The Twenty-First Century Lawyer's Evolving Ethical Duty of Competence

Andrew Perlman
Professor of Law, Suffolk University Law School

120 Tremont Street
Boston, MA 02108

www.law.suffolk.edu

The Twenty-First Century Lawyer's Evolving Ethical Duty of Competence

By Andrew Perlman

Andrew Perlman is a professor at Suffolk University Law School, where he is the Director of the Institute on Law Practice Technology and Innovation. He was the Chief Reporter of the ABA Commission on Ethics 20/20 and is the Vice Chair of the newly created ABA Commission on the Future of Legal Services. This article contains the author's own opinions and does not reflect the views of any ABA entity or any other organization with which he is or has been affiliated.

Just twenty years ago, lawyers were not expected to know how to protect confidential information from cybersecurity threats, use the Internet for marketing and investigations, employ cloud-based services to manage a practice and interact with clients, implement automated document assembly and expert systems to reduce costs, or engage in electronic discovery. Today, these skills are increasingly essential, and many lawyers want to know whether they are adapting quickly enough to satisfy their ethical duty of competence. This short article describes several relevant recent changes to the Model Rules of Professional Conduct and identifies new skills and knowledge that lawyers should have or develop.

The Duty of Competence in a Digital Age

The ABA Commission on Ethics 20/20 was created in 2009 to study how the Model Rules of Professional Conduct should be updated in light of globalization and changes in technology. The resulting amendments addressed (among other subjects) a lawyer's duty of confidentiality in a digital age, numerous issues related to the use of Internet-based client development tools, the ethics of outsourcing, the facilitation of jurisdictional mobility for both US and foreign lawyers, and the scope of the duty of confidentiality when changing firms.

One overarching theme of the Commission's work was that twenty-first century lawyers have a heightened duty to keep up with technology. An amendment to Model Rule 1.1 (Duty of Competence), Comment [8] captured the new reality (italicized language is new):

> 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.

The Model Rules had not previously mentioned technology, and the Commission concluded that the Rules should reflect technology's growing importance to the delivery of legal and law-related services.

New Competencies for the Twenty-First Century Lawyer

The advice to keep abreast of relevant technology is vague, and the Commission intended for it to be so. The Commission understood that a competent lawyer's skillset needs to evolve along with technology itself. After all, given the pace of change in the last twenty years, the specific skills lawyers will need in the decades ahead are difficult to imagine.[1] In the meantime, a few new competencies appear to be critical.

Cybersecurity

Long gone are the days when lawyers could satisfy their duty of confidentiality by placing client documents in a locked file cabinet behind a locked office door. Lawyers now store a range of information in the "cloud" (both private and public) as well as on the "ground," using smartphones, laptops, tablets, and flash drives. This information is easily lost or stolen; it can be accessed without authority (e.g., through hacking); it can be inadvertently sent; it can be intercepted while in transit; and it can even be accessed without permission by foreign governments or the National Security Agency.[2]

In light of these dangers, lawyers need to understand how to competently safeguard confidential information. Newly adopted Model Rule 1.6(c) requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." New comments advise lawyers to examine a number of factors when determining whether their efforts are "reasonable," including (but not limited to) "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."

The particular safeguards lawyers need to use will necessarily change with time. For now, and at a minimum, competent lawyers need to understand the importance of strong passwords (lengthy passwords that contain a mix of letters, numbers, and special characters; the word "password," for example, is a lousy password), encryption (both for information stored in the "cloud" and on the "ground," such as on flash drives and laptops), and multifactor authentication (ensuring that data can be accessed only if the lawyer has the correct password as well as another form of identification, such as a code sent by text message to the lawyer's mobile phone). Lawyers also need to understand what metadata is and how to get rid of it, how to avoid phishing scams, the dangers of using public computers and Wi-Fi connections (including cloning and twinning of public Wi-Fi networks), the risks of using file sharing sites, and how to protect devices against malware.

Law firms with internal networks (also sometimes referred to as private clouds) should consult with competent data security experts to safeguard the information, and law firms that outsource these services (i.e., use a public cloud to store client data) need to ensure they select a service that uses appropriate security protocols. Recent changes to Rule 5.3, Comment [3] offer additional guidance on these issues, as do numerous ethics opinions related to cloud computing.[3] A growing body of federal and state law also governs the area.

In sum, basic knowledge of cybersecurity has become an essential lawyer competency. Although lawyers cannot guard against every conceivable cybersecurity threat, they must take reasonable precautions. Failing to do so threatens the confidentiality of clients' information and puts lawyers at a heightened risk of discipline or malpractice claims.

