Cybersecurity and Practicing Remotely

Thomas A. Tietz, Esq. and Prof. S. Alan Medlin

Thomas A. Tietz is a partner at **Shenkman Tietz, LLP** practicing in New York and New Jersey. He has lectured for the New Jersey State Bar Association, New Jersey Institute of Continuing Legal Education, CPA Academy, the Financial and Estate Planning Council of Metropolitan Detroit, the Bergen County Estate Planning Council, the National Academy of Continuing Legal Education and numerous other institutions. He has published articles in many publications, including the American Bar Association E-Report, the National Association of Estate Planning Council's Journal of Estate and Tax Planning, Steve Leimberg's Estate Planning Newsletter, Wealthmanagement.com, and Trusts & Estates Magazine. He is a member of the American Bar Association, Real Property, Trust, and Estate Law section, the New York State Bar Association, the New Jersey State Bar Association, and the Bergen County Estate Planning Council. He can be reached at his email: Tietz@shenkmanlaw.com.

S. Alan Medlin is the David W. Robinson Professor of Law at the University of South Carolina School of Law. Since 1984, he has taught courses in Trusts and Estates, Fiduciary Administration, Property, Real Estate Finance, Real Estate Transactions I, Real Estate Transactions II, Professional Responsibility, Advanced Professional Responsibility, Fundamentals of Law Practice and Professionalism, Law Practice Workshop, Introduction to the Legal Profession, and Wills, Trusts and Estates. Since 1989, he has co-authored and co-edited, along with Professor Lad Boyle, Howard Zaritsky and Sam Donaldson, the Probate Practice Reporter, a monthly publication distributed nationally. He has served as editor-in-chief, resident editor, and associate editor of the American Bar Association's Real Property, Trust and Estate Journal, the scholarly journal of the ABA's Real Property, Trust and Estate section; he also served on the editorial board of Probate and Property magazine, the bi-monthly magazine of the ABA's Real Property, Trust and Estate section. He has authored or co-authored 5 books, several book chapters, and approximately 225 articles, and he has made over 200 presentations to regional and national audiences in the areas of legal ethics, estate planning, probate, and real estate law. He is an Academic Fellow of the American College of Trust and Estate Counsel and is a former chair of the Board Governing Certified Specialists in Estate Planning and Probate for South Carolina. Professor Medlin has been named Outstanding Law Faculty Teacher eight times. He is a recipient of the South Carolina Compleat Lawyer Award and is an honorary member of the South Carolina Association of Probate Judges. He is a former Chair of the Real Estate Practices Section of the South Carolina Bar. He has served as Reporter for the South Carolina Trust Code, the South Carolina Uniform Power of Attorney Act, and several revisions to the South Carolina Probate Code. He received the 2004 Treat Award recognizing excellence from the National College of Probate Judges. He is the 2021 recipient of the South Carolina Bar's Robert Wilkins Award.

TABLE OF CONTENTS

Contents

1. **Introductory Comments.**
    a. **Not suggesting a standard of practice**.
        i. This paper does not intend to imply that anything discussed is essential, or a standard of practice. Rather, the goal is to merely discuss points and practitioners might consider when managing their practice with a particular emphasis on evolving landscape of technology, the need for cybersecurity and some of the ethical issues they raise.[1]
    b. **Elder Financial Abuse Dwarfs Estate Tax**.
        i. During a one-year period ending in June 2023, U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) found $27 billion in reported suspicious activity that was linked to elder financial exploitation.[2] By comparison, approximately $24 billion was collected from the estate tax in 2023.[3] Contrast the attention given to estate tax minimization planning during the planning process versus that given to elder abuse, identity theft, and similar losses.
        ii. With an aging population, increasing concerns of elder financial abuse, and few taxpayers subject to estate taxation (and even less after the increase of the Federal estate tax exemption to $15 million for 2026 due to the One Big Beautiful Bill Act), the emphasis needs to evolve. Further, with document drafting software proliferating in the profession, and the likelihood of AI expanding the ease of use and sophistication of such programs, practitioners might benefit by offering broader estate planning guidance beyond document preparation. Broader advice might include ancillary matters like security and access to client financial, legal and other records health care navigation, etc. It is not uncommon for practitioners to discuss with clients their personal excess liability insurance policy (umbrella policy), who might be appropriate as a fiduciary, safeguards to put in place to monitor fiduciaries (e.g., a trust protector) and a range of other topics. One suggestion of this paper is that tech conversations and client cybersecurity at some point might be part of the conversation about security, asset protection and elder planning. If an attorney feels unqualified or unskilled to address these matters consider the ethical requirements to be reasonably informed about technology, cyber security and AI discussed below. The process of addressing ethical considerations may provide some foundation for the discussions with clients.
    c. **Retainer agreements should reflect technology and ethics concerns**.
        i. **Practice Suggestion**:
            1. Practitioners may consider periodically reviewing their retainer agreements (engagement letters) and updating them to reflect new ethics rules, changing practices, integration of new technology or cybersecurity measures into their practice, etc.
            2. The majority of states have adopted the ABA Model Rules of Professional Conduct ("RPC") changes from 2012 which relate to technology.
                a. RPC 1.1 was modified to require technical competence[4], including the addition of the following language to the Comments: "*[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…*"
                b. RPC 1.4: Communications discusses the attorneys' use of technology, it requires appropriate communications with clients "*about how the client's objectives are to be accomplished*,"

including how the practitioner employs technology in their practice. It requires keeping the client informed and, depending on the circumstances, may require obtaining "*informed consent.*" It requires sending notice to a client of a compromise of confidential information relating to the client.

c. RPC 1.6 requires lawyers to use “reasonable efforts” or “reasonable precautions” to prevent the inadvertent or unauthorized disclosure of confidential client data.
    i. It broadly requires protection of "*information relating to the representation of a client*;" it is not limited to confidential communications and privileged information. Disclosure of protected information generally requires express or implied client consent (in the absence of special circumstances, like misconduct by the client).
    ii. The 2012 amendments added the following new subsection to RPC 1.6:
        1. “*(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*.”
    iii. This requirement addresses two areas—inadvertent disclosure and unauthorized access. Inadvertent disclosure includes threats like leaving a briefcase, laptop or smartphone in a restaurant or hotel, sending a confidential e-mail to the wrong individual, producing privileged documents or data in litigation, or exposing confidential metadata. Unauthorized access includes threats like hackers, malicious actors, malware and insider threats.
    iv. The 2012 amendments also include additions to Comment [18] to RPC 1.6, providing that "reasonable efforts" require a risk-based analysis, considering 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 them, and the extent to which they would adversely affect the lawyer's ability to use the technology. The amendment also provides that a client may request the lawyer implement special security measures not required by the rule or may give informed consent to forgo security measures that would otherwise be required by the rule.
    v. Comment [19] to RPC 1.6 applies to electronic communications and requires "r*easonable precautions to prevent the information from coming into the hands of unintended recipients*." It provides:
        1. “*This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable*

expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement…

vi. What is a "reasonable precaution?" The language about "special security measures" might be viewed as meaning that attorneys never need to use special measures, like encryption. While it does state that "special security measures" are not generally required, it contains qualifications and notes that "special circumstances" may warrant "special precautions." It includes the important qualification – "*if the method of communication affords a reasonable expectation of privacy.*"

vii. What are reasonable efforts? This is a nebulous statement that needs both common sense applications, judgment, and to review what opinions consider reasonable to determine your technology policies moving forward.

viii. Reasonable efforts may be interpreted to include due diligence regarding technology procedures. Required training for employees, thoughtful policies implemented and followed, etc. all show that due diligence and that reasonable efforts were made to prevent disclosure.

d. One approach to the ethical duty of protecting electronic communications (discussed further below) is to have an express understanding with clients (such as in an engagement letter or other writing) about the nature of communications that will be (and will not be) sent electronically, and whether or not encryption and other security measures will be utilized.

ii. Practitioners should not ignore the changes technology and other developments are having for retainer agreements and other related practice management steps.

iii. Engaging in discussion with clients and providing information on the practitioner's cybersecurity measures to protect confidential data can help assuage concerns the client may have and allow the client to provide commentary on what uses of technology they are comfortable with. As each practitioner utilizes technology in unique ways, the engagement letter should be customized by the practitioner.

iv. **Sample Clause**: A sample provision for an engagement letter could include, "*You authorize the back-up and storage of records on cloud-based back up services, including but not limited to those provided by ShareFile, Microsoft 365, SugarSync, Datto and NetDocuments and others, posting PDFs of your documents in the cloud on ShareFile or a similar service, and emailing of unencrypted confidential records. If you wish us to use encrypted electronic communications, we can do so*."

d. **Great variability by practice**.
    i. The ideas presented must be adapted and modified for every practice. Every practice is unique in terms of the nature of the typical clients, the practitioner's comfort level with technology, capabilities of the administrative staff, etc.
    ii. A paperless, cloud-based practice will necessarily have different cybersecurity requirements than a practice that is paper based and employs other analog tools.
    iii. **Practice Suggestion**: Each practitioner has to find the cybersecurity road map that works for them. This depends upon the practitioner's style, how technologically savvy they are, what changes are appropriate for their practice, the timeframe for implementation of any changes and how you anticipate evolving. Many practitioners only reluctantly adopt a cybersecurity strategy. Implementing a cybersecurity measure and improperly using the technology may not provide the protection desired. Practitioners should research options to find what fits their style, is within their comfort zone and meets the security needs for their practice. Identify a logical sequence to approach the process, and steps that are small enough to be actionable without being overwhelming.

e. **Remote Work is Popular**.
    i. While there have been many reports in the media regarding the return to office trend, remote work continues to be popular, with 67% of companies surveyed stating they offer hybrid work options for their employees.[5] Remote or Hybrid work can enhance quality of life. For an attorney that commutes three hours daily into a major city, a day or two a week of remote work can provide considerable extra time that may reduce stress and pressure. For those with parenting responsibilities, remote work can bridge gaps in childcare and enhance parenting. For senior attorneys, remote work may facilitate extended periods of work from a beloved vacation home and perhaps even motivate someone who would have retired to continue to practice. For an attorney who practiced in a cold Northern city for decades, the option to practice part time for six months of the year from a condo in a warm Southern climate may make continuing to practice on a lesser basis their encore career. That can be good for the practitioner, the firm and clients. For those facing the challenges of disabilities or chronic illness, being able to work remotely may mean the difference between being able to work or not. For example, severe chronic fatigue is a symptom of many chronic diseases. Working from home can help the affected attorney conserve energy and permit rest when necessary. For many demographics of attorneys, working remotely can make life not just easier, but make working possible.
    ii. "*A …national survey sponsored by the American Bar Association shows most lawyers want the option to work from home…*"[6] Here are some other findings from the study:
        1. *"…remote options are especially important to young lawyers, 44% of whom said they would leave their jobs for a greater ability to work remotely*."
        2. "*The vast majority (87%) said their workplace allows lawyers to work remotely. About 30% of lawyers work from home almost all the time. Another 30% work in the office nearly 100% of the time*."
        3. "*Most lawyers reported that working remotely or on a hybrid basis has not adversely impacted the quality of their work, productivity or billable hours. This is particularly true for women lawyers, 56% of whom said that remote or hybrid working increased their ability to balance work and family obligations.*"

