that lawyers can agree to a representation without having the requisite legal knowledge so long they can become competent through study and investigation.[11]

In 2019, the duty of competence applicable to Texas lawyers was expanded beyond substantive competence to include technological competence.[12] No disciplinary action may arise for being technologically incompetent because only the comments were

---

[7] Unless otherwise stated, references to Rules are to the Texas Disciplinary Rules of Professional Conduct.
[8] *See generally* ABA CYBERSECURITY LEGAL TASK FORCE, THE ABA CYBERSECURITY HANDBOOK (2d ed. 2018) (discussing cybersecurity in the context of different legal practice settings, including large and small firms, in-house counsel, government lawyers, and public interest attorneys).
[9] "Competence" refers to the "possession of legal knowledge, skill, and training reasonably necessary for the representation." Rule 1.01, cmt. 1, referring to Terminology section in the Preamble to the Rules.
[10] Coronavirus Aid, Relief, and Economic Security Act, P.L. 116-136, 3/27/2020.
[11] Rule 1.01, cmt. 4.
[12] Rule 1.01, cmt. 8 (lawyers should "strive to become and remain proficient and competent in the practice of law, *including the benefits and risks associated with relevant technology*") (emphasis added). This 2019 change substantially follows a 2012 change to the ABA's Model Rule regarding competence, which provides: "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*." ABA Model Rule of Professional Conduct 1.1, cmt. 8 (emphasis added).

amended, as opposed to the competency rule itself.[13] Nonetheless, the practice of law in a remote environment is inextricably reliant on technology. It would be difficult to competently represent clients without the ability to navigate video conferencing platforms, to access email communications and documents remotely, to electronically file documents with courts, and to remotely appear for hearings. Ideally, lawyers would receive adequate training on new technologies being deployed. Ongoing support to navigate technological challenges would also be desirable, particularly for lawyers who are less technologically proficient. Additionally, it would be helpful to ensure that support staff are able to provide seamless service to attorneys even while they are physically separated, particularly for those lawyers who heavily relied on support staff while working in the brick-and-mortar office.

C. Rule 1.03: Communication

Rule 1.03(a) requires a lawyer to "keep a client reasonably informed about the status of a matter and promptly comply with reasonable requests for information." Furthermore, lawyers need to handle client matters with reasonable diligence and promptness.[14] Obvious issues that should be addressed to ensure prompt and effective communication with clients while working remotely include: (1) procedures for the intake and delivery of physical mail; (2) ensuring the prompt receipt of voicemails; (3) protocols for communicating with clients; and (4) tools for keeping abreast of deadlines.

Physical mail - Physical mail that is delivered to the brick-and-mortar law office should promptly either be physically delivered to addressees or scanned and electronically delivered.

Voicemail - To ensure lawyers promptly receive voicemails, one simple approach is to establish a policy that establishes the frequency with which lawyers are expected to remotely check their voicemails. Work-from-home frictions can be reduced by automating the process. One simple way is for lawyers to forward their work phones to another phone at their remote location. Alternatively, a law firm might have the functionality to send email notifications of voicemails or convert voicemails to audio files and send them by email. The recipient is then able to access voicemails from their email account and listen to voicemails by a simple click of the audio file.

Staying connected to clients – Clients should understand the best ways and times to get in touch with their attorneys. Thought should also be given to the best mode of communication given the nature of the relationship between the lawyer and client as well as the information being conveyed. For example, it might be more challenging to develop and maintain rapport in a virtual environment where cues such as body language that help us adjust our communication style are lacking. Particularly for prospective clients and new clients, communicating via video call to at least simulate an in-person meeting may be beneficial. If given the choice, even long-standing clients with whom you have an

[13] TRPC, Preamble: Scope ¶ 10.