Electronic Discovery

A sound grasp of e-discovery has become a necessity, especially for litigators, and lawyers face discipline and sanctions if they do not understand the basics of electronically stored information (ESI) or fail to collaborate with those who do. For example, a Massachusetts lawyer was recently disciplined for failing to take appropriate steps to prevent a client's spoliation of ESI.[4] In addition to violating Rule 1.4 (for failing to communicate to his client the nature of the discovery obligations) and Rule 3.4 (for unlawfully obstructing access to evidence), the lawyer was found to have violated Rule 1.1 because he represented a client on "a matter that he was not competent to handle without adequate research or associating with or conferring with experienced counsel, and without any attempt to confirm the nature and content of the proposed deletions [of electronically stored information by the client]."[5]

In New York, e-discovery competence is now mandated in section 202.12(b) of the Uniform Rules for the Supreme and County Courts:

> Where a case is reasonably likely to include electronic discovery, counsel shall, prior to the preliminary conference, confer with regard to any anticipated electronic discovery issues. Further, counsel for all parties who appear at the preliminary conference must be sufficiently versed in matters relating to their clients' technological systems to discuss competently all issues relating to electronic discovery: counsel may bring a client representative or outside expert to assist in such e-discovery discussions.[6]

In California, a recently released draft of an ethics opinion covers similar ground and once again emphasizes the importance of e-discovery competence:

> Attorney competence related to litigation generally requires, at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, i.e., the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a given matter and the nature of the ESI involved. Such competency requirements may render an otherwise highly experienced attorney not competent to handle certain litigation matters involving ESI.[7]

Competence is not the only ethical duty at stake. The California draft opinion (like the Massachusetts disciplinary case) observes that the improper handling of e-discovery "can also result, in certain circumstances, in ethical violations of an attorney's duty of confidentiality, the duty of candor, and/or the ethical duty not to suppress evidence."[8] The opinion concludes that, if lawyers want to handle matters involving e-discovery and do not have the requisite competence to do so, they can either "(1) acquire sufficient learning and skill before performance is required; [or] (2) associate with or consult technical consultants or competent counsel. . . ." [9]

Related issues arise when lawyers advise their clients about social media content that might be discoverable. Recent opinions suggest that lawyers must competently advise clients about this content, such as whether they can change their privacy settings or remove posts, while avoiding any advice that might result in the spoliation of evidence.[10] The bottom line is that e-discovery is a new and increasingly essential competency, and unless litigators understand it or associate with those who do, they risk court sanctions and discipline.

Internet-Based Investigations

Lawyers no longer need to rely exclusively on private investigators to uncover a wealth of factual information about a legal matter. Lawyers can learn a great deal from simple Internet searches.

Lawyers ignore this competency at their peril. Consider an Iowa lawyer whose client received an email from Nigeria, informing him that he stood to inherit nearly $19 million from a distant Nigerian relative by paying $177,660 in taxes owed to the Nigerian government. The client's gullible lawyer raised the "tax" money from other clients in exchange for a promise to give them a cut of the inheritance. Unsurprisingly, the "inheritance" was a well-known scam, and the lawyer's clients lost their money. The lawyer was disciplined for subjecting his clients to the fraud and was expressly criticized for failing to conduct a "cursory internet search" that would have uncovered the truth.[11]

Internet research is also essential in more routine settings. For example, the Missouri Supreme Court recently held that lawyers should use "reasonable efforts," including Internet-based tools, to uncover the litigation history of jurors prior to trial in order to preserve possible objections to the empanelment of those jurors.[12] In Maryland, a court favorably cited a passage from a law review article that asserted that "[i]t should now be a matter of professional competence for attorneys to take the time to investigate social networking sites."[13] Other cases have emphasized the importance of using simple Internet searches to find missing witnesses and parties. Simply put, lawyers cannot just stick their heads in the sand when it comes to Internet investigations.

At the same time, lawyers need to be aware of the ethics issues involved with these kinds of investigations, especially when researching opposing parties, witnesses, and jurors. If the information is publicly available, these investigations raise few concerns. But when lawyers want to view information that requires a request for access, such as by "friending" the target of the investigation, a number of potential ethics issues arise under Model Rules 4.1, 4.2, and 4.3. A rapidly growing body of ethics opinions addresses these issues, including a recent ABA Formal Opinion.[14]

Internet-Based Marketing

A growing number of lawyers use Internet-based marketing, such as social media (e.g., blogs, Facebook, Twitter, and LinkedIn), pay-per-lead services (paying a third party for each new client lead generated), and pay-per-click tools (e.g., paying Google for clicks taking Internet users to the law firm's website). Given the increasing prevalence of these tools, lawyers need to understand how to use them properly.

A recent Indiana disciplinary matter illustrates one potential risk. A lawyer with over 40 years of experience and no disciplinary record received a private reprimand for using a pay-per-lead service whose advertisements failed to comply with the Indiana Rules of Professional Conduct. The Indiana Supreme Court concluded that the lawyer should have known about the improper marketing methods and stopped using the company's services.[15] The takeaway message is that lawyers need to understand how these new marketing arrangements operate and cannot ignore how client leads are generated on their behalf.

Even when lawyers take control of their own online marketing, they need to tread carefully. Potential issues include the inadvertent creation of an attorney-client relationship under Rule 1.18, the unauthorized practice of law under Rule 5.5 (when the marketing attracts clients in states where the lawyer is not licensed), and allegations of improper solicitation under Rule 7.3. (Newly adopted comments in Rules 1.18 and 7.3 can help lawyers navigate some of these issues.)

Leveraging New and Established Legal Technology/Innovation

Technological competence is not just a disciplinary or malpractice concern. It is becoming essential in a marketplace where clients handle more of their own legal work and use non-traditional legal service providers (i.e., providers other than law firms). To compete, lawyers need to learn how to leverage "New Law" – technology and other innovations that facilitate the delivery of legal services in entirely new ways. Lawyers are also being pressed to make better use of well-established technologies, such as word processing.