2. **Communications**.
    a. **Ethics Opinion 477R**.[7]
        i. ABA Formal Opinion 477R, "Securing Communication of Protected Client Information" explores the duty to use encryption and other safeguards to protect e-mail and electronic communications from evolving threats, developing technology, and available safeguards. It suggests a fact-based analysis and finds "*the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication*," but "*particularly strong protective measures, like encryption, are warranted in some circumstances*." It concludes that "*…a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security*."
        ii. Lawyers must use "reasonable efforts" to ensure the confidentiality of client information. Citing the ABA Cybersecurity Handbook, the opinion explains that the reasonable efforts standard is a fact-specific inquiry that requires examining the sensitivity of the information, the risk of disclosure without additional precautions, the cost of additional measures, the difficulty of adding more safeguards, and whether additional safeguards adversely impact the lawyer's ability to represent the client. What is "reasonable" is a gray area that we will consider below.
        iii. As previously mentioned, the RPC was modified to include that lawyers should keep abreast of changes in the law and its practice "*including the benefits and risks associated with relevant technology*."[8]
        iv. The opinion notes that generally lawyers may use unencrypted email when communicating routinely with clients.
        v. Attorneys who do not routinely use encryption should be prepared to explain why. The opinion includes several factors to consider when sending unencrypted emails:
            1. Understand the nature of the threat.
            2. Understand how client confidential information is transmitted and where it is stored.
            3. Understand and use reasonable electronic security measures.
            4. Determine how electronic communications about clients should be protected.
            5. Label client confidential information. This should include digital files.
            6. Train lawyers and non-lawyer assistants in technology and information security.
            7. Conduct due diligence on vendors providing communication technology.
        vi. **Practice Suggestion**: As a result, practitioners should consider having their IT or cybersecurity consultant prepare an annual letter to review matters in the office and suggest improvements. Then be certain to follow up on the improvements recommended for implementation. A process of periodic review and follow up documented in this manner may provide corroboration that the practitioner has acted with "reasonable efforts."
        vii. **Practice Suggestion**: There are technological solutions that permit certain sensitive emails, e.g. those with tax identification numbers, social security numbers, etc. to automatically be encrypted. There are also encryption services that make the use of encrypted email easy and efficient, e.g. through an extra button on the regularly used email interface, such as Outlook. Implementing

technology that automatically addresses protecting sensitive information may help reduce the risk of inadvertent disclosure of confidential data.

viii. **Practice Suggestion**: Practitioners should consider adopting a written policy for internet and email usage, secure passwords, mobile device security, and electronic equipment disposal. There are many free or low-cost sources on the web which can provide starting points for these policies. You might also provide basic cyber security training for all employees. There are many options available for this including the free online courses on cybersecurity.[9]

ix. **Practice Suggestion**: Security experts recommend password managers as an easy and effective way to upgrade any office's security[10]. Anyone can sign up for an individual plan, but many password manager providers also offer business plans that enable the employer to grant (or subsequently remove) access to firm information.

x. **Practice Suggestion**: Practitioners should consider how else they may demonstrate efforts to stay abreast of technology. Some practitioners may be sufficiently knowledgeable of current technology to address many issues based on their own expertise. It is likely that this is not the case for most practitioners. Consider adopting a policy, even in small firms, of mandating some professional education regarding the use of technology in estate planning practices even if there is no mandatory education required by the applicable authorities.

b. **Communicating Hypotheticals with Client Fact Patterns on the Internet**.

i. ABA Formal Opinion 511 addressed the situation where lawyers request insight on client issues by posing hypotheticals including client fact patterns on the internet, namely listservs.[11]

ii. The opinion notes:

1. "*RPC 1.6 prohibits a lawyer from posting questions or comments relating to a representation to a listserv, even in hypothetical or abstract form, without the client's informed consent if there is a reasonable likelihood that the lawyer's questions or comments will disclose information relating to the representation that would allow a reader then or later to infer the identity of the lawyer's client or the situation involved. A lawyer may, however, participate in listserv discussions such as those related to legal news, recent decisions, or changes in the law, without a client's informed consent if the lawyer's contributions will not disclose, or be reasonably likely to lead to the disclosure of, information relating to a client representation*."

iii. Keeping the client anonymous is a possibility:

1. "*Not all inquiries to a listserv designed to elicit information helpful to a representation will disclose information relating to the representation. In some situations, because of the nature of the lawyer's practice, the relevant client or the situation involved will never become known, and therefore the lawyer's anonymized inquiry cannot be identified with a specific client or matter. In other cases, the question may be so abstract and broadly applicable that it cannot be associated with a particular client even if others know the inquiring lawyer's clientele. In circumstances such as these, a lawyer may post general questions or hypotheticals because there is no reasonable possibility that any listserv member, or anyone else with whom the post may be shared, could identify the specific client or matter.*"

3. **Policies on Hiring Outside Consultants for Technology**.
    a. While there is no prohibition against members of the same firm maintaining data on the same network, RPC 5.1 "Responsibilities of Partners, Managers, and Supervisory Lawyers" states that any partner in a firm needs to take reasonable measures "*to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.*"[12]
    b. RPC 5.3 addresses an attorney retaining nonlawyer assistance, and the ethical requirements regarding that assistance.
        i. It was amended in 2012 to expand its scope. "Assistants" was expanded to "Assistance," extending its coverage to all levels of staff and outsourced services ranging from copying services to outsourced legal services.
        ii. An attorney must make reasonable efforts "*to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer.*"[13]
    c. This requires attorneys to employ reasonable safeguards, including performing due diligence, reviewing contractual requirements, supervision and monitoring to ensure that nonlawyers, both inside and outside the law firm, provide services in compliance with the attorney's ethical duties, including confidentiality. If a practitioner retains an outside IT consultant, be certain the firm has familiarity with issues faced uniquely by lawyers. Does the IT firm represent other law firms? Are they familiar with the RPC?
    d. What happens if an outside consultant violates the attorney ethics rules, such as client confidentiality? The RPC indicates that an attorney may be ethically liable for the conduct of the outside consultant, as an attorney is responsible for any violations by the nonlawyer if "*the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved*."[14]
    e. There may be numerous attorneys, non-attorney staff and outside consultants accessing the firm network, including sections with confidential client data.
    f. Consider creating a firm policy addressing when an attorney, non-lawyer staff, or outside consultants can be given access to the firm network, partitioning off sections of the network based on need for each individual, as well as policies on vetting outside consultants before they are given access to the firm network.
    g. Consider when employing third party vendors the kind of information they may have access to. Would they have the ability to retain the files? Do they have the ability to remotely access your network (such as with IT consultants)? Consider the use of Non-Disclosure Agreements ("NDA") for any vendors that have access to sensitive information to show reasonable efforts were made to protect confidential data. Also consider including in the NDA a provision that requires the third-party vendor to destroy any confidential information they may have stored, either in paper or electronic format, as part of assisting you, within a reasonable frame of time. You can determine a reasonable amount of time based upon the kind of work the third-party vendor is performing.
4. **Client Property and Electronic Storage**.
    a. **Safekeeping of Client Property**.
        i. RPC 1.15(a) [15] provides that complete records of client trust account funds and other property shall be kept and preserved by the lawyer for a certain period of time after the termination of the representation. The number of years varies by jurisdiction, e.g. 7 years.
        ii. Some ethics opinions and articles have applied it to electronic data held by attorneys (see discussion above).

b. **Client records – File and Data Destruction**.
    i. Simply because you can destroy a file after 7 years (or some other period) does not mean that you should. Consider defensive practice when deciding what to do with the file. If there is the possibility of a malpractice claim at some point, might the file be critically important for the lawyer's defense? Or might it be harmful? The policy established on destroying files should be consistent.
    ii. If any portions of a client's file are destroyed, care should be taken to preserve the confidentiality of the information contained in the documents. If there is a litigation hold all electronic records should be preserved until the litigation has been concluded.
    iii. When upgrading hardware, such as providing new laptops to firm employees, the destruction of any data on devices being retired will need to be addressed. Practitioners may wish to create a written policy that all hard drives or other storage devices must be removed from any desktops or laptops when being decommissioned, and properly disposed of to ensure all data is destroyed. Third party vendors can be contracted to destroy a hard drive and provide a certificate of destruction proving the data was destroyed.[16] There are also electronic programs that can safely wipe a hard drive, so the data is not recoverable. For practitioners that choose to electronically wipe data, for example if the laptop is going to be repurposed to be used by an individual who should not have access to the confidential data on the device, consider having your IT consultant assist you in wiping the hard drive, and have the consultant provide written proof they assisted.

c. **Personal Laptops**.
    i. Every device of any kind that holds client data should be encrypted. Further, if the practitioner has a home computer that is encrypted but to which their spouse has access (because they know the password), client confidential data should not be stored on that computer.
    ii. **Sample Clause**: Consider the following policy: "*An attorney or staff member is specifically prohibited from storing electronic business records of the firm on a home computer or other device to which others have access, and which is not encrypted. If an attorney or staff member creates or edits an electronic business record using a home computer, laptop, or other device, that person must save the record on the firm's electronic document management system as soon as possible. No firm attorney or staff member is permitted to store electronic business records anywhere other than the firm's electronic document management system*."
    iii. Remote access programs such as "GotomyPC" by Citrix, and hosted server arrangements (from companies such as ProCirrus or Uptime Legal) can allow access to a device on the firm's protected network without storing confidential client information on personal devices.

d. **Cloud Storage**.
    i. A law firm is permitted to store the electronic materials relating to the client on a remote server under third-party control as long as the law firm carefully selects the third-party company to ensure that the information is kept confidential.
    ii. What should be done to corroborate the selection?
    iii. Attorneys must take reasonable care to protect a client's information in a cloud environment.[17]

