USCIT Judicial Conference

The Ethics of Electronic Information and Working in a Virtual Environment

October 27, 2022

The Ethics of Electronic Information and Working in a Virtual Environment

Panelists

Hon. Leo M. Gordon
U.S. Court of International Trade

Simeon Yerokun
Crowell & Moring LLP

Tracy Kepler
CNA Insurance

Stephen P. Vaughn
King & Spalding, LLP

Disclaimer

- This is not legal advice, nor should it be considered legal advice.
- This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.
- This presentation is offered for educational and informational uses only.

Cyber Attacks on Law Firms

The Numbers

- According to PwC Law Firm's Survey in 2020, cyber risk is the second greatest threat to law firms since 2020 after Covid-19.
- An ABA Report from 2020 showed that 29% of law firms reported a security breach, and 35% reported malware infections.
- 71% of the Top 100 firms said they were "somewhat concerned" or "extremely concerned" about cybersecurity threats.
- **The problem is only 22% of Top 100 firms have a Cybersecurity Committee.**

It is critical that law firms follow ethical guidelines

- Law firms are specific targets for cyber hacks.
- Failure to respond properly to a cyber incident can open a firm to serious ethical issues.
- **Firms are ethically obligated to protect this sensitive data, offering cybercriminals the opportunity for a quick payout**.
- Law firms are also managed by attorneys who usually have little to no background and experience with cybersecurity matters.

Why are law firms major targets for cyber attacks?

- Law firms have money, house valuable, confidential client information, and are usually not prepared for a cyber attack.

- In July 2021, Campbell Conroy & O'Neil announced that their "network was impacted by ransomware, which prevented access to certain files on the system."

- The firm could not confirm whether the bad actors viewed or accessed their client files, however, they did note that the "system included certain individuals' names, dates of birth, driver's license numbers/state identification numbers, financial account information, Social Security numbers, passport numbers, payment card information, medical information, health insurance information, biometric data, and/or online account credentials (i.e., usernames and passwords)."

Security measures that firms should implement

- As technology continues to evolve, firms must implement robust security measures, as not doing so means easier access to sensitive information for cyber criminals.
- Law firms tend to implement weaker security measures, which provides hackers increased accessibility to sensitive information.
- As a result, law firms are increasingly targeted by hackers seeking client information.

Who Attacks Firms?

- There is a wide variety of hackers with their own skill-sets and motivations

- Examples of distinct groups include:

1. Nation States
2. Non-state organizations, including criminal enterprises, terrorist groups, and sophisticated hacker communities
3. “Lone-wolf ” hackers and insiders

Firm Liability

- Law firms may be increasingly liable for client's damages resulting from a cyber attack.
- Statutes can vary widely from state to state on issues such as notification to law enforcement, and Congress has yet to pass a national data breach notification law.
- This means law firms and other businesses that possess private client information on firm networks must be prepared to meet the data breach notification requirements of any jurisdiction in which they do business, including internationally.

ABA 2021 Report on Cybersecurity

- The ABA produced a 2021 Legal Technology Survey Report that “explores security threats and safeguards that reporting attorneys and their law firms are using to protect against them.”

- Some key takeaways from the report:

1. Consequences of data breaches included: downtime/loss of billable hours (36%); consulting fees for repair (31%); destruction or loss of files (13%); replacement of hardware/software (18%).
2. 24% of firms noted that they had to notify a client or clients of the breach.
3. 42% of firms noted that they had cyber liability insurance.

Data Breach Cases

- Major cases focus on data leaks, failure to secure information, failure to supervise, discovery issues, and malpractice issues
  - Understand scope and purpose of data breach investigation
    - Remediation v. obtaining legal advice
    - Impact on discoverability of investigation's report and attendant communications