Examples of "New Law" include automated document assembly, expert systems (e.g., automated processes that generate legal conclusions after users answer a series of branching questions), knowledge management (e.g., tools that enable lawyers to find information efficiently within a lawyer's own firm, such as by locating a pre-existing document addressing a legal issue or identifying a lawyer who is already expert in the subject), legal analytics (e.g., using "big data" to help forecast the outcome of cases and determine their settlement value), virtual legal services, and cloud-based law practice management. These kinds of tools can be identified and implemented effectively through the sound application of legal project management and process improvement techniques (which reflect another set of important new competencies). Lawyers are not ethically required to use these tools and skills, at least not yet. But if lawyers want to remain competitive in a rapidly changing marketplace, these competencies are quickly becoming essential.

Clients also have less patience with lawyers who fail to use well-established legal technology appropriately.[16] For instance, a corporate counsel at Kia Motors America (Casey Flaherty) has conducted "technology audits" of outside law firms to ensure they make efficient and effective use of available tools, such as word processing and spreadsheets. He has found they do not. On average, tasks that lawyers should have been able to perform in an hour took them five. (Casey Flaherty has partnered with my law school to automate the audit so that it can be used widely throughout the legal industry. I am working closely with Casey on the project.) Lawyers who fail to develop (or maintain) competence when using these established technologies risk alienating both existing and potential clients.

Conclusion

The seemingly minor change to a Comment to Rule 1.1 captures an important shift in thinking about competent twenty-first century lawyering. Technology is playing an ever more important role, and lawyers who fail to keep abreast of new developments face a heightened risk of discipline or malpractice as well as formidable new challenges in an increasingly crowded and competitive legal marketplace.

Endnotes

1. *See generally*RICHARD SUSSKIND, TOMORROW'S LAWYERS: AN INTRODUCTION TO YOUR FUTURE (2013).
2. James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES (Feb. 15, 2014), http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html.
3. *See, e.g.*, *Cloud Ethics Opinions Around the U.S.*, A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited Oct. 6, 2014).
4. Kenneth Paul Reisman, Public Reprimand, No. 2013-21, 2013 WL 5967131 (Mass. B. Disp. Bd. Oct. 9, 2013).
5. *Id*. at *2.
6. N.Y. UNIF. R. TRIAL CT. §202.12(b), *available at*http://www.nycourts.gov/rules/trialcourts/202.shtml#12 (last visited Oct. 7, 2014).
7. State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 11-0004 (2014).
8. *Id.*
9. *Id.*
10. NYCLA Comm. on Prof'l Ethics, Formal Op. 745 (2013); Phila. Bar Ass'n Prof'l Guidance Comm., Formal Op. 2014-5 (2014).
11. Iowa Supreme Court Att'y Disciplinary Bd. v. Wright, 840 N.W.2d 295, 301-04 (Iowa 2013).
12. Johnson v. McCullough, 306 S.W.3d 551, 558-59 (Mo. 2010).
13. Griffin v. Maryland, 995 A.2d 791, 801 (Md. Ct. Spec. App. 2010) (quoting Sharon Nelson et al., *The Legal Implications of Social Networking*, 22 REGENT U. L. REV. 1, 13 (2009-2010)), *rev'd on other grounds*, Griffin v. State, 419 Md. 343 (Md. 2011).
14. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 466 (2014).
15. *In re* Anonymous, 6 N.E.3d 903, 907 (Ind. 2014).
16. Casey Flaherty, *Could You Pass This In-House Counsel's Tech Test? If the Answer Is No, You May Be Losing Business*, A.B.A. J. (Jun. 17, 2013, 1:30 PM), http://www.abajournal.com/legalrebels/article/could_you_pass_this_in-house_counsels_tech_test.

TELEWORK ESSENTIALS TOOLKIT

EXECUTIVE LEADERS

DRIVE CYBERSECURITY STRATEGY, INVESTMENT, CULTURE

After rapidly adopting wide-scale remote work practices in response to COVID-19, organizations have started planning for more permanent and strategic teleworking postures. An organization's executive leaders, IT professionals, and teleworkers all have roles to play in the shift from temporary to long-term or permanent telework strategies. The Cybersecurity and Infrastructure Security Agency (CISA) is providing these recommendations to support organizations in re-evaluating and strengthening their cybersecurity as they transition to long-term telework solutions.