5. **<u>Confidentiality of Information in the Electronic Age</u>**.
    a. **Confidentiality of information**.[18]
        i. RPC 1.6 indicates that "*A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized to carry out the representation, and except as stated in paragraphs (b), (c) and (d).*"
        ii. 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*."
        iii. A comment to the rule requires a lawyer to competently act to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure.[19]
    b. **Protecting Confidential Information**.
        i. Consider using encrypted emails, e.g. ShareFile, Microsoft 365 encryption, etc. to transmit documentation with TINs, social security numbers, and other confidential data.
        ii. Take precautions to protect the physical office facilities.
            1. Defensive measures employed are only as strong as their "weakest link." Even if sufficient electronic safeguards are created, if the physical location of the firm's devices and network are not also protected, the data could potentially be compromised.
            2. The use of an alarm system at office locations would provide notification of a break-in and reduce time a bad actor would have access to any electronic devices.
            3. Disabling the USB ports on any devices connected to the firm's network, unless proper authorization has been provided to unlock the port, would prevent a weak point in protection from either an inadvertent infection of a network, or malicious actions.
        iii. If flash drives or external hard drives are necessary, consider buying encrypted versions of those devices, which are readily available.[20] In some instances, firms might limit the use of USB drives solely to non-client data such as PowerPoints taken to speeches.
        iv. Take precautions to protect the integrity of electronic data. This might include:
            1. Encryption and password protection of laptops, smartphones and other equipment.
            2. Providing guest internet access, which is password protected and outside the firm firewall, for clients and other visitors in the firm office.
            3. Protect all systems with appropriate virus protection, spam filters, intrusion protection, Multi-Factor Authentication, etc. See additional discussion below.
            4. Dark Web Scanning. Compromised information is often uploaded to the dark web, where information brokers sell the stolen information. If the practitioner has regular scans performed, and information is identified on the dark web, it may provide the practitioner with warning that a breach has occurred and allow corrective action to be taken.
            5. As discussed above, consider requesting that a memorandum be prepared by the firm's IT department or IT consultant outlining steps already taken to protect electronic systems and confidential information, and have additional suggested steps included in the memorandum. Subsequent memoranda should show efforts made to implement the

suggestions made in previous years. Establishing a history of activity taken and due diligence performed may show that actions taken by the practitioner in protecting electronic information were reasonable.

v. Use best judgment regarding when you need to take extra security measures. Consider the reasonable efforts factors mentioned in Ethics Opinion 477, discussed above.

c. **Addressing a Data Breach**.

i. Understand that the risk of data breaches are a constant in modern life.

1. Breaches have become so prevalent that a common saying in cybersecurity today is: "*there are two kinds of companies: those that have been breached and know it and those that have been breached and don't know it.*"[21] This is as true for law firms as it is for other businesses and enterprises.
2. ABA Formal Opinion 477R (May 2017) describes the same threat environment: "C*ybersecurity recognizes a … world where law enforcement discusses hacking and data loss in terms of 'when,' and not 'if…'*"
3. Ethical rules and malpractice avoidance leave no doubt: lawyers must be prepared to prevent and remediate data breaches.

ii. Several RPCs may apply during the occurrence of a data breach.

1. RPC 4.1 (false statements to third persons) and RPC 4.3 (dealing with unrepresented persons) may apply in certain situations involving breach notification laws where applicable.
2. RPC 1.8 comment 5 (use of information to the disadvantage of a client may violate the duty of loyalty) and RPC 1.7 comment 1 (conflicts arising from a lawyer's own interests) may also require disclosure to the client of a data breach.

iii. The ABA in Formal Opinion 483 stated that if a data breach occurs that involves client information, lawyers have a duty to notify current clients of that data breach.[22]

1. The opinion discusses the obligations of monitoring for a data breach, stopping a breach, restoring systems, and determining what occurred. It finds that RPC 1.15 applies to electronic client files as well as paper files and requires attorneys to exercise the care required of a professional fiduciary. The opinion concludes: "*Even lawyers who, (i) under Model RPC 1.6(c), make "reasonable efforts to prevent the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model RPC 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data breach under Model RPC 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation.*"
2. However, if the data accessed was encrypted, there may be nothing for the client to worry about and the breach notification laws in most states may not be triggered (if they only require notification if "unencrypted" data is accessed by an unauthorized party).

iv. Attorneys have a requirement to monitor for any data breaches, so current clients can be informed if one is discovered.
v. There are programs that can be used to assist in monitoring the practitioner's various devices and network to attempt to identify data breaches and end unauthorized access to confidential data as quickly as possible.[23]
vi. Interestingly, there is no requirement to notify former clients. Practitioners might wish to consider what action is appropriate, taking into consideration the nature of the data breach and if former client data was affected. Notification might be advisable regardless of whether it is required.

6. **<u>What Cybersecurity Risks are there, and how can Practitioners and Their Clients Address Them?</u>**
   a. Practitioners should not and need not fill the role of IT consultant, but many clients do not retain personal IT consultants and do not take adequate protective measures. So, the role practitioners can take is building awareness and making general suggestions to help guide clients. This is no different that the wide-ranging advice that is often discussed in a holistic approach to estate planning. Practitioners can use regular firm newsletters and other communications to inform clients about cybersecurity risks.
   b. There is another aspect to consider. Some of the nefarious actors may send out vast numbers of attacks knowing they only need a few "bites" to make it a financially rewarding endeavor. The targets that may "fall" for the scams are often elderly, infirm or otherwise challenged individuals. These are the same individuals estate planners typically serve and try to help protect with planning and proper legal documentation.
   c. The following suggestions are made from this viewpoint.
      i. Anti-virus software is essential. The free versions of anti-virus that typically come with new computers may not be sufficient, especially for clients who use the Windows operating system.
      ii. Phishing protection is another important protective element. Phishing is an email sent from what appears to be a reputable company, but which is merely a cover for cyber-criminals seeking to induce individuals to reveal personal information such as passwords and credit card information. With the proliferation of artificial intelligence like Chat GPT, Microsoft Co-Pilot, etc. phishing attacks have increased in number and become more advanced. A report on the state of phishing in 2023 noted that phishing attacks had increased 1,265% in 2023 after the release of Chat GPT in November 2022.[24] The updated report in 2024 reflected an additional 703% increase in credentialed phishing attacks.[25] Examples of phishing might include: fake invoices, an email account upgrade, advance-fee requests, fraudulent google documents, a Dropbox scam, email from an attorney with documents for the recipient, etc.[26] These attacks can appear deceptively genuine and can easily entrap a sophisticated attorney, and more so an aging or challenged client. In addition, bad actors often send these attacks at specific times in an attempt to increase success. For example, an email may be sent to the practitioner (or their administrative staff) at 4pm on a Friday, when the individual may be tired and thinking about the upcoming weekend, increasing the risk of clicking the link and compromising the firm's system.
      iii. Clients should be cautioned to be alert for requests for sensitive information, unexpected emails, suspicious attachments, too good to be true. If the recipient clicks on the fake link or attachment malware may be downloaded to spy on their computer usage.
      iv. While many people are aware of email phishing, bad actors are innovative and continuously thinking of new ways to attempt compromising an individual. For example, QR-ishing, which is scanning QR codes in public locales such as

restaurants, can pose risk. Criminals have replaced retail QR codes with substitutes that nefariously redirect the user to a dangerous website. For an elderly client that is particularly susceptible to being scammed, consider whether it might be feasible to block camera access to their cellphone to avoid scanning questionable QR codes.[27] For practitioners that have client contact data and confidential emails on their cell phone, might a policy to never scan QR codes with such a phone be prudent?

v. Smishing is another variation that may take the form of a text message, which appears to be sent from a reputable company seeking to induce the recipient to reveal personal information. These might include: a bank account verification scam (a warning of unauthorized activity in the recipient's bank account attempting to extract sensitive data), notice of a package delivery alert to induce the recipient to click a link and provide data, or account suspension alerts from what appears to be a reputable company. Clients might be advised to exercise caution if they receive a text from an unidentified or unknown telephone number. The nefarious text message may claim to be from a company the recipient knows. Urgency is often conveyed in the message. There may be requests for money or information. If the recipient clicks the link their cellphone may be subject to security threats.

vi. Vishing is a telephone call made by a seemingly reputable company seeking to induce individuals to reveal personal information. For example: A cybercriminal may call and appeal to the target's human instincts of trust, fear, greed and desire to help. The criminal may ask for bank account information, credit card details, mailing address, etc. The criminal may request a funds transfer, or disclosure by phone or email of confidential information or documents. The caller may pretend to be a government representative, tech support representative, a telemarketer, or banker with the target's bank. Pay close attention to any caller. Do not answer calls from unknown numbers. Never provide personal information to an unsolicited caller. Register your phone number with the Do Not Call Registry. For an elderly or infirm client, perhaps their use of their cell phone might be monitored, or they can be instructed and reminded that only a named person handles all their finances so that if anyone calls about financial information they should do no more than tell the caller to call that named person. Perhaps a remainder sign might be framed and left on the table where the phone is typically kept.

vii. Social Engineering (using any of the above and/or social media) is an attack intended to deceive the victim and obtain control over a computer system or steal personal financial or other confidential information. Social engineering techniques account for 98% of all cyberattacks.[28] Social engineering may use phishing and other strategies. In September 2023, hackers breached large casinos including MGM and Caesars, accomplished via social engineering.[29] Hackers impersonated firm employees and convinced the technology helpdesk to provide them duplicate access. The hack was accomplished by hacking group ALPHV, who posted about the hack on its website and warned MGM of further attacks if MGM didn't comply with its demands.

viii. End-Point Detection Response ("EDR") software. This is next-generation anti-virus software. Examples include: SentinelOne Singularity, CrowdStrike Falcon, Sophos Intercept X, Trend Vision One.[30] Traditional anti-virus companies respond when a computer virus is released, figuring out how to neutralize the virus and protect against it, and then push out an update. Anti-virus companies have

traditionally pushed out updates almost daily. However, how often do individuals actually update their anti-virus protection? In contrast, EDR is a more holistic approach, viewing the actions taken by the computer, and if it finds unusual activity indicative of a virus, the software will shut the computer's activity down and stop it from accessing the internet to prevent further damage and data loss. This then provides time for a counter to the virus to be found. This helps prevent "Zero day" virus infections. To address updating software consistently, set rules can be implemented that provide for updates to be completed automatically. Practitioners may consider recommending that clients create a habit of restarting their computers at least weekly to apply the updates that have been queued.

ix. Password managers. A password manager is a repository that will store all passwords. Certain password managers will allow the individual to "auto-fill" login credentials on websites, but all of them will allow the copy and paste of login information when needed. A password manager makes it easier to create robust and unique passwords. Many clients (and practitioners) will reuse passwords across multiple programs and websites. A recent study found that 78% of people reuse the same password across multiple accounts.[31] If that password is compromised all those accounts are compromised.

x. Multi-Factor Authentication ("MFA") should be considered whenever available. Passwords, even strong complex ones generated by a password manager, are no longer sufficient to rely on to secure an account. Even the strongest password can be defeated by malicious programs such as keyloggers, which provide a third party with all keystrokes made on the computer if compromised. MFA provides an additional layer of security beyond a password to access an account. This is typically a numerical code that is provided through one of several methods: via email, text message ("SMS"), or an authenticator app on the user's cellphone. The use of MFA also potentially provides the practitioner with a warning that the password has been compromised when access is attempted without the proper multi factor access.