Ethics Rules

American Bar Association Model Rules of Professional Conduct

Rule 1.1 – Competence

Rule 1.3 – Diligence

Rule 1.4 – Communication with Clients

Rule 1.6 – Confidentiality

Rule 4.4 – Respect for Rights of Third Person

Rule 5.1 – Responsibilities of a Partner or Supervisory Lawyer

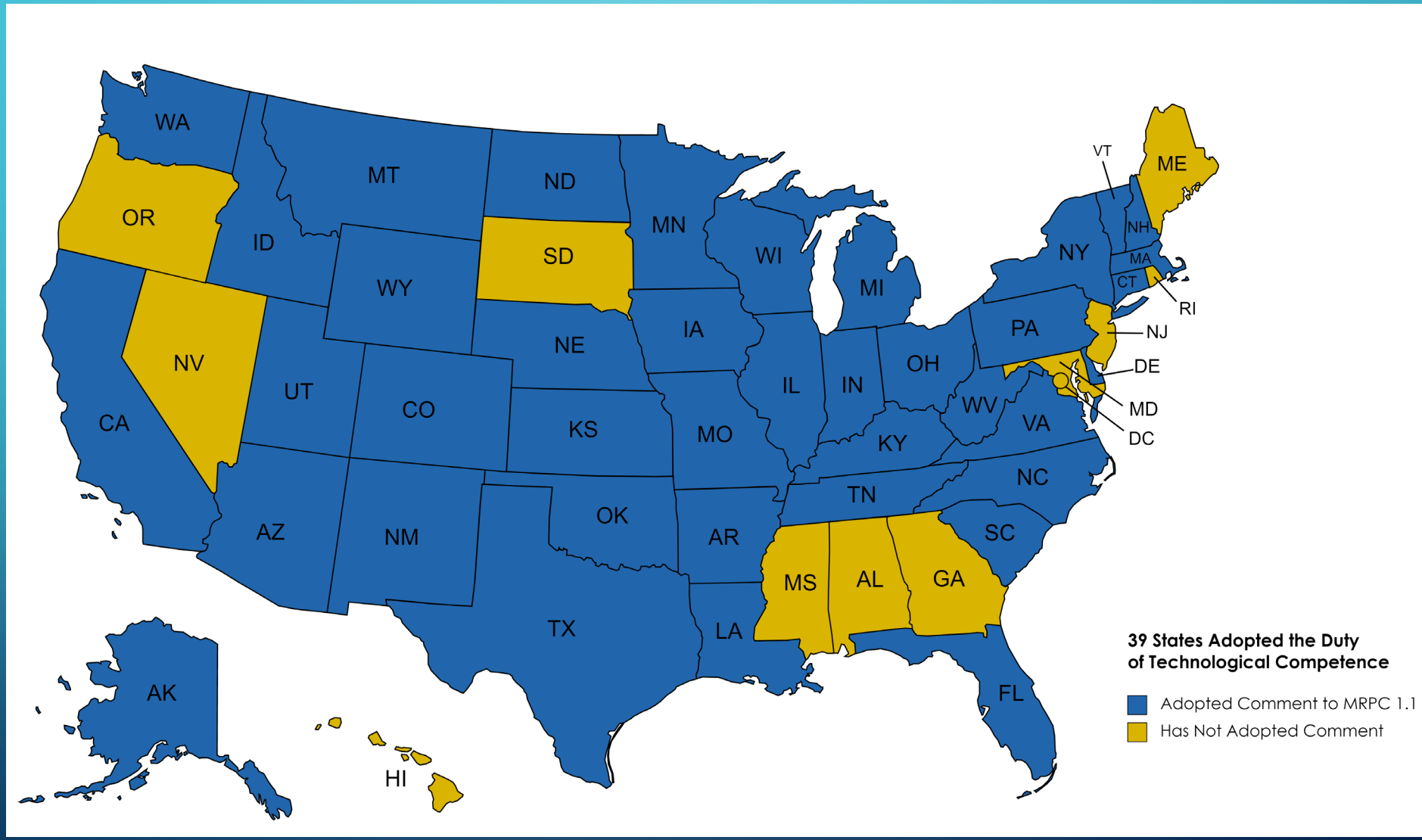
Rule 5.2 – Responsibilities of a Subordinate Lawyer