ACTIONS

1 ORGANIZATIONAL POLICIES AND PROCEDURES

Review and update organizational policies and procedures to address the cybersecurity considerations raised by the shift to a remote workforce. Clearly communicate new remote work expectations and security requirements to the workforce. (STRATEGIC)

- National Cyber Security Alliance
- NIST Special Publication (SP) 800-46: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
- CISA Telework Guidance and Resources
- CISA Cyber Essentials Toolkit 1
- Cyber Readiness Institute Remote Work Resources: Securing a Remote Workforce and Making Your Remote Workforce Cyber Ready

2 CYBERSECURITY TRAINING REQUIREMENTS

Implement cybersecurity training requirements for your organization to improve working knowledge of cybersecurity concepts, current threats, and trends to empower workforce decision making when accessing organizational systems and data remotely. (STRATEGIC)

- CISA Cyber Essentials
- CISA Cyber Essentials Toolkit 2
- Cyber Readiness Institute Cyber Readiness Program

3 MOVING ORGANIZATIONAL ASSETS

Determine the cybersecurity risks associated with moving organizational assets beyond the traditional perimeter to activities not accessible by the organization's monitoring and response capabilities (e.g., printing at home, use of personal email accounts, use of personal devices, use of personal mobile devices). Develop, implement, and enforce enterprise-wide policies that address the threats and vulnerabilities presented by the new extended perimeter. These policies should include requirements for workers to securely configure and update corporate devices, personal devices, mobile devices, and home networks. (STRATEGIC)

- CISA and NSA Telework Best Practices
- NSA Telework and Mobile Security Guidance
- Cyber Readiness Institute Remote Work Resources: Top Three Dos & Don'ts for Remote Workers, Securing a Remote Workforce, and Making Your Remote Workforce Cyber Ready
- NIST National Cybersecurity Center of Excellence Mobile Device Security Guidance

4 CYBER SECURE, HYBRID CULTURE

Create a cyber secure, hybrid culture that includes remote employees, on-premise employees, and employees who may do both. Ensure policies focus on human behavior, address the basics in cyber hygiene—such as phishing, software updates, passwords/authentication, USB use, and removable media— and are clear, updated, and communicated to the workforce regularly. (STRATEGIC)

- Cyber Readiness Institute Cyber Readiness Program
- Cyber Readiness Institute Remote Work Resources: Creating a Cyber Ready Culture in Your Remote Workforce: Five Tips

As the Nation's risk advisor, CISA has compiled telework guidance to improve general cybersecurity posture. For the latest resources: CISA Telework Guidance

TELEWORK ESSENTIALS TOOLKIT

IT PROFESSIONALS

DEVELOP SECURITY AWARENESS AND VIGILANCE

After rapidly adopting wide-scale remote work practices in response to COVID-19, organizations have started planning for more permanent and strategic teleworking postures. An organization's executive leaders, IT professionals, and teleworkers all have roles to play in the shift from temporary to long-term or permanent telework strategies. The Cybersecurity and Infrastructure Security Agency (CISA) is providing these recommendations to support organizations in re-evaluating and strengthening their cybersecurity as they transition to long-term telework solutions.

ACTIONS

1 PATCHING AND VULNERABILITY MANAGEMENT

Ensure hardware and software inventories include new items added due to teleworking to ensure patching and vulnerability management are effective. Maintain patch and vulnerability management practices by keeping software up to date and scanning for vulnerabilities. Enable automatic software updates or use a managed solution wherever feasible. (TECHNICAL)

- CISA Tip on Understanding Patches and Updates
- GCA Cybersecurity Toolkit for Small Business: Know What You Have
- GCA Cybersecurity Toolkit for Small Business: Update your Defenses
- GCA Patch to Protect
- Cyber Readiness Institute Software Updates Guidance

2 ENTERPRISE CYBERSECURITY CONTROLS

Implement, maintain, and invest in enterprise cybersecurity controls to securely connect employees to the organization's network and assets. In modern IT environments, zero trust architecture may be preferable to virtual private network (VPN) solutions due to the lack of perimeter defense in cloud and distributed systems. Evaluate the current security architecture and ensure that it is properly protecting—and providing visibility into—remote sites and endpoints, including employees who may use public WiFi. (TECHNICAL)

- CISA Tip on Enterprise VPN Security
- NIST SP-800-207: Zero Trust Architecture
- GCA Public Wifi Wisdom

3 MULTI-FACTOR AUTHENTICATION

Enforce multi-factor authentication (MFA) for remote access to organizational systems and services. Develop contingency plans or solutions when MFA is not feasible or available. (TECHNICAL)

- CISA Tip on Supplementing Passwords with MFA
- CISA Guidance on MFA
- Work From Home Coalition Guidance on Enabling MFA on Microsoft Office and Google Suite
- GCA Cybersecurity Toolkit for Small Business: Beyond Simple Passwords
- Cyber Readiness Institute Authentication/ Passwords Guidance

4 ORGANIZATIONALLY APPROVED PRODUCTS

Maintain a list of organizationally approved products, including collaboration tools and teleconferencing applications. Provide users guidance on using these tools securely. (TACTICAL)

- CISA Tips for Video Conferencing
- CISA Guidance for Securing Video Conferencing
- CISA Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing
- GCA Cybersecurity Toolkit for Small Business: Know What You Have

5 FREQUENT BACKUPS

Perform frequent backups of the organization's systems and important files, verify backups regularly, and store backups offline and offsite. Prioritize protecting against ransomware attacks due to their potential for prolonged disruption in the telework environment. (TACTICAL/TECHNICAL)

- CISA Tip for Protecting Against Ransomware
- GCA Cybersecurity Toolkit for Small Business: Defend Against Ransomware (Backup)
- Cyber Readiness Institute Ransomware Playbook

6 DOMAIN-BASED MESSAGE AUTHENTICATION

Implement a Domain-Based Message Authentication, Reporting & Conformance (DMARC) validation system to address increased risk of phishing and business email compromise in remote working environments. (TECHNICAL)