7. **Aging Clients, Technology and Cybersecurity**.

   a. **Should Advisors Discuss Cybersecurity with their Clients?**

      i. Clients routinely communicate with their estate planners and other advisers electronically via email, sending confidential documents, transmitting data through online portals, web meetings, electronic signature of certain documents (perhaps retainer agreements and other items), etc. Even if the practitioner has state-of-the-art cyber-security measures in place, if the client has inadequate protection, or fails to use the systems the adviser provides (e.g., sending tax documents via unencrypted email, rather than using a secure portal provided by the practitioner), the client's data could be compromised. Estate planners routinely discuss planning for issues of aging (e.g., a durable power of attorney), asset protection, and other planning considerations. Addressing client cybersecurity and related issues is an important part of those conversations, even if the practitioner does not have the technological expertise for a detailed or in-depth discussion. Merely highlighting some of the key issues might educate a client sufficiently that the client will then take appropriate measures.

      ii. Clients frequently provide their professionals with sensitive information (personal identifiable information) such as tax returns, financial statements, and more. Without proper protection, e.g., the client may merely send sensitive documents via unencrypted email and without password protection, disaster could ensue. If the client's email is compromised, a bad actor could gain access to those sensitive documents which might lead to theft, elder abuse, etc.

iii. Cybersecurity can be an overwhelming topic for many if not most clients, especially older clients who may feel less tech savvy. However, whatever steps practitioners might suggest, or even just risks that can be communicated, may help clients move in the direction of better security. That can safeguard the client from elder financial abuse, identity theft and other risks. While these issues are not as central to the estate planning process as drafting a will, evaluating life insurance coverage, and other traditional steps, they may be integral to a holistic estate planning process, and to helping clients.

b. **Bad Actors Target Estate Planning Clients.**

i. Helping advise clients on protecting their wealth should be given priority. Practitioners can have conversations with clients to ensure that the client understands the risks, and what steps they can take to reduce those risks, even if the only step communicated is to retain a personal IT consultant. Practitioners can discuss with clients how significant a data breach event could be, and the time and effort it takes to rectify an issue once it happens. It is far more costly and time-consuming to fix an issue than it is to spend the time protecting themselves in the first place. Each year, the FBI releases a report analyzing nationwide internet crime.[32] In 2019, the FBI received 467,361 complaints totaling $3.5 billion in losses. By 2024, the FBI received 859,532 complaints, which totaled $16 billion in losses.[33] This represents a growth of nearly double the complaints, and more than quadruple the losses per year in just 5 years! The growth of AI may accelerate these incidences as bad actors may be able to provide more convincing and deceptive email and phone call attacks.

ii. Elder abuse and identity theft can create a huge disruption in the client's lives. Clients should understand how disruptive it would be to lose access to their LinkedIn accounts, Facebook accounts, cloud storage programs like Dropbox, Microsoft 365, etc. for their day-to-day lives. This discussion may help a client understand how significant technology is in their lives, and how a data breach or loss of access would affect them.

c. **Clients Avoid Using Safeguards Due to Complexity.**

i. Some clients are recalcitrant to use safeguards offered by practitioners, such as a client portal, because of their lack of familiarity with those mechanisms. Perhaps some are embarrassed to admit that they cannot master the technology involved. Consider offering "cheat sheets," or instruction manuals, which explain with simple steps and screen shots what to do and how to use a particular piece of technology. Short video clips posted to a firm website providing instruction on using the firm's portal, cybersecurity measures private wealth clients might consider, and similar topics should be inexpensive to create and may not only help clients, but they may protect the practitioner as well. Offer to help clients struggling with these safeguards to join a web meeting and talk them through how to use the tools provided.

ii. A survey from Nationwide that concentrated on cyber security and the proliferation of identity theft insurance revealed that while 80% of respondents expressed concern about identity theft, only 16% reported having identity theft insurance.[34] The survey found that 77% of respondents have accepted the risk of identity theft as a normal part of life. However, 28% admitted they have never sought more information about cyber protection. Many consumers neglect essential cybersecurity precautions due to misconceptions about the cost and effectiveness of these measures. This should come as no surprise as many law firms have no such coverage.

iii. FiServ prepared a study regarding the general public's awareness of cyber security, remarking "*a surprising number of U.S. consumers have little awareness of how to defend themselves against a cyberattack. Some never change their passwords and when they do, it's only because they're forced*." The study found that 59% of consumers are bothered by temporary inconveniences brought about by advanced security measures, even if it means higher levels of safety and protection.[35]

d. **How Should Clients Transmit Information to the Practitioner?**

i. Practitioners might consider incorporating into their practices how clients can send data securely to the practitioner they may need for the estate planning process.

1. Providing clients with tools to securely communicate data with you as a professional is a service to clients and a way to facilitate clients communicating and providing documents in a safer manner. This could be by providing a secure portal clients can use to upload data, suggest clients password protect any confidential data that will be sent via regular email (and not to send the password in the email), and/or to obtain more secure email service.
2. Practitioners might establish a policy in their firm that if a client sends an email with confidential data that is unencrypted, someone at the firm would be notified and follow up with the client and endeavor to help provide guidance.
3. What is the right level of protection for clients to use in their email? There are certain legacy email systems that may be dangerous to continue to use in today's environment. If a client still has an AOL, Hotmail, or similar older email address, practitioners may suggest that the clients consider updating to a more modern and secure email.
4. There are paid versions of many email systems that may be more secure than a free/unpaid version: Gmail, Outlook, Yahoo, etc. If the client merely switches to an inexpensive paid version of what they are using they may materially enhance their protection. It does not take a significant amount of time to set up these paid services that provide additional protections. Typical cost for these email services is approximately $5-20 a month, and maybe an hour or two of an IT professional's time to set-up. These paid email systems may provide: Better spam and phishing filters; better alerts for any security issues; access to support from the company you purchase the email from; an easier environment with protective tools for an IT professional to manage.[36]
5. However, even with the paid versions of these common email systems, emails are not automatically encrypted. Discuss with clients that communicating securely needs both a baseline of protections, as well as discipline. For example, Outlook 365 can encrypt email without having any third-party software. Outlook can send emails using these "sensitivity levels" that only allows people with that specific access to be able to view the email. Encrypt-only encrypts the email and the attachments. However, these protections can only be implemented with a proactive approach, reviewing the various options in Outlook 365, determining the clients risk threshold and comfort level with restrictions (certain security measures may block legitimate emails, and clients may be frustrated by

that) and understanding that those security measures will need to be reassessed on a periodic basis to determine if evolution in cybersecurity warrants changes. All of this could be overwhelming to a client, even with the assistance of an IT professional.

ii. Another common issue is clients use their professional or business email account to transmit their personal communications. While some clients may choose to communicate through their business emails for administrative ease (i.e., they don't want to maintain multiple email accounts), or due to their business emails having a heightened level of protection, practitioners should consider warning clients that there could be concerns with communicating on personal matters through their business emails.
    1. If a client uses business email for personal matters, this results in all such personal communications being stored on the business email server (and documents on the business network or cloud).
    2. If the client leaves the company (voluntarily or by being fired), they could lose access to all of the personal email information.
    3. For clients that are business owners, they may not have concerns with losing access to their personal information. However, what if the business is sold? What if their business is sued, could the client's confidential personal information be discoverable and accessible to the adversarial party? Consider the impact of personal financial statements, or estate planning memorandum discussing asset protection steps, falling into the hands of plaintiff's counsel. Most if not all clients should have a separate personal email address with appropriate cybersecurity and not use a business email address for personal matters.

iii. Secure client portals. Practitioners might consider obtaining a system to create a portal so that they provide clients with a mechanism to securely send or upload confidential documents. There are a host of providers and many of these can be branded for the firm to generate a positive image of concern for client security.
    1. This can also provide a means for practitioners to maintain online access for clients, and those individuals the client designates (e.g., other advisers, fiduciaries, family members) to electronic copies of signed estate planning documents.
    2. For example, the practitioner could upload copies of a client's signed will, trusts, health care documents, powers of attorney, etc. in the client's portal. This could be both an added service for the client and a potentially a way to reduce administrative burden for the practitioner.
    3. If a client has ready access to copies of their documents online, and chooses to give other advisers, e.g. their CPA and wealth adviser, access to their portal, they may not have to reach out to the practitioner to ask for copies of those documents. Such a request can result in nonbillable administrative time and also concerns if a CPA or other adviser asks for documents. All of that might be avoided.
    4. The portal can be used for more than securely sending confidential documents. Certain applications will permit additional communications through the system, such as supporting a "chat" function and texting integration. For clients comfortable using the portal, communicating through the portal could protect sensitive conversations from potential exposure. If the client's email system is compromised, then any emails sent to or received from the practitioner would be accessible to the bad

actor. A secure portal chat function may protect that sensitive information.

iv. Practitioners will need to lead by example. They should use the portal, use encrypted email, show clients that they take cybersecurity seriously and clients may reciprocate.