[14] Rule 1.01(b)(1) ("In representing a client, a lawyer shall not neglect a legal matter entrusted to the lawyer.").

established rapport may prefer face-to-face communications, even if only in two dimensions on a screen, instead of conversations over text or email. Similarly, more face-to-face client contact might be desired in a family law or immigration law practice where emotions might run high, while clients with real estate or business matters might be less inclined to face-to-face interaction. The available information indicates that the majority of lawyers pivoted to video conferencing in response to COVID-19.[15] If employing videoconferencing, be sure to be familiar with the platform to minimize technical difficulties. When choosing the appropriate mode of communication, attention must be given to minimizing the risk of inadvertently disclosing client confidences or otherwise sensitive information. The issue of confidentiality is discussed further in the next section.

D. Rule 1.05: Client Confidentiality

Comprehensive data protection legislation is lacking at the federal level, and only a minority of states have wide-ranging data privacy laws.[16] Despite the lack of comprehensive data privacy laws, a patchwork of laws apply to particular industries. One relevant example is the Federal Trade Commission's Safeguards Rule, which requires tax return preparers to create and enact security plans to protect client data.[17]

In addition to statutory data privacy laws, lawyers have an ethical obligation—perhaps the most sacrosanct of all the ethical obligations—to safeguard confidential and privileged client information, including work product. This protection extends not only to information protected by the attorney-client privilege, but also to "all information relating to a client or furnished by the client . . . acquired by the lawyer during the . . . representation of the client."[18] Texas-licensed lawyers may be disciplined for "knowingly reveal[ing] confidential information of a client or a former client" to unauthorized persons.[19] The knowledge qualifier is not limited to actual knowledge. A lawyer's knowledge may also be "inferred from circumstances."[20]

There are at least three challenges in the virtual law office setting that implicate the duty of confidentiality. The first is cyberthreats due to the digital transmission and storage of client information. The second set of challenges relates to risks associated with employees' remote workspaces. The third is the risk associated with lawyers using their own personal devices to access firm email and networks.

---

[15] Celia Colista, *How Attorneys are Coping in the Pandemic* (June 9, 2020), https://www.martindale-avvo.com/blog/how-attorneys-are-coping-in-the-pandemic/ (80% of survey respondents deployed video conferencing after COVID-19 hit).

[16] *See* Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, https://iapp.org/resources/article/state-comparison-table/ (as of October 14, 2020, only California, Maine, and Nevada have comprehensive privacy laws). Section 521.052 of the Texas Business and Commerce Code requires businesses to "implement and maintain reasonable procedures" to protect the disclosure of "sensitive personal information," which includes social security numbers and financial account information.

[17] *See* IRS Publication 4557, Safeguarding Taxpayer Data.

[18] Rule 1.05(a).

[19] Rule 1.05(b)(1).

[20] TRPC, Terminology.

1. Cyberthreats and Confidentiality

Law firms are attractive to cyberthieves for two reasons. First, law firms maintain what cyberthieves see as lucrative client data, such as intellectual property, trade secrets, financial data, and business and litigation strategies.[21] Consider the following examples:

- Three individuals were indicted in 2016 for insider trader for allegedly stealing confidential information from prominent international law firms engaged in corporate mergers and acquisitions.[22]
- Seyfarth Shaw LLP was the subject of a ransomware attack in October 2020.[23]
- Earlier this year, a New York City entertainment law firm whose clients include numerous high-profile celebrities became the target of a ransomware attack. After the firm rebuffed a $21 million ransom demand, the attackers leaked stolen data about Lady Gaga, one of the firm's clients.[24]
- Perhaps the most well-known law firm hack was of the former Panama-based law firm Mossack Fonseca in 2016.[25] The hack resulted in the leak of the so-called Panama Papers, which resulted in the disclosure of confidential information of "hundreds of thousands of individuals and entities."[26] Mossack Fonseca's outdated technology and lax computer security likely contributed to the hack.[27]
- Closer to home, several Texas firms and national firms with Texas offices were reportedly being targeted by hackers back in 2016.[28]