- CISA Insights on Enhance Email & Web Security
- GCA Cybersecurity Toolkit for Small Business: Protect Your Email and Reputation

As the Nation's risk advisor, CISA has compiled telework guidance to improve general cybersecurity posture. For the latest resources: CISA Telework Guidance

TELEWORK ESSENTIALS TOOLKIT

TELEWORKERS – YOUR HOME NETWORK

DEVELOP SECURITY AWARENESS AND VIGILANCE

After rapidly adopting wide-scale remote work practices in response to COVID-19, organizations have started planning for more permanent and strategic teleworking postures. An organization's executive leaders, IT professionals, and teleworkers all have roles to play in the shift from temporary to long-term or permanent telework strategies. The Cybersecurity and Infrastructure Security Agency (CISA) is providing these recommendations to support organizations in re-evaluating and strengthening their cybersecurity as they transition to long-term telework solutions.

ACTIONS

1 CONFIGURED AND HARDENED

Ensure your home network is properly configured and hardened. Change all default passwords and use strong, complex passwords. Ensure your home wireless router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum and disable legacy protocols such as WEP and WPA. Ensure the wireless network name (service set identifier [SSID]) does not identify your physical location or router manufacturer/model. Use a protective Domain Name System (DNS) service. (TECHNICAL)

- CISA Tip on Securing Wireless Networks
- Center for Internet Security (CIS) Telework and Small Office Network Security Guide
- GCA Cybersecurity Toolkit for Small Business
- Work From Home Coalition Guidance

2 SECURE PRACTICES AND ORGANIZATIONAL POLICIES

Follow secure practices and organizational policies for handling sensitive data including: personally identifiable information (PII), protected health information (PHI), classified materials, intellectual property, and sensitive customer/client information. Avoid storing or transmitting sensitive organizational information on personal devices. If personal devices are approved for telework use, regularly apply the latest patch and security update on your devices. Follow your organization's guidance on securing your devices, including implementing basic security controls like password authentication and anti-virus software. (TACTICAL/TECHNICAL)

- Cyber Readiness Institute Data Protection Basics for Remote Workers
- Cyber Readiness Institute Authentication/Passwords Guidance
- GCA Cybersecurity Toolkit for Small Business

3 OPENING EMAIL ATTACHMENTS AN CLICKING LINKS

Use caution when opening email attachments and clicking links in emails. Increase your awareness of phishing tactics, current phishing campaigns, and social engineering to effectively report suspicious emails and communications. (TACTICAL)

- CISA Tip on Using Caution with Email Attachments
- Cyber Readiness Institute Phishing Guidance

4 COMMUNICATING SUSPICIOUS ACTIVITIES

Make sure you know the procedures for communicating suspicious activities to your organization's IT security team and promptly report all suspicious activity. (TACTICAL)

- Telework Security Basics

As the Nation's risk advisor, CISA has compiled telework guidance to improve general cybersecurity posture. For the latest resources: CISA Telework Guidance

PENNSYLVANIA BAR ASSOCIATION
COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY

April 10, 2020

FORMAL OPINION 2020-300

ETHICAL OBLIGATIONS FOR LAWYERS WORKING REMOTELY

I. Introduction and Summary

When Pennsylvania Governor Tom Wolf ordered all "non-essential businesses," including law firms to close their offices during the COVID-19 pandemic, and also ordered all persons residing in the state to stay at home and leave only under limited circumstances, many attorneys and their staff were forced to work from home for the first time. In many cases, attorneys and their staff were not prepared to work remotely from a home office, and numerous questions arose concerning their ethical obligations.

Most questions related to the use of technology, including email, cell phones, text messages, remote access, cloud computing, video chatting and teleconferencing. This Committee is therefore providing this guidance to the Bar about their and their staff's obligations not only during this crisis but also as a means to assure that attorneys prepare for other situations when they need to perform law firm- and client-related activities from home and other remote locations.

Attorneys and staff working remotely must consider the security and confidentiality of their client data, including the need to protect computer systems and physical files, and to ensure that telephone and other conversations and communications remain privileged.

In Formal Opinion 2011-200 (Cloud Computing/Software As A Service While Fulfilling The Duties of Confidentiality and Preservation of Client Property) and Formal Opinion 2010-100 (Ethical Obligations on Maintaining a Virtual Office for the Practice of Law in Pennsylvania), this Committee provided guidance to attorneys about their ethical obligations when using software and other technology to access confidential and sensitive information from outside of their physical offices, including when they operated their firms as virtual law offices. This Opinion affirms the conclusions of Opinions 2011-200 and 2010-100, including:

- An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.

- An attorney may maintain a virtual law office in Pennsylvania, including a virtual law office in which the attorney works from home, and associates work from their homes in various locations, including locations outside of Pennsylvania;

- An attorney practicing in a virtual office at which attorneys and clients do not generally meet face to face must take appropriate safeguards to: (1) confirm the identity of clients and others; and, (2) address those circumstances in which a client may have diminished capacity.