Rule 5.3 – Responsibilities Regarding Non-Lawyer Assistance

Competence and Supervision

- **The "Technology" Amendments to the Rules of Professional Conduct**
  - Some states have not adopted a duty of technological competence
- **The Baseline Knowledge of Technology to be a Competent Attorney**
  - CA Ethics Opinion 2015-193 and the Handling of Electronically Stored Information
  - Duty to Supervise Lawyers and Non-Lawyers
- **Competence in Dealing with New Technologies**
  - The Ethical Challenges of Integrating Artificial Intelligence into the Practice of Law
  - How the Ethically Competent Attorney Should Respond to New Technology

MRPC 1.1 - Adopted by 39 States & Counting



Model Rule 1.1 – Duty of Competence

- Model Rule 1.1.
  - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

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

Example

A lawyer would have difficulty providing competent legal services in today's environment without knowing how to efficiently use email or create an electronic document.

Competence: Baseline Knowledge Resources

California State Bar Standing Committee on Professional Responsibility and Conduct states in Formal Opinion No. 2015-193 (June 30, 2015) that attorneys should have technical competence and skill – either by themselves, co-counsel, or expert consultants.

https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINAL.pdf

Competence: Baseline Knowledge Resources

- S.L. Klevens & A. Clair, "The Evolving Duty of Competence in the Digital Age," *N.J.L.J.* (Mar. 24, 2021), The Evolving Duty of Competence in the Digital Age | New Jersey Law Journal

- Selected Sedona Conference Working Group Series Publications (May 2021), Publications_Catalogue_May_2021.pdf (thesedonaconference.org)

Competence: Baseline Knowledge Resources

- *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263 (2020), https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary

- A. Tadler, *et al., The Sedona Conference "Jumpstart Outline": Questions to Ask Your Client & Your Adversary to Prepare for Preservation, Rule 26 Obligations, Court Conferences & Requests for Production* (Mar. 2016 version), Microsoft Word - 10 Jumpstart Outline - Tadler et al Final Gen Use (thesedonaconference.org)

Model Rule 1.3 - Diligence

- Model Rule 1.3
  - A lawyer shall act with reasonable diligence and promptness in representing a client.

Model Rule 1.4 - Communications

- Model Rule 1.4(a)(1)
  - A lawyer shall promptly inform the client of any decision or circumstance with respect to which the client's informed consent…is required by these rules.
- Model Rule 1.4(a)(3)
  - A lawyer shall keep the client reasonably informed about the status of the matter.
- Model Rule 1.4(a)(4)
  - A lawyer shall promptly comply with reasonable requests for information.
- Model Rule 1.4(b)
  - A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

Model Rule 1.4 - Communications

- Comments:
  - [1]: Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.
  - [4]: When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request.
  - [5]: The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so.
  - [7]: In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication...A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person.

Model Rule 1.6 – Confidentiality of Information

- Model Rule 1.6(a)
  - A lawyer shall not reveal information relating to the representation of a client unless certain circumstances arise.
- Model Rule 1.6(c)
  - Lawyers must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client.
  - Comment [18]: The unauthorized access to, or the inadvertent disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

“Reasonable Efforts” Definition

- Comment [18] includes non-exclusive factors as a guide for lawyers in making a “reasonable effort”
  - The sensitivity of the information,
  - The likelihood of disclosure if additional safeguards are not employed,
  - The cost of employing additional safeguards,
  - The difficulty of implementing the safeguards, and
  - The extent to which the safeguards adversely affect the lawyer’s ability to represent clients.
- Comment [19]
  - When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.
  - This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy.

Model Rule 4.4 – Respect for Rights of Third Person

- Model Rule 4.4(b)
  - A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.
    - Comment [2]: Paragraph (b) recognizes that lawyers sometimes receive a document or electronically stored information that was mistakenly sent or produced by opposing parties or their lawyers… If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures.
    - Comment [3]: Some lawyers may choose to return a document or delete electronically stored information unread, for example, when the lawyer learns before receiving it that it was inadvertently sent.

Model Rule 5.1 – Responsibilities of a Partner or Supervisory Lawyer

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

Model Rule 5.1 – Responsibilities of a Partner or Supervisory Lawyer

- Comment [2]
  - Paragraph (a) requires lawyers with managerial authority within a firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Rules of Professional Conduct. Such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.