---

[21] *See* Nathan Powell, *Electronic Ethics: Lawyers' Ethical Obligations in a Cyber Practice*, 29 GEORGETOWN J. LEG. ETHICS 1237, 1238 (2016). *See also Large Law Firms' Secret Information From Big-Money Clients Entice Cyberthieves*, ABA J. (Jan. 2018), https://www.abajournal.com/magazine/article/large_law_firms_cybertheft_risk/P1

[22] U.S. ATTORNEY'S OFFICE FOR THE SOUTHERN DISTRICT OF NEW YORK PRESS RELEASE, *Manhattan U.S. Attorney Announces Arrest of Macau Resident and Unsealing of Charges Against Three Individuals For Insider Trading Based on Information Hacked From Prominent U.S. Law Firms* (Dec. 27, 2016), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-arrest-macau-resident-and-unsealing-charges-against.

[23] Xiumei Dong, *Seyfarth Cyberattack Spotlights Gaps in Law Firm Security*, Law360 (Oct. 15, 2020), https://www.law360.com/articles/1319407/seyfarth-cyberattack-spotlights-gaps-in-law-firm-security.

[24] Kathryn Rubino, *Lady Gaga Documents Leaked After Law Firm Was Hacked*, Above the Law (May 18, 2020), https://abovethelaw.com/2020/05/lady-gaga-documents-leaked-after-law-firm-was-hacked/.

[25] *See*, *e.g.*, Luke Harding, *What are the Panama Papers? A Guide to History's Biggest Data Le*ak, The Guardian (Apr. 5, 2016), https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers. Mossack Fonseca ceased its operations in 2018. Jaclyn Jaeger, *Mossack Fonseca Closing its Doors*, Compliance Week (Mar. 19, 2018), https://www.complianceweek.com/mossack-fonseca-closing-its-doors/8635.article.

[26] Victor L. Hou et al., *Cleary Gottlieb Discusses U.S. Criminal Prosecutions Based on Panama Papers Hack*, The CLS Blue Sky Blog (Jan. 29, 2019), https://clsbluesky.law.columbia.edu/2019/01/29/cleary-gottlieb-discusses-u-s-criminal-prosecutions-based-on-panama-papers-hack/.

[27] *See* James Temperton and Matt Burgess, *The Security Flaws at the Heart of the Panama Papers*, Wired (Apr. 6, 2016), https://www.wired.co.uk/article/panama-papers-mossack-fonseca-website-security-problems. One expert described the law firm as "caught in a time warp."

[28] John G. Browning, *Why Cybercriminals are Targeting Law Firms*, D Magazine (Aug. 2016), https://www.dmagazine.com/publications/d-ceo/2016/july-august/cybercrime-targets-law-firms/.

These examples barely scratch the surface. ABA survey data from 2018 estimates that about one of every four firms has experienced a data security breach.[29] The risk seems to be somewhat correlated to firm size. In particular, 14% of solo practitioners reported a breach as compared to 42% of firms with 50-99 lawyers and 31% of firms with 100 or more lawyers.[30] In 2020, the number of firms who experienced a data security breach increased to about one in every three firms.[31]

Beyond the valuable information that law firms possess, the second reason that law firms are attractive to cyberthieves is because hackers perceive law firms to be easy targets. The legal industry generally does not have a reputation for being technologically savvy.[32] A cyber security expert paints this picture: "Look at the back seat of the car of the average partner's BMW and I think you'd be quite shocked. These guys still take large bundles of papers around tied up with ribbons."[33] Objectively, there is some truth in this observation.