This Opinion also affirms and adopts the conclusions of the American Bar Association Standing Committee on Ethics and Professional Responsibility in Formal Opinion 477R (May 22, 2017) that:

> A lawyer generally may transmit information relating to the representation of a client over the [I]nternet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, 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.

The duty of technological competence requires attorneys to not only understand the risks and benefits of technology as it relates to the specifics of their practices, such as electronic discovery. This also requires attorneys to understand the general risks and benefits of technology, including the electronic transmission of confidential and sensitive data, and cybersecurity, and to take reasonable precautions to comply with this duty. In some cases, attorneys may have the requisite knowledge and skill to implement technological safeguards. In others, attorneys should consult with appropriate staff or other entities capable of providing the appropriate guidance.

At a minimum, when working remotely, attorneys and their staff have an obligation under the Rules of Professional Conduct to take reasonable precautions to assure that:

- All communications, including telephone calls, text messages, email, and video conferencing are conducted in a manner that minimizes the risk of inadvertent disclosure of confidential information;
- Information transmitted through the Internet is done in a manner that ensures the confidentiality of client communications and other sensitive data;
- Their remote workspaces are designed to prevent the disclosure of confidential information in both paper and electronic form;

- Proper procedures are used to secure and backup confidential data stored on electronic devices and in the cloud;
- Any remotely working staff are educated about and have the resources to make their work compliant with the Rules of Professional Conduct; and,
- Appropriate forms of data security are used.

In Section II, this Opinion highlights the Rules of Professional Conduct implicated when working at home or other locations outside of a traditional office. Section III highlights best practices and recommends the baseline at which attorneys and staff should operate to ensure confidentiality and meet their ethical obligations. This Opinion does not discuss specific products or make specific technological recommendations, however, because these products and services are updated frequently. Rather, Section III highlights considerations that will apply not only now but also in the future.

II. Discussion

A. Pennsylvania Rules of Professional Conduct

The issues in this Opinion implicate various Rules of Professional Conduct that affect an attorney's responsibilities towards clients, potential clients, other parties, and counsel, primarily focused on the need to assure confidentiality of client and sensitive information. Although no Pennsylvania Rule of Professional Conduct specifically addresses the ethical obligations of attorneys working remotely, the Committee's conclusions are based upon the existing Rules, including:

- Rule 1.1 ("Competence")
- Rule 1.6 ("Confidentiality of Information")
- Rule 5.1 ("Responsibilities of Partners, Managers, and Supervisory Lawyers")
- Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistance")

The Rules define the requirements and limitations on an attorney's conduct that may subject the attorney, and persons or entities supervised by the attorney, to disciplinary sanctions. Comments to the Rules assist attorneys in understanding or arguing the intention of the Rules, but are not enforceable in disciplinary proceedings.

B. Competence

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.

Rule 1.1 ("Competence") states in relevant part:

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

Further, Comment [8] to Rule 1.1 states

> 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. To provide competent representation, a lawyer should be familiar with policies of the courts in which the lawyer practices, which include the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania.

Consistent with this Rule, attorneys must evaluate, obtain, and utilize the technology necessary to assure that their communications remain confidential.

C. Confidentiality

An attorney working from home or another remote location is under the same obligations to maintain client confidentiality as is the attorney when working within a traditional physical office.

Rule 1.6 ("Confidentiality of Information") states in relevant part:

> (a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).
>
> …
>
> (d) 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.

Comments [25] and [26] to Rule 1.6 state:

> [25] Pursuant to paragraph (d), a lawyer should act in accordance with court policies governing disclosure of sensitive or confidential information, including the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania. Paragraph (d) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3. The

> unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (d) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].
>
> [26] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Comment [25] explains that an attorney's duty to understand the risks and benefits of technology includes the obligation to safeguard client information (1) against unauthorized access by third parties (2) against inadvertent or unauthorized disclosure by the lawyer or other persons subject to the lawyer's supervision. Comment [26] explains that an attorney must safeguard electronic communications, such as email, and may need to take additional measures to prevent information from being accessed by unauthorized persons. For example, this duty may require an attorney to use encrypted email, or to require the use of passwords to open attachments, or take other reasonable precautions to assure that the contents and attachments are seen only by authorized persons.

A lawyer's confidentiality obligations under Rule 1.6(d) are, of course, not limited to prudent employment of technology. Lawyers working from home may be required to bring paper files and other client-related documents into their homes or other remote locations. In these circumstances, they should make reasonable efforts to ensure that household residents or visitors who are not associated with the attorney's law practice do not have access to these items. This can be accomplished by maintaining the documents in a location where unauthorized persons are denied access, whether through the direction of a lawyer or otherwise.

D. Supervisory and Subordinate Lawyers

Rule 5.1 ("Responsibilities of Partners, Managers, and Supervisory Lawyers") states:

> (a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.
>
> (b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.
>
> (c) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:
>
> > (1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or
> >
> > (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistance") states:

> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> (a) a partner and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer.

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

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

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

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

Therefore, 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.

III. Best Practices When Performing Legal Work and Communications Remotely[1]

A. General Considerations

In Formal Opinion 2011-200, this Committee concluded that a lawyer's duty of competency extends "beyond protecting client information and confidentiality; it also includes a lawyer's ability to reliably access and provide information relevant to a client's case when needed. This is essential for attorneys regardless of whether data is stored onsite or offsite with a cloud service provider." When forced to work remotely, attorneys remain obligated to take reasonable precautions so that they are able to access client data and provide information to the client or to others, such as courts or opposing counsel.