8. **Reviewing Your Own Personal Cybersecurity**.
    a. As practitioners review the role that they can serve when encouraging clients to take precautionary measures, they should also evaluate whether they themselves have taken appropriate precautionary measures. Some practitioners, whose firms have state-of-the-art cyber protection and other security, have wholly inadequate personal cyber security.
    b. Consider that one in four lawyers reported that their firm had a cybersecurity breach in 2022, according to a 2023 report from the American Bar Association.[37] Navigating personal and firm tech enhancements will help equip the practitioner to take the same messages to their clients.
    c. Practitioners that use personal laptops and cellular phones for any work-related matters, e.g., answering emails, need to be alert to and should endeavor to have protections installed, as their falling prey to any of the cyber-attacks discussed above could jeopardize confidential client data. Work-related laptops should be part of the firm's cybersecurity ecosystem and appropriately secured.
9. **Routers and Firewalls- Securing Home Internet**.
    a. The proliferation of remote work has practitioners operating out of their homes, accessing the internet on devices with confidential client data through home networks. Consider, how protected is your home internet? Firewalls are often used by businesses, but many practitioners (and clients) neglect to implement them for personal use. Bad actors often look for the "weakest link" to compromise a system. If the practitioner has a spouse or children accessing their personal network, the devices family members operate on may not be as secure as those the practitioner uses. Bad actors can access the network through compromising those less protected devices. Practitioners may be using a personal laptop on the same network their business laptop is on, with that personal laptop having less protection then what they would ever accept for their professional devices. Practitioners may conduct their banking, and other sensitive activities from that laptop. Bad actors may be able to pierce those lesser protections and cause significant damage to the practitioner's life.
    b. Many individuals have older routers with outdated security. There have been bad actors that have hacked routers in residential neighborhoods. They can drive around the neighborhood and attempt to connect to the network from outside the home. This is called "Wardiving."[38] Internet service providers (Spectrum, Verizon, etc. "ISP") provide customers with a modem to access the internet. A basic router, if provided by an ISP, may also provide a firewall, but may not offer stateful packet inspection (where all network traffic is analyzed inbound and outbound for threats). Obtaining and installing an after-market router that incorporates a more robust firewall may be prudent. A stronger firewall protects everyone accessing the internet on your network.[39]
    c. The phrase "Internet of Things" has entered the lexicon. This refers to not just the obvious cell phones and laptops, but also the many home appliances that are connected to the internet through a home network. This can include smart refrigerators, Nest security devices, Ring doorbells, microwaves, even cat litter boxes that may all be wired to the internet and to cellphone apps. These items may have weaker security protections, and bad actors may hack into them and use that as a "backdoor" to access a home network.[40] For example, consider whether the default password for accessing the smart TV or smart refrigerator has been changed. It is likely that many practitioners will have one or more

devices connected to their network that is using a default administrator password. Bad actors could traverse a neighborhood attempting to connect to these devices with manufacturer passwords and see if they can access any devices. An aftermarket router may provide better protection through the implementation of a firewall for the myriad of items that are on a typical home network. In addition, periodically updating the firmware of appliances may help mitigate these risks.

10. **<u>Can an Attorney Remotely Work in a State Where They Are Not Licensed to Practice Law?</u>**
    a. **How Common is this Issue?**
        i. Working from home for many may involve working from a state in which you are not admitted to the bar ("Non-Licensed State"), for a practice in a second state where you are admitted ("Admitted State"). As remote and hybrid work continues to evolve, this potential ethical issue may be raised more often. Further, more older lawyers may wish to reduce hours but continue to practice. The instances in which lawyers will be practicing in a state where a second home is located and in which the practitioner is not licensed are likely to increase for this demographic.
    b. **Two Step-Analysis Required.**
        i. In Formal Opinion 495,[41] the American Bar Association ("ABA") addressed whether an attorney can remotely work from a state in which they are not licensed. A two-step analysis was established to determine what is acceptable:
            1. Opinion 495 concludes that "*Lawyers may ethically engage in practicing law as authorized by their licensing jurisdiction(s) while being physically present in a jurisdiction in which they are not admitted under specific circumstances enumerated in this opinion*." So, when engaging in remote work, as the first prong of the analysis, you might want to confirm that whatever circumstances your situation involves reasonably fit within the permissible parameters of Opinion 495.
            2. Opinion 495 goes on to state: "*this Committee will not opine whether working remotely by practicing the law of one's licensing jurisdiction in a particular jurisdiction where one is not licensed constitutes the unauthorized practice of law under the law of that jurisdiction*." Thus, as the second prong of the analysis, it may also be prudent to confirm what the laws in the jurisdiction in which you are working, but are not licensed, provide.
    c. **Advertising, Business Cards, and Holding Out Tests.**
        i. ABA Opinion 495 states: "*Lawyers may remotely practice the law of the jurisdictions in which they are licensed while physically present in a jurisdiction in which they are not admitted if the local jurisdiction has not determined that the conduct is the unlicensed or unauthorized practice of law and if they do not hold themselves out as being licensed to practice in the local jurisdiction, do not advertise or otherwise hold out as having an office in the local jurisdiction...*"
        ii. With the mobility that virtual practice affords, lawyers may be working on a case for their firm in a jurisdiction where they (or the firm) are licensed, from a home or vacation home located in a jurisdiction where they are not licensed.
        iii. Opinion 495 continues by noting: "*…and do not provide or offer to provide legal services in the local jurisdiction...*" If you participate in web meetings from that Non-Licensed State, is that equivalent to "*provid[ing] legal services in the local jurisdiction"*? It would seem not, but as web meetings become a dominant form of meeting, in contrast to the traditional physical or in-person meeting, might that analysis change? What if the lawyer's firm has an office in the Non-Licensed State,

might that rise to "*provid[ing] legal services in the local jurisdiction*"? The issue as to whether conducting web meetings in a state where the attorney is not licensed was raised in a recent Missouri ethics opinion.[42]

1. "*Question: Lawyer is planning to retire after a long career of practicing law in Missouri. Lawyer is moving to another state, but lawyer plans to continue to wind up lawyer's practice in Missouri and occasionally participate virtually in meetings with clients and appear virtually in Missouri courts. Is lawyer permitted to wind up lawyer's practice in Missouri from another state?*
2. *Answer: Lawyer needs to determine if the other state from which lawyer plans to wind up lawyer's Missouri practice and occasionally participate virtually in client meetings and appearances in Missouri courts constitutes the unauthorized practice of law in the other state. Rule 4-5.5(a) provides that "[a] lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction…." If the other state would determine lawyer's conduct to be the unauthorized practice of law, then lawyer may not proceed without violating Rule 4-5.5(a)."*

iv. The above Missouri opinion suggests that mere web meetings may potentially constitute the unauthorized practice of law in a jurisdiction where the attorney is not licensed if that local state's rules would deem it so. The intent and purpose in the example was winding down a law practice in Missouri, not practicing in the Non-Licensed State, but that had no impact on the comment. This might suggest that the threshold for unauthorized practice may be quite a low.

v. Are more than mere web meetings required? For example, would the attorney also have to hold herself out as practicing law from a physical office? Might a building directory sign indicating "Esq." suffice to constitute holding oneself out as practicing law? What is the difference between a lawyer maintaining a designated room in their home as a regular home office versus a separate office in an office building?

vi. At what point might the lawyer be deemed to be providing legal services from the Non-Licensed State jurisdiction? Is there a number of web meetings from, or into, a jurisdiction that may rise to the level of holding oneself out as practicing in that jurisdiction? What measure of activities might be required to constitute: "*other systematic and continuous presence?"*

vii. Opinion 495 suggests that "*Having local contact information on websites, letterhead, business cards, advertising, or the like would improperly establish a local office or local presence under the ABA Model Rules*." Does that suggest that even if an office is rented in the lawyer's Non-Licensed State for them to work remotely from, so long as the office is not listed on a letterhead, business card or advertising, then it is not deemed to be a local presence? Consider the comment above about whether a mere listing on a building directory would constitute holding oneself out as practicing law from that location. The use of co-work, shared, or rental office space specialized in a wide range of flexible office arrangements is growing. One such company advertises: "*Our Business Address plan provides a prime office address at any of our 4000 locations worldwide, enabling you to establish a business presence without the need for a dedicated office space. Perfect for remote businesses or those looking to expand…*"[43] Slight variations in the shared office arrangement may suggest that the arrangement has risen to the level of holding oneself out as practicing law in that location.

viii. Opinion 495 states:

1. "*Model Rule 5.5(b)(1) prohibits a lawyer from "establish[ing] an office or other systematic and continuous presence in [the] jurisdiction [in which the lawyer is not licensed] for the practice of law." Words in the rules, unless otherwise defined, are given their ordinary meaning. "Establish" means "to found, institute, build, or bring into being on a firm or stable basis." A local office is not "established" within the meaning of the rule by the lawyer working in the local jurisdiction if the lawyer does not hold out to the public an address in the local jurisdiction as an office and a local jurisdiction address does not appear on letterhead, business cards, websites, or other indicia of a lawyer's presence. Likewise it does not "establish" a systematic and continuous presence in the jurisdiction for the practice of law since the lawyer is neither practicing the law of the local jurisdiction nor holding out the availability to do so. The lawyer's physical presence in the local jurisdiction is incidental; it is not for the practice of law* [source footnotes omitted]."

ix. Consider an attorney who works remotely from a vacation home in a state where she is not licensed. However, she prefers the atmosphere of a formal office to working at home, so her firm contracts with a local co-work provider. The sole purpose of the arrangement is to provide the attorney with a place to work when and as she needs it. If the contract with the co-work firm assures the use of office space anytime she wishes, does that alone constitute a "systematic and continuous" presence in that jurisdiction?

x. It appears according to Opinion 495 one key is "…*hold[ing] out to the public an address in the local jurisdiction as an office and a local jurisdiction address does not appear on letterhead, business cards, websites, or other indicia of a lawyer's presence*..." Is listing a physical office address an appropriate determinative factor in the modern era of practice? If the entire client relationship is handled via web meetings, telephone calls and email, how relevant today is a physical office "address"? Nonetheless, the concepts underlying Opinion 495 in part remain based on the physical office.

xi. Consider the situation of a lawyer working from a vacation home in a Non-Licensed State. Perhaps that may not be an issue. But the lawyer is active socially in the community and natural conversations with friends, neighbors and fellow volunteers raise the topic of the person being an attorney. Is that casual personal conversation tantamount to holding oneself out as an attorney in that state? Not uncommonly, those same people may seek legal guidance. If those persons are full-time residents of the Non-Licensed State, without the attorney being licensed, providing legal services to them may be problematic. What if the community is a vacation community and those asking for services are residents of the lawyer's Admitted State, not the Non-Licensed State? Would that change the analysis?

d. **Technology and the Evolution of Practice.**

i. Many non-legal businesses make concerted efforts to encourage their customers to seek online solutions. In addition, for individuals in non-legal professions, omitting their physical address from email signatures may suggest a more national, or international, reach of their services. That is precisely the type of misperception, e.g., the ability to practice in a state where they are not admitted, that attorneys may be required by ethics rules to avoid. With modern technology, many service providers, including professionals, are not limited to state lines or any geographical constraint.

ii. As an example in the law, the international law firm Rimon has pushed the tech envelope and tried to recreate the model of a law firm to enhance the provision of legal services and profitability. On its website it states:

1. "*The traditional law firm's offices, like the feudal lord's castle, tend to be large, well appointed, impressive — and very expensive to maintain. A law firm often spends about one-third of its revenues to pay for real estate and technology. Spacious offices in desirable city-center locations, hundreds of computers, printers and copiers, and the staff to keep everything operating add up to high overhead. These costs tend to be fixed, while attorney work levels and income may fluctuate. The COVID pandemic has thrown into stark relief the unnecessary waste of maintaining extravagant commercial leases in the modern era and furthermore, has many attorneys considering a more modern solution. While prior to the pandemic only 37% of U.S. lawyers expressed an interest in remote work, 76% now say they would prefer to work from home at least one day a week*."[44]

iii. The question really is becoming what is an "office," how should an "office" be defined, and with the increasing provision of legal services online (e.g., LegalZoom.com, Trust & Will, etc.) is an "office" an important consideration in a consumer's retention of legal services? As competition from Artificial Intelligence ("AI") and other non-lawyer websites and services expands, are the restrictions on remote work and even specific state licensure practical to retain long term? Will they merely serve to harm both clients and attorneys? That is an issue beyond the scope of this paper, but given consistent evolution of technology, one that may warrant consideration.

e. **Analyzing Legal Letterhead Ethics Rules.**

i. Historically, before email, legal letterhead had been used for all non-verbal legal communications. The rules of professional conduct for a particular state may provide requirements for communication on legal letterhead in that state. Those rules may include a requirement to identify lawyers on the letterhead that are not licensed to practice in the state.

ii. Today, attorneys send most communications via email. According to a survey conducted by the American Bar Association in 2020, only 9% of lawyers reported using regular mail as their primary method of communication with their clients, while 75% reported using email as their primary method.[45] However, some attorneys do not include in their email signature the physical address of their office, or a statement indicating where they are licensed to practice law. Should different standards apply to letterhead than to email? Might not listing locations of physical offices or the states of licensure be inferred by the client as the sending attorney or firm practicing law in jurisdictions they are not licensed in? This concept may be handled differently state by state.

iii. As an example, in New Jersey, N.J. Ct. R. RPC 7.5(b) states: "*A law firm practicing in more than one jurisdiction may use the same law firm name in New Jersey, provided the law firm name complies with this Rule. In New Jersey, identification of all lawyers of the firm, in advertisements, on letterheads or anywhere else that the law firm name is used, shall indicate the jurisdictional limitations on those not licensed to practice in New Jersey. Where the name of an attorney not licensed to practice in this State is used in a law firm name, or where the law firm name does not include the name of a lawyer in the firm or the name of a lawyer who has ceased to be associated with the firm through death or retirement, any*

*advertisement, letterhead **or other communication** containing the law firm name must include the name of at least one licensed New Jersey attorney who is responsible for the firm's New Jersey practice or the local office thereof*. [emphasis added]"

iv. Should similar standards that govern letterhead apply to email? These concepts also seem to have relevance to the concepts in Opinion 495 as to remote practice.

11. **Reviewing Several State Ethics Rules on Remote Work.**

a. **Maine Ethics Opinion Provides Additional Detail for Opinion 495.**

i. Opinion 495 includes quotes and excerpts from a Maine ethics opinion that raises some additional considerations:[46]

1. "*Where the lawyer's practice is located in another state and where the lawyer is working on office matters from afar, we would conclude that the lawyer is not engaged in the unauthorized practice of law. We would reach the same conclusion with respect to a lawyer who lived in Maine and worked out of his or her home for the benefit of a law firm and **clients located in some other jurisdiction**. In neither case has the lawyer established a professional office in Maine, established some other **systematic and continuous presence** in Maine, held himself or herself out to the public as admitted in Maine, or even provided legal services in Maine where the lawyer is working for the benefit of a non-Maine client on a matter focused in a jurisdiction other than Maine.* [emphasis added]"

ii. The "systematic and continuous presence" standard is found in the ethics opinions of numerous states, and will be discussed in more detail below.

b. **New Jersey Ethics Opinion Provides Additional Information on the Continuous and Systematic Presence Test.**

i. A New Jersey ethics opinion[47] provided points regarding actions a lawyer cannot take in New Jersey if not licensed to practice in the state:

1. "*Non-New Jersey licensed lawyers may practice out-of-state law from inside New Jersey provided they do not maintain a "continuous and systematic presence" in New Jersey by practicing law from a New Jersey office or otherwise holding themselves out as being available for the practice of law in New Jersey. **A "continuous and systematic presence" in New Jersey requires an outward manifestation of physical presence, as a lawyer, in New Jersey**. As the American Bar Association, Standing Committee on Ethics and Professional Responsibility, recently stated, lawyers do not "hold themselves out to the public" when they are "for all intents and purposes invisible as a lawyer to a local jurisdiction where the lawyer is physically located, but not licensed." ABA Formal Opinion 495 (December 16, 2020). Hence, **actions that merely manifest presence in New Jersey in the capacity of a private citizen or resident, and not as a lawyer, do not raise such concerns**. Such outward manifestations of physical presence include, most significantly, practicing from a law office located in New Jersey. See Jackman, supra, 165 N.J. at 588 (Massachusetts lawyer practicing from a New Jersey law firm office)…* [emphasis added]"

ii. While the New Jersey opinion provides a clear statement that an attorney working from their home in New Jersey while practicing law for their Admitted State may not create an issue, it requires an analysis of whether they have created an "outward manifestation of physical presence" of their practice. With a clear example of practicing from an office in New Jersey their firm may run, should a

practitioner who lives in New Jersey, but is licensed in another state, have concerns if their firm chooses to open a New Jersey satellite office?

c. **Does District of Columbia Ethics Opinion Referencing COVID-19 Pandemic Create Staleness Concerns?**
    i. The District of Columbia ("DC") was one of the first jurisdictions to release an ethics opinion, on March 23, 2020, before ABA Opinion 495 was released.[48] The opinion is linked to the COVID pandemic, and its continued application may be uncertain. This opinion concludes:
        1. "*In view of the foregoing principles, the Committee's opinion is that an attorney who is not a member of the District of Columbia bar may practice law from the attorney's residence in the District of Columbia under the "incidental and temporary practice" exception of Rule 49(c)(13) if the attorney (1)* ***is practicing from home due to the COVID-19 pandemic****; (2) maintains a law office in a jurisdiction where the attorney is admitted to practice; (3) avoids using a District of Columbia address in any business document or otherwise holding out as authorized to practice law in the District of Columbia, and (4)* ***does not regularly conduct in-person meetings with clients or third parties in the District of Columbia****…* [emphasis added]"
    ii. No subsequent ethics opinions released by the DC Bar addressing the practice of remote work were identified. If this is the most recent opinion, now that the COVID-19 pandemic has ended, can attorneys continue to rely on the DC ethics opinion? In addition, if an attorney chooses to have in-person meetings in DC when they are not licensed there, what number or frequency of meetings rises to the standard of "*regularly conduct in-person meetings with clients or third parties in the District of Columbia*"?

d. **Missouri Opinion Suggests Need for Co-Counsel to Remotely Work.**
    i. Missouri releases ethics opinions through the creation of "Informal Opinions." In one of the more recent opinions addressing remote work, adopted on January 23, 2024,[49] Missouri appears to state that attorneys practicing the law of their Admitted State cannot work remotely from Missouri:
        1. "***Subject:*** *Unauthorized Practice of Law; Multijurisdictional Practice of Law*
        2. ***Summary:*** *Virtual practice of law of another jurisdiction from Missouri, but not licensed in Missouri; Missouri license required*
        3. ***Question:*** *Lawyer is licensed in State A but lives in Missouri. Lawyer is not licensed in Missouri. Lawyer plans to work for a law firm located in State A from Lawyer's home office in Missouri. Is Lawyer required to seek admission in Missouri?*
        4. ***Answer:*** *Yes. Rule 4-5.5(b)(1) prohibits a lawyer from establishing an "office or other systematic and continuous presence in this jurisdiction for the practice of law." That includes the practice of law of State A from Missouri. Lawyer does not meet any of the exceptions in 4-5.5(c) and is required to seek admission in Missouri. See also Informal Opinions 20030078, 980219, 980062, 980010, 970098, 960276, 960055, 940092, and 930152*."
    ii. The Informal Opinion references Missouri Rule 4-5.5(c), which states:[50]
        1. "*(c) A lawyer admitted and authorized to practice law in another United States jurisdiction and not disbarred or suspended from practice in any*

jurisdiction may provide legal services on a temporary basis in this jurisdiction that:

a. *(1) are undertaken in association with a lawyer who is admitted to practice in this jurisdiction and who actively participates in the matter;*
b. *(2) are in or reasonably related to a pending or potential proceeding before a tribunal in this or another jurisdiction if the lawyer or a person the lawyer is assisting is authorized by law or order to appear in such proceeding or reasonably expects to be so authorized;*
c. *(3) are in or reasonably related to a pending or potential arbitration, mediation, or other alternative dispute resolution proceeding in this or another jurisdiction if the services arise out of or are reasonably related to the lawyer's practice in a jurisdiction in which the lawyer is admitted and authorized to practice law and are not services for which the forum requires pro hac vice admission;*
d. *(4) are provided to the lawyer's employer or its organizational affiliates and are not services for which the forum requires pro hac vice admission; or*
e. *(5) are not within Rule 4-5.5(c)(2), (c)(3), or (c)(4) and arise out of or are reasonably related to the lawyer's practice in a jurisdiction in which the lawyer is admitted and authorized to practice law.*"

iii. Based upon the Missouri informal opinion, it appears that remote work for the attorneys Admitted State from their home in Missouri would not be permissible without being admitted in Missouri, or having Missouri co-counsel for the matters worked on while in Missouri. This highlights the need for attorneys to review the statutes and opinions of their Non-Licensed State, as Missouri's opinion appears to be in direct contrast to ABA Opinion 495 and the general trend of other states.