Failing to prioritize cybersecurity is risky given the work-from-home environment. "Nearly ubiquitous connectivity generates nearly ubiquitous vulnerability." Although this quote comes from a 2011 law review article, it aptly describes the state of affairs in the remote work environment brought on by the pandemic.[34] The rise in the number of employees working from home creates more opportunities for hackers to attack. One telling data point to consider: a leading cyber insurer reported that the frequency of ransomware attacks rose 260% in the first six months of 2020.[35] Given the increased vulnerability, it is imperative for law firms to take reasonable efforts to protect confidential information.[36]

Despite the obvious risk of cyber attack and the ethical obligations to protect client information, firms remain vulnerable. The ABA surveyed attorneys in private practice in law firms of all sizes between March and May of 2020—*i.e.*, while the country was in the early stages of dealing with the pandemic.[37] The following chart shows the percentage of survey respondents who have adopted each of the technologies:

Technology	Percentage of users
File encryption	43%

[29] David G. Ries, *2018 Cybersecurity*, ABA TechReport 2018 (Jan. 28, 2019), https://www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cybersecurity/.
[30] *Id.*
[31] John G. Loughnane, 2020 Cybersecurity, ABA TechReport 2020 (Oct. 19, 2020), https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/.
[32] *See e.g.*, Frank Ready, *Businesses Want Outside Counsel to be More Tech Savvy. What Does That Mean?*, NY L. J. (July 14, 2020) ("It's no secret that law firms in general remain behind the curve when it comes to incorporating new technology into their services.").
[33] *See* Temperton & Burgess, *supra* note 27 (quoting Dr. Daniel Dresner).
[34] Roland L. Trope & Sarah Jayne Hughes, *Red Skies in the Morning – Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 118 (2011).
[35] Dong, *supra* note 23.
[36] *See* Texas Ethics Op. No. 648 ("Since a 'knowing' disclosure can be based on actual knowledge or can be inferred, each lawyer must decide whether he or she has a reasonable expectation that the confidential character of the information will be maintained if the lawyer transmits the information by email.").
[37] Loughnane, *supra* note 31.

Email encryption	39%
Two-factor authentication	39%
Intrusion prevention	29%
Intrusion detection	29%
Remote device management and wiping	28%
Device recovery	27%
Web filtering	26%
Employee monitoring	23%
Biometric login	12%

Even before the pandemic struck the U.S. at the beginning of this year, the Professional Ethics Committee of the Texas State Bar had addressed the use of technology to transmit and store confidential information. Texas Ethics Opinion 648 (Apr. 2015) made clear that lawyers generally may use unencrypted email to communicate confidential information while also recognizing that the circumstances may justify communicating by other means. Texas Ethics Opinion 665 (Dec. 2016) discussed lawyers' role in mitigating and preventing the inadvertent transmission of metadata.[38] More recently, Texas Ethics Opinion 680 (Sept. 2018) concluded that lawyers may store confidential information and other data on the cloud if reasonable precautions are followed.[39]

To better protect confidential client information, the ABA, in its 2020 TechReport[40] recommends the following actions:

- Strengthen passwords
- Enable multi-factor authentication
- Fortify your network
- Secure your network administrator
- Enforce wi-fi authentication
- Limit guest access
- Protect internet systems[41]

[38] In simple terms, metadata is data that is automatically created by computers and embedded into computer-generated documents.

[39] Texas Ethics Opinion No. 680 (Sept. 2018). The cloud is a virtual storage space on the internet that allows employees, without regard to their physical location, to access digital resources like documents.

[40] Bryan Lieber, Law Firm Guide to Cybersecurity (Oct. 22, 2020).

[41] Individuals should review their own personal router settings to take the following steps to protect clients' information: (1) Make sure you have changed the device's default administrative (internal) password to one that is unique to you *and* (2) set a strong unique WiFi password (phrases are good) of 15 characters. (3) Change the name of the WiFi network (its SSID)—if you use the manufacturer's default you have effectively established your network as if it were public WiFi). In addition, (4) make sure that the router is using the latest encryption standard (preferably WPA2). (You should be able to find the various manufacturer settings by going to the manufacturer's website.) Anthony E. Davis and Janis M. Meyer, Rising to the Ethical Challenges of Remote Working, New York Law Journal (May 01, 2020), https://www.law.com/newyorklawjournal/2020/05/01/rising-to-the-ethical-challenges-of-remote-working/