While it is beyond the scope of this Opinion to make specific recommendations, the Rules and applicable Comments highlight that the need to maintain confidentiality is crucial to preservation of the attorney-client relationship, and that attorneys working remotely must take appropriate measures to protect confidential electronic communications. While the measures necessary to do so will vary, common considerations include:

[1] These various considerations and safeguards also apply to traditional law offices. The Committee is not suggesting that the failure to comply with the "best practices" described in Section III of this Opinion would necessarily constitute a violation of the Rules of Professional Conduct that would subject an attorney to discipline. Rather, compliance with these or similar recommendations would constitute the type of reasonable conduct envisioned by the Rules.

- Specifying how and where data created remotely will be stored and, if remotely, how the data will be backed up;
- Requiring the encryption or use of other security to assure that information sent by electronic mail are protected from unauthorized disclosure;
- Using firewalls, anti-virus and anti-malware software, and other similar products to prevent the loss or corruption of data;
- Limiting the information that may be handled remotely, as well as specifying which persons may use the information;
- Verifying the identity of individuals who access a firm's data from remote locations;
- Implementing a written work-from-home protocol to specify how to safeguard confidential business and personal information;
- Requiring the use of a Virtual Private Network or similar connection to access a firm's data;
- Requiring the use of two-factor authentication or similar safeguards;
- Supplying or requiring employees to use secure and encrypted laptops;
- Saving data permanently only on the office network, not personal devices, and if saved on personal devices, taking reasonable precautions to protect such information;
- Obtaining a written agreement from every employee that they will comply with the firm's data privacy, security, and confidentiality policies;
- Encrypting electronic records containing confidential data, including backups;
- Prohibiting the use of smart devices such as those offered by Amazon Alexa and Google voice assistants in locations where client-related conversations may occur;
- Requiring employees to have client-related conversations in locations where they cannot be overheard by other persons who are not authorized to hear this information; and,
- Taking other reasonable measures to assure that all confidential data are protected.

B. Confidential Communications Should be Private

1. Introduction

When working at home or from other remote locations, all communications with clients must be and remain confidential. This requirement applies to all forms of communications, including phone calls, email, chats, online conferencing and text messages.

Therefore, when speaking on a phone or having an online or similar conference, attorneys should dedicate a private area where they can communicate privately with clients, and take reasonable precautions to assure that others are not present and cannot listen to the conversation. For example, smart devices such as Amazon's Alexa and Google's voice assistants may listen to conversations and record them. Companies such as Google and Amazon maintain those recordings on servers and hire people to review the recordings. Although the identity of the

speakers is not disclosed to these reviewers, they might hear sufficient details to be able to connect a voice to a specific person.[2]

Similarly, when communicating using electronic mail, text messages, and other methods for transmitting confidential and sensitive data, attorneys must take reasonable precautions, which may include the use of encryption, to assure that unauthorized persons cannot intercept and read these communications.

2. What is Encryption?

Encryption is the method by which information is converted into a secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography. Unencrypted data is also known as plaintext, and encrypted data is called ciphertext. The formulas used to encode and decode messages are called encryption algorithms or ciphers.[3]

When an unauthorized person or entity accesses an encrypted message, phone call, document or computer file, the viewer will see a garbled result that cannot be understood without software to decrypt (remove) the encryption.

3. The Duty to Assure Confidentiality Depends Upon the Information Being Transmitted

This Opinion adopts the analysis of ABA Formal Opinion 477R concerning a lawyer's duty of confidentiality:

> At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.
>
> Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

[2] https://www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording

[3] https://searchsecurity.techtarget.com/definition/encryption

> . . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c)[4] includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In addition to the obligations under the Pennsylvania Rules of Professional Conduct, which are based upon the Model Rules, clients may also impose obligations upon attorneys to protect confidential or sensitive information. For example, some commercial clients, such as banks, routinely require that sensitive information be transmitted only with a password protocol or using an encryption method.

C. There Are Many Ways to Enhance Your Online Security

[4] Pennsylvania did not adopt Comment [18] in its entirety.

While this Opinion cannot provide guidance about specific products or services, its goal is to provide attorneys and law firms with guidance about how they can meet their obligation of competence while preserving client confidentiality. The following subsections of this Opinion outline some reasonable precautions that attorneys should consider using to meet their ethical obligations.

1. Avoid Using Public Internet/Free Wi-Fi

Attorneys should avoid using unsecured free Internet/Wi-Fi hotspots when performing client- or firm-related activities that involve access to or the transmission of confidential or sensitive data. Persons, commonly called hackers, can access every piece of unencrypted information you send out to the Internet, including email, credit card information and credentials used to access or login to businesses, including law firm networks. Hackers can also use an unsecured Wi-Fi connection to distribute malware. Once armed with the user's login information, the hacker may access data at any website the user accesses.