Model Rule 5.2 – Responsibilities of a Subordinate Lawyer

(a) A lawyer is bound by the Rules of Professional Conduct notwithstanding that the lawyer acted at the direction of another person.

(b) A subordinate lawyer does not violate the Rules of Professional Conduct if that lawyer acts in accordance with a supervisory lawyer's reasonable resolution of an arguable question of professional duty.

Model Rule 5.3 – Responsibilities Regarding Non-Lawyer Assistance

With respect to a non-lawyer employed or retained by or associated with a lawyer:

(a) A partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

(b) A lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

Model Rule 5.3 – Responsibilities Regarding Non-Lawyer Assistance

(c) A lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Model Rule 5.3 – Responsibilities Regarding Non-Lawyer Assistance

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

Model Rule 5.3 – Responsibilities Regarding Non-Lawyer Assistance

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

Model Rule 5.3 – Responsibilities Regarding Non-Lawyer Assistance

- Comment [2], cont'd
  - A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations.

Model Rule 5.3 – Responsibilities Regarding Non-Lawyer Assistance

- Comment [3]
  - The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the non-lawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) unauthorized practice of law.
  - When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the non-lawyer's conduct is compatible with the professional obligations of the lawyer.

Model Rule 5.3 – Responsibilities Regarding Non-Lawyer Assistance

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

Competence: Duty to Supervise

NY *RPC* 5.3(a):

"A law firm shall ensure that the work of nonlawyers who work for the firm is adequately supervised, as appropriate. A lawyer with direct supervisory authority over a nonlawyer shall adequately supervise the work of the nonlawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter and the likelihood that ethical problems might arise in the course of working on the matter."

Competence: Duty to Supervise

ISBA Professional Conduct Advisory Opinion No. 16-06 (Oct. 2016), https://www.isba.org/sites/default/files/ethicsopinions/16-06.pdf

"At the outset *** lawyers must conduct a due diligence investigation when selecting a provider. Reasonable inquiries and practices could include:

"1. Reviewing cloud computing industry standards and familiarizing oneself with the appropriate safeguards that should be employed;

2. Investigating whether the provider has implemented reasonable security precautions to protect client data from inadvertent disclosures, including but not limited to the use of firewalls, password protections, and encryption;

3. Investigating the provider's reputation and history;

Competence: Duty to Supervise

4. Inquiring as to whether the provider has experienced any breaches of security and if so, investigating those breaches;

5. Requiring an agreement to reasonably ensure that the provider will abide by the lawyer's duties of confidentiality and will immediately notify the lawyer of any breaches or outside requests for client information;

6. Requiring that all data is appropriately backed up completely under the lawyer's control so that the lawyer will have a method for retrieval of the data;

7. Requiring provisions for the reasonable retrieval of information if the agreement is terminated or if the provider goes out of business."

Competence: Duty to Supervise

Office of Disciplinary Counsel v. Krzton, No. 2802, (Aug. 6, 2021), *available at* *https://*wwwsecure.pacourts.us/assets/opinions/DisciplinaryBoard/out/86DB2020-Krzton.pdf?cb=1 (attorney suspended for 6 months for failure to properly supervise assistant who stole close to $200,000 from clients' estate accounts).

Competence: New Technology

Other “new” technologies include:

- Virtual meeting platforms
- Ephemeral messaging apps
- Social media platforms

Competence: New Technology

Attorneys and Security Requirements – Dealing with New Technologies:

- What is the existing technology framework?
- Who decides what new technology is needed?
- Who incorporates the new technology?
  - Internal?
  - Third Party?
- Who has access to the new technology?
- Who monitors the new technology?
- What is the audit trail for the new technology?

Competence: New Technology

ABA House of Delegates Resolution 112 (adopted as revised at the August 12-13, 2019 Annual Meeting), https://www.americanbar.org/content/dam/aba/images/news/2019/08/am-hod-resolutions/112.pdf:

"RESOLVED, That the American Bar Association urges courts and lawyers to address the emerging ethical and legal issues related to the usage of artificial intelligence ('AI') in the practice of law including: (1) bias, explainability, and transparency of automated decisions made by AI; (2) ethical and beneficial usage of AI; and (3) controls and oversight of AI and the vendors that provide AI."