The adage that "the best defense is a good offense" seems fitting during these pandemic times. Importantly though, the ethical duty of confidentiality does not require a foolproof system to prevent the unauthorized disclosure of confidential client information.[42] Eliminating all cybersecurity risks might not be possible, and in any event, is not practical. What is required is that lawyers undertake reasonable efforts in light of the circumstances.[43] An audit of the current technology might be warranted to determine whether existing data security efforts are reasonable in light of the now ubiquitous work-from-home environment.[44] Consideration should be given to the transmission and storage of sensitive client information such as financial information, social security numbers, bank account information, confidential deal information, and litigation strategies. Because technology is constantly evolving, lawyers must continuously reassess the risks associated with the technologies relied on.

2. Risk of Inadvertent Disclosures Due to Working From Home

As discussed in the last section, technology can help manage the risk of data breaches. But "frequently the weakest link in the security of a law firm is its personnel."[45] This section describes some of the steps that can be taken to manage the risk of data breaches due to working from home.

There is no friends-and-family exception to a lawyer's duty of confidentiality. This maxim was true in a bricks-and-mortar law practice and remains true in the virtual law office environment. Thus, lawyers have always had to resist the temptation to gossip about their clients. The difference now is that the risk of inadvertent disclosure of client information potentially is greater when lawyers are sharing a home workspace. The threat of this risk looms large because attorney-client privilege may be destroyed when otherwise confidential communications take place in the presence of a third party.[46] As noted above, even if the information is not subject to the attorney-client privilege, Rule 1.05 covers "all information . . . acquired by the lawyer during the course of or by reason of the representation of the client."[47]

Remote workspaces should be designed to minimize the inadvertent disclosure of client confidences to unauthorized persons such as members of the lawyer's household,

---

[42] *See* ABA Model Rule 1.6(c), cmt. 18 ("Factors to be considered in determining the reasonableness of the lawyer's efforts include . . . 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").

[43] *See* Rule 1.05(a) ("knowing" violations of confidentiality rule are prohibited) and TRPC, Terminology (defining "knowing" to include inferred knowledge). *See also* ABA Model Rule 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."). See also ABA Opinion 477R (2017).

[44] *See* Texas Ethics Opinion Rule No. 648 (acknowledging that an evaluation of "email technology and practices should be ongoing as there may be changes in the risk of interception of email communications over time that would indicate that certain or perhaps all communications should be sent by other means.").

[45] Steven M. Puiszis, *Can't Live With them, Can't Live Without Them: Ethical and Risk Management Issues for Law Firms that Adopt a "BYOD" Approach to Mobile Technology*, 2015 PROF. LAW. 33, 38 (2015).

[46] *See* Tex. R. Evid. 503; *In re Small*, 346 S.W.3d 657, 663 (Tex. Ct. App. 2009).

[47] Rule 1.05(a).

household staff, and guests. Lawyers should not carry on telephone or video calls within earshot of such persons. The use of headsets can also help to prevent others from hearing those conversations.

Some commentators suggest not recording or allowing others to record video calls.[48] The caution against recording is to prevent the intentional or inadvertent distribution of the digital file. As aptly stated at a recent State Bar Texas CLE, "lawyers should be very wary of recording any attorney-client conversation because you risk the exposure of privileged information."[49] Also, consider whether any benefits of sharing documents over video conferencing platforms such as Zoom outweigh any potential risks. To maintain control over such things as the ability to record or share screens, lawyers should insist on hosting video calls.[50]

Commentators recommend turning off or muting Alexa, Echo, and similar digital virtual assistants.[51] These devices are standing by ready to record your voice commands and the companies providing these services collect and digitally store that data.[52] There have also been reports of these devices inadvertently recording conversations.[53] Confidentiality concerns arise if an unauthorized person obtains access to client information recorded in that manner. There have also been instances where this kind of data stored from internet-connected devices might be obtained in connection with an investigation of some kind or used as evidence in court.[54]

Attention should also be given to the physical workspace. Ideally, the lawyer should have a separate physical working space that can be locked. If this is not possible, be careful to restrict access to computers and other digital devices with strong passwords and secure any physical files and documents. Employees should also understand how to properly dispose of physical documents containing confidential information.