e. **Virginia Ethics Opinion Gives Liberal Authority to Practice Remotely.**
   i. Virginia issued an ethics opinion on September 19, 2011[51] that broadly permitted attorneys who were not licensed in Virginia to practice from their homes in Virginia, stating:
      1. "*Foreign lawyers, i.e., non-Virginia lawyers admitted to practice in the United States or a foreign nation, may practice in a Virginia law firm or may establish an office or other systematic and continuous presence in Virginia if authorized by Virginia or federal law… Likewise, if their practice is limited to matters involving the law of the state or country in which they are admitted to practice, foreign lawyers may practice in Virginia on a systematic and continuous basis…*"
   ii. After the COVID-19 pandemic, Virginia released a second ethics opinion[52] directly addressing remote work, stating:
      1. "*In Legal Ethics Opinion 1856 (approved by the Supreme Court of Virginia November 2, 2016), the committee addressed several questions about multijurisdictional practice under Rule of Professional Conduct 5.5; specifically, what types of practice foreign lawyers may engage in while located in Virginia. This opinion reiterates that guidance to conclude that a foreign lawyer may work remotely in Virginia (from home or otherwise), for any length of time, with or without an emergency justification to do so, as long as the work done involves the practice of the law of the foreign*

lawyer's licensing jurisdiction or exclusively federal law that does not require Virginia licensure. ***The foreign lawyer must avoid holding out or implying licensure in Virginia but otherwise may have a public presence in Virginia and is not required to be "invisible" within the state.*** [emphasis added]"

iii. The opinions in Virginia appear to provide attorneys with broader discretion to practice in the state. So long as the attorney is working on matters from their Admitted State, and does not hold out that they are licensed in Virginia, they are even permitted to have a public presence in the state.

f. **State Opinions Consider Where the Client is Located.**

i. While several of the state opinions refer to the same standard as ABA Opinion 495 concerning "…*held himself or herself out*…" they add two additional important points. First, the client served is in another jurisdiction. So, for example, if a lawyer has a second home in the Non-Licensed State and works on a matter for a client in their Admitted State, that would seem not to raise an issue. But if the client is in the Non-Licensed State, a problem may be triggered. What if the client also has a vacation home in the Non-Licensed State, and is located in the Non-Licensed State at the time the attorney sends the communication? Further, if the attorney's firm had attorneys admitted to practice in the Non-Licensed State, the same attorney might potentially create an issue by working on that matter from their Admitted State home because of the partners the firm has admitted in the Non-Licensed State. To raise an issue with the same work because it was done in the Non-Licensed State instead would not seem to provide any better protection for the client in the Non-Licensed State. How might or should such a standard be applied?

g. **What Constitutes a "Systematic and Continuous Presence?"**

i. The second factor raised in several state opinions discussed above may raise a potentially nettlesome issue. If an attorney licensed in their Admitted State and employed by a firm with an office and presence in the Admitted State works only from home located in the Non-Licensed State, that initially may seem to be acceptable under the ABA Opinion 495 standards. However, if that attorney practices solely from her home the "systematic and continuous presence" criteria may be violated. But with remote work how can someone working from home (or even a vacation or winter home) avoid having a "systematic and continuous presence"? Does that mean that full time or regular remote work in any state that applies this standard may not be feasible unless licensed in the Non-Licensed State? How might that generally be applied to an attorney practicing in their Non-Licensed State, such as where they maintain a home or vacation home, for a practice in their Admitted State?

12. **<u>Use of Artificial Intelligence ("AI") by Law Firms Affects Cybersecurity.</u>**

a. **Challenges of Protecting Privacy in an AI World.**

i. The speed of technological innovation made possible through large data sets and AI exacerbates challenges in protecting client's confidential data in the digital world.

ii. Consider:

1. The predominant business model of most technology companies is based on harvesting, analyzing, *and selling* mass amounts of personal and non-personal information.
2. The impact of emerging technologies, especially AI, blurring the lines between online and offline harms; and

3. Cybersecurity threats posed by Spyware specifically targeted at undermining our digital privacy.

b. **Dangers of AI Use by Lawyers.**

i. The ease of creating content through AI means causes a siren temptation for shortcuts excused as efficiency. In *Mata v. Avianca, Inc.*,[53] lawyers failed to investigate the generative AI application ChatGPT before adopting it for legal research and citing in a court filing the authorities cited by ChatGPT that existed only as ChatGPT's fictitious outputs.

1. Statements made by the lawyers at a sanctions hearing indicated that they misunderstood how ChatGPT produced its outputs and had not verified the accuracy of each ChaptGPT output before using it as their own work. To exacerbate their problem, they did not take advantage of the reply brief and court orders to correct their misplaced reliance on the ChatGPT output. One of the lawyers mistakenly thought that ChatGPT was a "super search engine." When complying with the court order to produce the cases, the lawyer relied once again on ChatGPT.
2. This creation of false information is called a "hallucination" in the AI model, and poses a significant threat to practitioners.

ii. These results can occur based on the internal instructions that an AI legal tool might be given by its developers to guide it towards "helpfully" answering a legal question that a user submits. Such instructions are generally not visible to users but could contain built-in priorities about what precedents to favor, what follow up questions (if any) to ask the user, how much detail to provide in the output, or what details should be emphasized. These factors will then serve as the foundation for the creation of the answer and consequentially shape, perhaps wrongly, an understanding of what the law is on a given topic and how that law is best described.

iii. This does not mean that ChatGPT and similar AI programs cannot be used for legal research and other legal tasks, but lawyers must ensure that the use is appropriate for client work, basing that determination on a careful examination of AI's capabilities and known faults while taking measures to avert or mitigate the adverse effects of those faults. Any materials generated by AI should be carefully reviewed to determine if the information is correct, citations are to real cases (and that those cases have been shepardized), etc.

iv. One example of the inability to blindly trust AI involves the AI stock Nvidia. Nvidia computer chips are used by AI developers in building generative AI systems. Yet research firms have breached vulnerabilities in the chips.[54]

c. **ABA Formal Opinion 512 Addresses Ethical Use of AI.**

i. ABA Formal Opinion 512[55] addresses ethical considerations on the use of generative artificial intelligence ("GAI") tools in law practice.

ii. Opinion 512 notes that "*…Model Rule 1.1 obligates lawyers to provide competent representation to clients*." The opinion states that attorneys need to have a "*…reasonable understanding of the capabilities and limitations of the specific GAI technology that the lawyer might use…*"

iii. With the speed at which AI is evolving, what level of research and review is sufficient to have a "reasonable understanding"? Opinion 512 acknowledges the speed of change, and recommends that attorneys keep abreast of developments, reading materials on AI products designed for the legal profession, and consulting with individuals proficient in AI technologies.

iv. Practitioners may consider having a consultation with an IT individual with expertise in AI, and have that consultant communicate regarding the actions the practitioner and their firm are taking regarding AI, as well as any further suggestions the consultant may have. The practitioner can then have periodic update meetings with an AI consultant. If further communications (email for example) are provided this could create a record of the actions the firm has taken, and the implementation (or not) of any recommendations the consultant provided.

d. **Confidentiality and AI.**
   i. RPC 1.6 requires attorneys to protect their clients' information.
   ii. AI uses "machine learning" to improve the AI and create more comprehensive responses to queries. This is done through retaining any information provided to the AI model. For a non-subscription-based service, it is likely all information provided is included in an online database for machine learning purposes. So, if an attorney were to use a free AI, and included confidential client information in the query, that would potentially violate their ethical obligations under RPC 1.6.
   iii. As a result of the above attorneys may wish to avoid using any AI they have not paid a subscription for. In addition, practitioners should consider reviewing the provider's terms of service ("TOS") to determine if the practitioner believes, based on their "reasonable understanding," that client data will be protected. Alternatively, or in addition, it may be worthwhile having a tech consultant confirm that confidential client data is protected when using the AI program, and save that communication to corroborate in the future the reasonableness of the practitioner's actions.
   iv. Practitioners should understand that some/many AI models not only search the internet for information but scour the firm's own database/network for information. That can be incredibly powerful especially for a larger or older firm that has massive electronic file databases that would be impractical to search efficiently for information by other means. But that access to the firm's confidential data is a potential exposure point many are not aware of.

e. **Basic Steps to Consider Regarding the Safe use of AI.**
   i. Undertaking a thorough due diligence check on the generative AI application to determine how the application could advance work done for a client consistent with counsel's professional obligations — i.e., know what is being used and how it works.
   ii. Reading key documentation on the developer's website that describes the application, how the application works, what it was designed to do, its current limitations and deficiencies, and any possibility of putting at risk a client's interests, like the possibility of generating inaccurate outputs. Review such resources as the developer's Terms of Use, Frequently or Commonly Asked Questions ("FAQs"), and any System Cards, which explain, for example, a generative AI's performance, capabilities, and limitations.
   iii. Seek out reviews and undertaking tests to identify inaccurate or biased results and training users about known indicia of inaccurate and biased outputs to help users recognize and remediate those deficiencies.
   iv. Examine how use of the technology could pose security risks, including collection and processing of data that could compromise client confidentiality, inadvertently waive attorney-client or attorney work product privileges, and compromise the enforceability of client trade secrets and opportunity to file

timely patent applications. *These risks must be able to be averted or the AI cannot be used.*

v. Considering carefully whether introduction of the technology might cause counsel to violate ethical obligations to (i) provide competent representation to clients, (ii) inform clients and obtain their consent to the use, (iii) protect client confidential information, and (iv) avoid unauthorized practice.

vi. Create a short memorandum to file listing the steps taken in due diligence, to reflect that the practitioner took "reasonable efforts," see RPC 1.6 discussion above, when analyzing the AI program used.

f. **Additional Guidelines for the Use of AI Systems.**

i. It would seem reasonable that a lawyer conducting due diligence on the prudence of using certain AI in practice would consider a Blueprint for AI issued by the White House in October 2022.[56] The "bill of rights" included the following points:

1. AI systems should be safe and effective;
2. Algorithms should not discriminate, and AI systems should be designed and used in equitable ways;
3. Data practices should protect privacy;
4. Design and use of AI should be disclosed and explained in plain language; and
5. There should be a human alternative and human backstop to AI applications.

ii. The Florida Bar recently released a guide on getting started with AI.[57] This information is valuable for practitioners in all jurisdictions to read.

1. The guide includes a list of current AI models that exist, a glossary of certain AI terms, a discussion on how to craft prompts for queries to receive more concise answers, the kinds of tasks AI can currently assist with, and more.
2. The guide notes that Florida practitioners should not use free AI software, "*…Free General AI models may use your questions and uploaded documents to train future models. To maintain client confidentiality, you will need a paid subscription…*"
3. For any practitioner that has not researched AI before, this guide can be used as a starting point to determine if they wish to begin implementing AI, which kinds of models they wish to look further into, and provides more comprehensive resources to review for further research.