Dealing with service providers

- Cyber risks that flow from trusted service providers
  - E.g., Payroll and timekeeping providers, healthcare providers
  - Contract management software companies – remote work environments

Improving Cyber and Digital Awareness

Improving Cyber and Digital Awareness

- Guidance on protection of information
- Importance of data privacy and technology use policies
- Creation of a culture of cyber and digital awareness and reporting
  - Leadership counts – modeling from the top matters
  - Work technology v. personal technology
  - Issues of remote work
  - Education programs
  - Policy creating, testing, and review

Bar Association Ethics Opinions

“Cloud computing” while keeping client information confidential

- “Cloud computing” is where remote servers are networked so data storage can be shared within large groups. Lawyers need to take reasonable precautions and must ensure that there is “adequate access” to the client’s information where it is stored remotely, the service provider has “adequate security,” and the confidentiality of the client’s information is maintained.
- Florida Bar Ethics Opinion 12-3 (2013).

Using the internet as a means to transmit information relating to the representation of a client

- Under Model Rule 1.1, a lawyer has a duty to understand the “benefits and risks associated with relevant technology.”
- Model Rule 1.6(c) states that a lawyer must make “reasonable efforts” to prevent unauthorized access or disclosure of a client’s information.
- Under Model Rule 1.4, a lawyer may be required to inform the client of security safeguards. A lawyer can use the internet to transmit client information as long as reasonable efforts were made to prevent unauthorized access to said information.
- American Bar Association Formal Opinion 477R (2017).

Lawyer's obligations after an electronic data breach or cyberattack

- "Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes. Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be."
- ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018)

Virtual Practice

- The opinion states that "...w*hen practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies."*
- Attorneys have ethical and common law duties, and contractual and regulatory duties that require them to take competent and reasonable measures to safeguard information relating to clients.
- ABA Formal Opinion 498 (February 2021)

Competence: Remote Practice of Law

"A lawyer's duty to provide competent representation includes the obligation to understand the risks and benefits of technology, which this Committee and numerous other similar committees believe includes the obligation to understand or to take reasonable measures to use appropriate technology to protect the confidentiality of communications in both physical and electronic form."

PA Bar Association Formal Op. 2020-300 at 4

Competence: Remote Practice of Law

"a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, must make reasonable efforts to ensure that the firm has in effect requirements that any staff, consultants or other entities that have or may have access to confidential client information or data comply with the Rules of Professional Conduct with regard to data access from remote locations and that any discussions regarding client-related matters are done confidentially."

PA Bar Association Formal Opinion 2020-300 at 7

Competence: Remote Practice of Law

- “Hard/Software Systems”
- “Accessing Client Files and Data”
- “Virtual Meeting Platforms and Videoconferencing”
- “Virtual Document and Data Exchange Platforms”
- “Smart Speakers, Virtual Assistants, and Other Listening-Enabled Devices”
- “Supervision”

ABA Formal Opinion 498, “Virtual Practice” (ABA: Mar. 10, 2021), aba-formal-opinion-498.pdf (practicesource.com)

Competence: Remote Practice of Law Resources

- "Key Takeaways from the Cybersecurity Thought Leadership Conf. of the Tech. and the Legal Prof. Comm. of the NY State Bar Ass'n" (Feb. 3, 2020), https://nysba.org/app/uploads/2020/02/FINAL-NYSBA-Cyber-Key-Takeaways-13120.pdf
- "Cybersecurity Alert: Tips for Working Securely While Working Remotely Issued by the Tech. and the Legal Prof. Comm. of the NY State Bar Ass'n" (Mar. 12, 2020), https://nysba.org/app/uploads/2020/03/NYSBA-Cyber-Alert-031220.pdf

Competence: Remote Practice of Law Resources

- "Cybersecurity Alert: Discovery of Recordings from Virtual Meeting Platforms Issued by the Tech. and the Legal Prof. Comm. of the NY State Bar Ass'n" (June 25, 2020), https://nysba.org/app/uploads/2020/06/NYSBA-Virtual-Meetings-Alert-062520.pdf
- "Cybersecurity Alert: Tips for Purchasing Cyber Insurance Issued by the Tech. and the Legal Prof. Comm. of the NY State Bar Ass'n" (July 6, 2020), https://nysba.org/app/uploads/2020/07/FINAL-NYSBA-Cyber-Insurance-Application-Alert-70820.pdf