Given the portability of our work, caution must be exercised when lawyers are working in public places such as coffee shops within earshot or eyeshot of others. Moreover, refrain from using public Wi-Fi because in most cases public Wi-Fi is not secure.[55] Joining the internet using the coffee shop's network is more secure if you use a virtual private network

---

[48] Nichole Bunker-Henderson and Cole Hutchison, Mark, Will you Keep my Client's Secret?, State Bar of Texas 32nd Annual TXCLE Advanced Admin. L. (2020).
[49] *Id.*
[50] *Id.*
[51] *See*, *e.g.*, Crystal Tse and Jonathan Browning, *Locked-Down Lawyers Warned Alexa is Hearing Confidential Calls*, Bloomberg (Mar. 20, 2020), https://www.bloomberg.com/news/articles/2020-03-20/locked-down-lawyers-warned-alexa-is-hearing-confidential-calls
[52] Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You This Whole Time*, Wash. Post (May 6, 2019), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/.
[53] *See id.*
[54] Haley Sweetland Edwards, *Alexa Takes the Stand: Listening Devices Raise Privacy Issues*, Time (May 4, 2017).
[55] FED'L TRADE. COMM'N, *Tips for Using Public Wi-Fi Networks*, https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks.

(VPN).[56] A VPN adds security to a public Wi-Fi by encrypting data moving between your computer and the internet.[57]

Finally, anyone with access to confidential information should receive training on relevant data security policies and procedures and the importance of data security and client confidentiality should consistently be emphasized. Even with state-of-the-art technology, threats exists due to human error.[58]

3. Bring Your Own Device (BYOD) Risks

BYOD refers to employees' use of their own personal devices to access the firm's computer network, including the email system, documents, and other work product.[59] Twenty years ago, it was common for law firms to dole out firm-owned BlackBerrys.[60] In recent years, it has become more common for lawyers to use their personal phones to access work emails and their own tablets, laptops, or home computers to access the firm's network.[61] BYOD offers several advantages. First, law firms save money by not having to provide every lawyer one or more of these devices.[62] Firms also benefit from the potential for greater productivity of lawyers who have the flexibility to work from anywhere at any time.[63] Employees also benefit by not having to carry around and manage multiple devices. Moreover, the flexibility afforded to employees to work from anywhere perhaps leads to greater job satisfaction and better employee morale.

However, the benefits of BYOD are not risk-free. When employees work on client matters using firm-owned devices, the firm can ensure that the devices have the necessary tools to minimize the risk of cyberthreats. Firms can require strong passwords. Devices can be set to lock after a period of inactivity. Software can be used to help to protect data from hackers. Firms can prescribe the kinds of software and applications that can and cannot be used on firm-owned devices. But by allowing employees to use their own devices, firms forego some of that control, which opens the door to increased cybersecurity threats.[64] An unsecured or under-secured personal device can serve as a cyberthief's