13. **<u>Conclusion</u>**.

a. Technology continues to evolve at an ever-faster pace. The programs, and the uses of those programs, discussed in this paper are a small sample size of the myriad of products and potential applications that the modern estate planning firm can employ to protect their client's confidential client information in the digital age.

b. Practitioners should be diligent and thoughtful when employing new technology in their practices. Consider "beta testing" the programs before wide dissemination is performed to ensure that there are no unexpected side effects to use of new technology that could open the firm to issues or liability concerns.

c. It's extremely difficult to keep up with the dizzying pace of change related to technology. There are companies that can help you with all of these decisions. Lawyers always want their clients to ask for help when dealing with areas of unfamiliarity; and they should be mindful to follow their own advice as it relates to technology.

d. When a practitioner decides to work remotely, while ABA Opinion 495 and state opinions provide useful guidance with the evolution of technology and law practice it may already

be difficult, even precarious, to merely apply these standards. In addition, as ABA Opinion 495 leaves the issue to each state, attorneys should consider reviewing whether there are any local ethics opinions in any states in which they intend to remotely practice. With the rapid changes in technology, societal norms, and other factors attorneys should stay abreast of journal articles and new ethics opinions addressing remote work and related issues.

---

[1] The authors acknowledge that materials in this paper have been adapted from the following articles: (1) 45th Notre Dame Tax & Estate Planning Institute, "Using Technology for the Modern Estate Planning Practice," presented by Thomas A. Tietz and Martin M. Shenkman, South Bend, IN (September 27, 2019), (2) E-Report, American Bar Association, "What Estate Planners Should Tell Clients about Security Including Cybersecurity?," authored by Thomas A. Tietz, Brian Cluxton and Martin M. Shenkman, (2025 Winter Issue), and (3) Estate Planning Magazine, "Remote Work and ABA Ethics Opinions 495: Applying Ethics Standards in an Evolving Environment," authored by Rachel Wasserman, Thomas Tietz, Esq. and Martin M. Shenkman, Esq., 52 ETPL 8 (May 2025).

[2] https://www.fincen.gov/sites/default/files/2024-12/Press-Release-for-Interagency-Statement-on-Elder-Fraud-FINAL-508C.pdf issued Dec. 4, 2024, accessed August 10, 2025.

[3] See https://taxpolicycenter.org/briefing-book/how-many-people-pay-estate-tax, accessed August 10, 2025

[4] See https://www.lawsitesblog.com/tech-competence, accessed August 15, 2025.

[5] https://founderreports.com/return-to-office-statistics/, accessed August 11, 2025.

[6] "ABA Survey: Most Lawyers Want Options for Remote Work, Court and Conferences," AM. BAR. ASS'N (Sept. 28, 2022), https://www.americanbar.org/news/abanews/aba-news-archives/2022/09/aba-survey-lawyers-remote-work/, accessed August 11, 2025.

[7] Ethics Opinion 477R updates Ethics Opinion 99-413 to reflect the now common use of technology such as tablet devices, smartphones, and cloud storage.

[8] Comment 8 of RPC 1.1.

[9] For information from the Cybersecurity & Infrastructure Security Agency, see https://www.cisa.gov/cybersecurity-training-exercises, accessed August 10, 2025.

[10] For an excellent explanation of this, see Everything You Need to Know About Password Managers by Andrew Chaikivsky for Consumer Reports on February 7, 2017 - https://www.consumerreports.org/electronics-computers/password-managers/how-to-use-a-password-manager-a7687059222/, accessed August 15, 2025.

[11] ABA Formal Opinion 511 (May 8, 2024), https://www.lawnext.com/wp-content/uploads/2024/05/aba-formal-opinion-511.pdf, accessed August 12, 2025.

[12] RPC 5.1(a).

[13] RPC 5.3(a).

[14] RPC 5.3(c)(1).

[15] RPC 1.15.

[16] Examples of companies that perform these services include: Iron Mountain https://solutions.ironmountain.com/ and Shred-It https://www.shredit.com/en-us/secure-shredding-services/hard-drive-destruction, accessed August 15, 2025.

[17] See NYSBA Ethics Opinion 842 (9/10/10).

[18] RPC 1.6.

[19] RPC 1.6, Comment 18, paragraph (c).

[20] For examples of 10 encrypted USB drives, see https://buyersguide.org/encrypted-USB/t/best, accessed August 10, 2025.

[21] For a discussion on the origin of this quote, see https://taosecurity.blogspot.com/2018/12/the-origin-of-quote-there-are-two-types.html, accessed August 12, 2025.

[22] ABA formal opinion 483.
[23] One example would be implementing Endpoint Detection and Response technology, https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response, accessed August 10, 2025.
[24] https://www.prnewswire.com/news-releases/slashnexts-2023-state-of-phishing-report-reveals-a-1-265-increase-in-phishing-emails-since-the-launch-of-chatgpt-in-november-2022--signaling-a-new-era-of-cybercrime-fueled-by-generative-ai-301971557.html, accessed August 10, 2025.
[25] https://www.prnewswire.com/news-releases/slashnexts-2024-phishing-intelligence-report-shows-credential-phishing-attacks-increased-by-703-in-the-second-half-of-the-year-302334475.html, accessed August 10, 2025.
[26] For an article providing additional examples of phishing attacks, including pictures of samples, see https://www.csoonline.com/article/514515/what-is-phishing-examples-types-and-techniques.html, accessed on August 10, 2025.
[27] For further discussion of QR-ishing, see https://medium.com/it-security-in-plain-english/understanding-qr-code-phishing-qrishing-2ab6c79ce9ba, accessed August 10, 2025.
[28] https://www.proofpoint.com/us/threat-reference/social-engineering, accessed August 15, 2025
[29] For a discussion on how the casinos were breached, see https://www.cybersecuritydive.com/news/mgm-caesars-attacks-social-engineering/693956/, accessed August 10, 2025.
[30] For articles that discuss EDR in more detail, see https://www.gartner.com/reviews/market/endpoint-protection-platforms, accessed August 10, 2025.
https://www.sentinelone.com/cybersecurity-101/endpoint-security/what-is-endpoint-detection-and-response-edr/, accessed August 10, 2025.
[31] https://www.securitymagazine.com/articles/100765-78-of-people-use-the-same-password-across-multiple-accounts, accessed August 10, 2025.
[32] The 2024 internet crime report, released on April 23, 2025, can be viewed at https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf, accessed August 10, 2025.
[33] https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report, accessed August 10, 2025.
[34] "SURVEY: Consumers Are Ignoring Cybersecurity Risks Despite Identify Theft Concerns," https://news.nationwide.com/survey-consumers-are-ignoring-cybersecurity-risks-despite-identify-theft-concerns/ created September 29,2024, accessed August 10, 2024.
[35] Fiserv, "Consumers' Awareness, Behavior and Concerns Around Cybersecurity," https://merchants.fiserv.com/content/dam/firstdata/us/en/cybersecurity-awareness-insights-study/pdf/FDC_Cybersecurity_and_Awareness_eBook.pdf, accessed August 10, 2025
[36] For an article providing further discussion on free versus paid email systems, see https://www.techradar.com/pro/software-services/free-secure-email-vs-paid-secure-email-what-are-the-differences, accessed on August 10, 2025.
[37] The 2023 Cybersecurity Tech Report by the American Bar Association can be viewed at https://www.americanbar.org/groups/law_practice/resources/tech-report/2023/2023-cybersecurity-techreport/ accessed August 10, 2025.
[38] https://www.kaspersky.com/resource-center/definitions/what-is-wardriving, accessed August 10, 2025.
[39] For additional discussion on firewalls, see https://help.ui.com/hc/en-us/articles/115006615247-Intro-to-Networking-Network-Firewall-Security, accessed August 10, 2025.
[40] https://www.newsweek.com/how-cyber-thieves-use-your-smart-fridge-door-your-data-1603488, accessed August 10, 2025.
[41] See ABA Comm. on Ethics & Pro. Resp., Formal Op. 495 (2020), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-495.pdf (discussing lawyers working remotely), accessed August 15, 2025.

[42] Informal Opinion Number: 2024-12, adopted August 8, 2024, viewed at https://news.mobar.org/ethics-fourteen-new-informal-advisory-opinion-summaries-published/ accessed August 10, 2025.
[43] https://www.regus.com/en-us/virtual-offices/business-address, accessed August 11, 2025
[44] *Disputing the Law Firm Model*, RIMON L., https://www.rimonlaw.com/disrupting-the-law-firm-model/, accessed August 11, 2025.
[45] Manuel Lamiroy, "How lawyers communicate with clients," Feb. 29, 2024, https://www.lamiroy.com/blog/how-lawyers-communicate-with-clients/, accessed August 11, 2025.
[46] Bd. of Overseers of the Bar, Pro. Ethics Comm'n, Op. 189 (2005).
[47] N.J. Comm. on the Unauthorized Prac. of L. & Advisory Comm. on Pro. Ethics, Joint Op. 59/742 (2021), https://www.njcourts.gov/sites/default/files/notices/2021/10/n211007c.pdf., accessed August 11, 2025.
[48] D.C. Ct. App. Comm. on Unauthorized Prac. of L., Op. 24-20 (2020), https://www.dccourts.gov/sites/default/files/2020-03/CUPL-Opinion-24-20.pdf, accessed August 11, 2025.
[49] Informal Opinion Number: 2024-03, adopted January 23, 2024, viewed at https://mo-legal-ethics.org/informal-opinion/2024-03/, accessed August 11, 2025.
[50] Missouri Supreme Court Rule 4-5.5, https://www.courts.mo.gov/courts/clerkhandbooksp2rulesonly.nsf/c0c6ffa99df4993f86256ba50057dcb8/84187ab9f9f1995486256ca600521226?OpenDocument, accessed August 11, 2025.
[51] Va. Legal Ethics Op. 1856 (2011), https://www.vacle.org/opinions/1856.htm (approved by the Supreme Court of Virginia), accessed August 11, 2025.
[52] Va.Legal Ethics Op.1896 (2022), https://www.vacle.org/opinions/1896.htm (approved by the Supreme Court of Virginia), accessed August 11, 2025.
[53] Mata v. Avianca, Inc. (No. 22-cv-1461 (PKC), 2023 U.S. Dist. LEXIS 108263, at *4 (S.D.N.Y. June 22, 2023).
[54] See https://www.wiz.io/blog/wiz-research-critical-nvidia-ai-vulnerability, accessed August 12, 2025.
[55] ABA Standing Committee on Ethics and Professional Responsibility Formal Opinion 512, released July 29, 2024, viewed at https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf, accessed August 15, 2025.
[56] WHITE HOUSE OFF. OF SCI. & TECH. POL'Y, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE 3 (Oct. 2022), https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/, accessed August 12, 2025.
[57] "The Florida Bar Guide to Getting Started with AI," released January 7, 2025, viewable at https://www.legalfuel.com/guide-to-getting-started-with-ai/, accessed on August 10, 2025.