Competence: Remote Practice of Law Resources

- “Ethics in the COVID-19 Pandemic” (Michigan State Bar: Undated), https://www.michbar.org/opinions/ethics/COVID-19
- “Coronavirus Response: Legal Ethics FAQ” (Oregon State Bar: Undated), https://www.osbar.org/_docs/resources/CoronavirusEthicsFAQ.pdf

Competence: Remote Practice of Law Resources

- R. Rosensweig, *Unauthorized Practice of Law: Rule 5.5 in the Age of COVID-19 and Beyond*, ABA (Aug. 12, 2020), *available at* https://www.americanbar.org/groups/litigation/committees/ethics-professionalism/articles/2020/unauthorized-practice-of-law-rule-55-in-the-age-of-covid-19-and-beyond/
- *The Florida Bar Re: Advisory Opinion—Out-Of-State Attorney Working Remotely from Florida Home,* No. SC20-1220 (Fl. Sup. Ct. May 20, 2021)

Competence: Remote Practice of Law Resources

- Formal Op. 754-2020, Ethical Obligations when Lawyers Work Remotely" (NYCLA Comm. on Prof. Ethics), NYCLA Op. 754-2020 - Ethical Obligations when Lawyers Work Remotely.pdf
- Formal Op. 2020-300, "Ethical Obligations for Lawyers Working Remotely" (Pa. Bar Ass'n Comm. on Legal Ethics and Prof. Responsibility: Apr. 10, 2020), http://www.pabar.org/members/catalogs/Ethics%20Opinions/formal/F2020-300.pdf
- C.H. Cohen & C. Yang, "New Normal of Remote Lawyering Has Ethical Implications," *N.Y.S.B.A.J.* 30 (May/June 2021), New Normal of Remote Lawyering Has Ethical Implications - New York State Bar Association (nysba.org)

Ethical Implications, Etc. Resources

- *The Sedona Conference Primer on Social Media, Second Edition* (Aug. 2019), https://thesedonaconference.org/download-publication?fid=4508
- "Best Practices for Professional Electronic Communication" (Florida Bar: Updated Nov. 2019), https://www-media.floridabar.org/uploads/2019/11/Professional_Electronic_Communications_Best_Practices.pdf
- *NYSBA Social Media Ethics Guidelines* (Release Date June 20, 2019) ("*NYSBA Guidelines*"), http://www.nysba.org/socialmediaguidelines/

Ethical Implications, Etc. Resources

- C.M. Chiccine, "Model Rules on Attorney Advertising Streamlined: Rules 7.1 through 7.5 are streamlined and clarified to keep pace with technology," *Litigation News* (ABA: Mar. 1, 2019), https://www.americanbar.org/groups/litigation/publications/litigation-news/featured-articles/2019/model-rules-attorney-advertising-streamlined/
- California State Bar Standing Comm. on Prof. Responsibility & Conduct Formal Opinion 2016-196 ("Under what circumstances is 'blogging' by an attorney a 'communication' subject to the requirements and restrictions of the Rules of Professional Conduct and related provisions of the State Bar Act regulating attorney advertising") (footnotes omitted), http://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/CAL%202016-196%20[12-0006]%20Blogging.pdf

Ethical Implications, Etc. Resources

- New Jersey Supreme Court Advisory Committee on Professional Ethics Opinion 735 (June 25, 2019) ("Lawyer's Use of Internet Search Engine Keyword Advertising"), https://www.njcourts.gov/notices/2019/n190806c.pdf
- D.C. Manning & K.B. Rockwood, "Emoticons and Emojis: Hazards to be Aware of in Discovery," *New Jersey Lawyer* 68 (Apr. 2019), https://community.njsba.com/blogs/njsba-staff/2019/04/12/emoticons-and-emojis-hazards-to-be-aware-of-in-dis?ssopc=1