---

[56] *Id.*
[57] *Id.*
[58] ABA CYBERSECURITY HANDBOOK 274, *supra* note 8 ("Countless studies, audit trails, and surveys over the years have repeatedly confirmed that the biggest data protection threats come from within one's own organization.").
[59] Puiszis, *supra* note 45, at 33.
[60] Anonymous Partner, *Biglaw's BlackBerry Bye-Bye*, ABOVE THE LAW (Sept. 10, 2013), https://abovethelaw.com/2013/09/biglaws-blackberry-bye-bye/.
[61] The Sedona Conference Data Privacy Primer, 19 SEDONA CONF. J. 273, 425 (2018).
[62] *See id.*
[63] *See id.* A survey in March 2020 indicated that 63% of employers worried about a decline in worker productivity due to remote working. By June, that concern decreased decreased significantly to 26%. *PwC US CFO Pulse Survey* (June 15, 2020), https://www.pwc.com/us/en/library/covid-19/pwc-covid-19-cfo-pulse-survey.html#challenges. See also Andrew Maloney, *COVID-19 is Driving Long-Term Changes in Big Law for Remote Work, Fees, Hiring* (Oct. 5, 2020), https://www.law.com/americanlawyer/2020/10/05/covid-19-is-driving-long-term-changes-in-big-law-for-remote-work-fees-hiring/ (reporting that the Seattle office of Davis Wright Tremaine's client service levels post-COVID are comparable to pre-COVID levels of productivity).
[64] *See*, *e.g.*, Puiszis, *supra* note 45, at 34 ("Owners of BYOD devices frequently download software they prefer to use when working remotely and applications for their personal use during off hours. Thus, BYOD

entry point to the firm's computer network. Additional risks are generated if employees download sensitive or confidential information onto their unsecured or under-secured personal devices or their otherwise adequately secured personal device that is lost or stolen. There are also risks if an employee stores client data using an unapproved cloud service such as Dropbox.

The safest bet is to prohibit the use of employee-owned devices. But to the extent that the proverbial horse is out of the barn, a complete ban is no longer practical. If you decide to permit personal devices to access firm or client data, it might be beneficial for employees to identify devices that employees are working on from home. Some firms might find it desirable to limit the kinds of devices that may be used for firm business.

Firms that permit personal devices to access firm or client data should have a BYOD policy.[65] Such a policy, assuming it is understood by employees and enforced, can give firms the ability to exercise control over non-firm owned devices that will interface with the firm's computer network or email system. A BYOD policy could include provisions such as: password requirements, the requirement for the device to automatically lock after a period of inactivity, restricting use by others of any personal device to be used for firm business, the requirement for the device to be locked remotely if it is lost or stolen, and mandated encryption and antivirus software. The policy could also prohibit employees from storing any firm or client information to a non-approved cloud or to their personal devices. Mobile device management software can be used to implement and manage these tasks.

A BYOD policy should also describe what happens to firm-owned or client-owned data on personally owned devices when employment is terminated.[66] Firms could obtain employees' consent to submit their personal devices to the firm to allow any such data to be identified and removed. It is also possible to remotely erase data from a device, oftentimes using software that is already on the device. In some cases, it may be possible to wipe only work accounts instead of all data. For example, if an employee has both a personal Google account and a work account, the employer might be able to delete only the data associated with the work account.

These kinds of BYOD policies create a tension with an employee's expectations of privacy. After all, the devices we are talking about are owned by the employee, not the firm. How much access should an employer have to employees' personally owned devices to enforce the firm's BYOD policy? To what extent should an employer be able to access employees' personal information on their personally owned devices and for what purpose? Monitoring employees' personally owned devices and removing data from them might

---

inevitably brings with it BYOS ('Bring Your Own Software') and BYOA ('Bring Your Own Applications') because of their popularity and ease of use. Frequently, this software is cloud-based, which means BYOD often also frequently results in BYOC ('Bring Your Own Cloud').").

[65] Sample BYOD policies are included in Puiszis's article (see *supra* note 45) and Powell's article, which is cited in *supra* note 21.

[66] Relatedly, procedures should exist to retrieve firm-owned devices and physical files and other property from employees when employment ceases. In cases of involuntary termination, it might make sense to get the devices prior to termination.

implicate privacy protection laws such as the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA).[67] In the interest of simplicity, the ECPA protects electronic communications while in transit while the SCA protects stored electronic communications.[68] But liability can be avoided by obtaining the employee's prior consent.[69]

E. RULES 5.01 AND 5.03: REMOTE SUPERVISION OF JUNIOR LAWYERS AND NONLAWYERS

Partners in law firms and those having direct supervisory authority over lawyers should take steps to ensure the quality of the legal advice that junior lawyers provide and the work product that junior lawyers produce.[70] Moreover, supervising lawyers should ensure that junior lawyers comply with the rules of professional conduct. Supervising lawyers also need to ensure that nonlawyers, such as legal assistants and secretarial staff, conduct themselves in a manner that is consistent with the rules of professional conduct.[71] Failing to appropriately supervise junior lawyers and nonlawyers could subject the supervising lawyer to discipline pursuant to Rules 5.01 and 5.03 of the Texas Disciplinary Rules of Professional Conduct.

Supervision and career development can be challenging when people do not share the same physical location. But there are steps that can be taken to ease some of the challenges. First, lawyers should be reminded that the pandemic does not relieve them from their ethical obligations. Second, supervising lawyers should become familiar with tools that are designed to enable communication. Popular examples include Slack and Microsoft Teams. Thoughtful consideration should be given to the right communication tool given what needs to be accomplished. Is an asynchronous mode such as an email or memo appropriate or would a synchronous mode such as a phone or video call better? For example, an email, chat, or text probably works fine for simple requests or tasks. A phone call can often be used to help clarify something or to clear up a misunderstanding. Complex matters though might justify a video call where the participants can see one another and documents or slides or a whiteboard can be shared remotely. Emotional or sensitive issues might also justify a synchronous mode of communication such as a video call.

---

[67] 18 U.S.C. § 2509 et. seq. (ECPA) and 18 U.S.C. § 2701-2711 (SCA). The federal district court for the southern district of Texas held that an employer had no liability under the ECPA after it remotely wiped all data from a former employee's iPhone—both company-owned and personal. *Rajaee v. Design Tech Homes, Ltd.*, No. H-13-2517, 2014 WL 5878477 (2014). The ex-employee used his iPhone to access his work calendar and emails. The court found that the statute was not intended to cover this kind of a circumstance. Even if courts might be narrowly interpreting these federal data protection statutes, employers would be wise to fully explain to employees the risks involved with remote wiping of devices.

[68] Michael Kelsheimer and Travis Crabtree, *Privacy Rights of Employees in an Electronic World*, 56 THE ADVOC. (TEXAS) 60, 63 (2011).

[69] *Id.* at 61-64.

[70] Rule 5.01. A partner or supervising lawyer is subject to discipline under Rule 5.01 if that person orders or knowingly permits a junior lawyer to violate the ethical rules or that person, knowing that a junior lawyer has violated the rules, fails to take remedial action.

[71] Rule 5.03(a). Lawyers can also be subject to discipline for ordering or encouraging nonlawyers to engage in conduct that would violate the ethical rules if the person were a lawyer or for failing to take remedial action after a knowing violation. Rule 5.03.

Expectations regarding deadlines, billable hours, work schedules, and similar matters should be clearly communicated. An important consideration is instituting ways to replicate office drop-ins among lawyers, particularly to give less experienced lawyers avenues to ask questions of, and seek advice from, more senior lawyers. Unique issues generated as a result of the pandemic should also be addressed. For example, do at-home distractions justify reducing billable hour loads? What impact does the pandemic have for lawyers on the partnership track? What support, financial and otherwise, will be provided to lawyers who become ill or become caretakers for someone who is ill?

Finally, the emotional toll of COVID-19 has been the subject of several recent studies.[72] Those studies document increased levels of stress, anxiety, burnout, and substance abuse.[73] Law firm partners and management should be sensitive to lawyers' emotional well-being. Not only is this the humane thing to do, but mental wellness could implicate a lawyer's competence and ability to provide effective representation. In addition to check-ins with colleagues, law firms should communicate to lawyers available mental health resources, such as employee assistance programs and mental health care.

[72] Rhitu Chatterjee, *Pandemic's Emotional Hammer Hits Hard*, NPR (Sept. 2, 2020).
[73] *Id.*