Ethical Implications, Etc. Resources Electronic Filing

- *Two-Way Media LLC v. AT&T, Inc*., 782 F.3d 1311, 1316 (Fed. Cir. 2015) ("In this era of electronic filing—post-dating by some 60 years the era in which the cases cited by the dissent were issued—we find no abuse of discretion in a district court's decision to impose an obligation to monitor an electronic docket for entry of an order which a party and its counsel already have in their possession ***.")
- *Emerald Coast Utilities Auth. v. Bear Marcus Pointe, LLC,* Case No. 1D15-5714, 2017 WL 4448526 (Fla. 1st Dist. Ct. App. Oct. 6, 2017) (*per curiam*) ("Counsel have a duty to have sufficient procedures and protocols in place to ensure timely notice of appealable orders.")
- *Krivak v. Home Depot U.S.A., Inc.,* No. 20-1276 (7th Cir. June 17, 2021) (affirming dismissal of action for failure of counsel to prosecute and to "exercise diligence in monitoring" scheduling obligations)

Ethical Implications, Etc. Resources Electronic Filing

- "Judiciary Addresses Cybersecurity Breach: Extra Safeguards to Protect Sensitive Court Records," *United States Courts* (Jan. 6, 2021), Judiciary Addresses Cybersecurity Breach: Extra Safeguards to Protect Sensitive Court Records | United States Courts (uscourts.gov)
- "Highly Sensitive Document Procedures and Court Orders," *United States Courts* (last updated Apr. 1, 2021), Highly Sensitive Document Procedures and Court Orders | United States Courts (uscourts.gov)
- New Jersey Adv. Comm. on Prof. Ethics Opinion. 734 (Sept. 9, 2018), "Ethical Responsibilities of Lawyers Who Use Third Party Vendors to Electronically File Documents," https://njlaw.rutgers.edu/collections/ethics/acpe/acp734_1.html

Insurance

- What can you do to protect yourself when the inevitable occurs?
- Intersection of professional liability policies and cyber insurance policies.
- Cost vs. scope of coverage
- Impact of rising number of claims
- Risk vs. catastrophic risk
- Ransomware payments:

  The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) advisory around ransomware payments (October 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Real-World Examples

Targeted attacks are increasing

- In 2021, 80% of law firms reported phishing attempts. (InfoSecurity North America)
- The FBI has reported that law firms are often viewed as “one-stop shops” for attackers (with information on multiple clients), and it has seen hundreds of law firms being increasingly targeted by hackers. (American Bar Association)
  - Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more).

Seyfarth Shaw LLP & Fragomen, Del Rey, Bernsen & Loewy LLP

- Both BigLaw firms announced security incidents, involving a malware attack that risked clients' sensitive information.
- In the Seyfarth case, the ransomware attack involved criminals freezing the victims out of the network and demanding payment to restore access. The firm reported it had restored all critical systems and that no client/firm data was accessed.
- In the Fragomen data breach, an "unauthorized third party" gained access to a file with the employment eligibility data of Google staffers. This breach was most likely caused by credential compromise rather than malware.

Cadwalader, Wickersham & Taft

- This firm issued a notice that stated that one of its third-party vendors, TBG West Insurance, suffered a ransomware attack on March 27, 2020.
- What happened?
  - The attack encrypted files within its system.
  - In July 2020, the vendor informed Cadwalader that some of its current and past employee social security numbers might have been exposed.
  - However, the firm also stated that the vendor breach did not impact their firm's systems or any client data.
- What was the result?
  - In the end, the vendor "paid the ransom to regain access to their data."
- What did the vendor and firm do?
  - The vendor made changes that would boost their security
  - All residents that were potentially affected were sent notices by July 30, 2020.
  - Additionally, Cadwalader noted that they were evaluating their own assessments of vendor security in response to the attack.

Key Takeaways

- Reasonable diligence to secure the confidentiality of confidential client information should be practiced by lawyers working remotely.
- Portable electronic devices should not contain client information, or the devices should be able to remotely deactivated and scrubbed.
- The laws of jurisdictions in which you practice, and your clients do business should be consulted.
- “Different states may vary in their interpretation of lawyers’ professional responsibilities regarding data breaches.”