2. Use Virtual Private Networks (VPNs) to Enhance Security

A VPN, or Virtual Private Network, allows users to create a secure connection to another network over the Internet, shielding the user's activity from unauthorized persons or entities. VPNs can connect any device, including smartphones, PCs, laptops and tablets to another computer (called a server), encrypting information and shielding your online activity from all other persons or entities, including cybercriminals. Thus, the use of a VPN can help to protect computers and other devices from hackers.

3. Use Two-Factor or Multi-Factor Authentication

Two-Factor or Multi-Factor Authentication is a security method that requires users to prove their identity in more than one way before signing into a program or a website. For example, a user might require a login name and a password, and would then be sent a four- or six-digit code by text message to enter on the website. Entering this additional authentication helps to ensure only authorized persons are accessing the site. Although these forms of enhanced security may seem cumbersome, its use provides an additional layer of security beyond simple password security.

4. Use Strong Passwords to Protect Your Data and Devices

One of the most common ways that hackers break into computers, websites and other devices is by guessing passwords or using software that guesses passwords, which remain a critical method of gaining unauthorized access. Thus, the more complex the password, the less likely that an unauthorized user will access a phone, computer, website or network.

The best method to avoid having a password hacked is by using long and complex passwords. There are various schools of thought about what constitutes a strong or less-hackable password, but as a general rule, the longer and more complex the password, the less likely it will be cracked. In addition, mobile devices should also have a PIN, pass code or password. The devices

should lock/time out after a short period of time and require users to re-enter the PIN code or password.

5. Assure that Video Conferences are Secure

One method of communicating that has become more common is the use of videoconferencing (or video-teleconferencing) technology, which allows users to hold face-to-face meetings from different locations. For many law offices, the use of videoconferences has replaced traditional teleconferences, which did not have the video component.

As the popularity of videoconferencing has increased, so have the number of reported instances in which hackers hijack videoconferences. These incidents were of such concern that on March 30, 2020 the FBI issued a warning about teleconference hijacking during the COVID-19 pandemic[5] and recommended that users take the following steps "to mitigate teleconference hijacking threats:"

- Do not make meetings public;
- Require a meeting password or use other features that control the admittance of guests;
- Do not share a link to a teleconference on an unrestricted publicly available social media post;
- Provide the meeting link directly to specific people;
- Manage screensharing options. For example, many of these services allow the host to change screensharing to "Host Only;"
- Ensure users are using the updated version of remote access/meeting applications.

6. Backup Any Data Stored Remotely

Backups are as important at home as they are at the office, perhaps more so because office systems are almost always backed up in an automated fashion. Thus, attorneys and staff working remotely should either work remotely on the office's system (using services such as Windows Remote Desktop Connection, GoToMyPC or LogMeIn) or have a system in place that assures that there is a backup for all documents and other computer files created by attorneys and staff while working. Often, backup systems can include offsite locations. Alternatively, there are numerous providers that offer secure and easy-to-set-up cloud-based backup services.

7. Security is Essential for Remote Locations and Devices

Attorneys and staff must make reasonable efforts to assure that work product and confidential client information are confidential, regardless of where or how they are created. Microsoft has published its guidelines for a secure home office, which include:

[5] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic. Although the FBI warning related to Zoom, one brand of videoconferencing technology, the recommendations apply to any such service.

- Use a firewall;
- Keep all software up to date;
- Use antivirus software and keep it current;
- Use anti-malware software and keep it current;
- Do not open suspicious attachments or click unusual links in messages, email, tweets, posts, online ads;
- Avoid visiting websites that offer potentially illicit content;
- Do not use USBs, flash drives or other external devices unless you own them, or they are provided by a trusted source. When appropriate, attorneys should take reasonable precautions such as calling or contacting the sending or supplying party directly to assure the data are not infected or otherwise corrupted. [6]

8. Users Should Verify That Websites Have Enhanced Security

Attorneys and staff should be aware of and, whenever possible, only access websites that have enhanced security. The web address in the web browser window for such sites will begin with "HTTPS" rather than "HTTP." A website with the HTTPS web address uses the SSL/TLS protocol to encrypt communications so that hackers cannot steal data. The use of SSL/TLS security also confirms that a website's server (the computer that stores the website) is who it says it is, preventing users from logging into a site that is impersonating the real site.

9. Lawyers Should Be Cognizant of Their Obligation to Act with Civility

In 2000, the Pennsylvania Supreme Court adopted the Code of Civility, which applies to all judges and lawyers in Pennsylvania.[7] The Code is intended to remind lawyers of their obligation to treat the courts and their adversaries with courtesy and respect. During crises, the importance of the Code of Civility, and the need to comply with it, are of paramount importance.

During the COVID-19 pandemic, the Los Angeles County Bar Association Professional Responsibility and Ethics Committee issued a statement, which this Opinion adopts, including:

> In light of the unprecedented risks associated with the novel Coronavirus, we urge all lawyers to liberally exercise every professional courtesy and/or discretional authority vested in them to avoid placing parties, counsel, witnesses, judges or court personnel under undue or avoidable stresses, or health risk. Accordingly, we remind lawyers that the Guidelines for Civility in Litigation … require that lawyers grant reasonable requests for extensions and other accommodations.
>
> Given the current circumstances, attorneys should be prepared to agree to reasonable extensions and continuances as may be necessary or advisable to avoid in-person meetings, hearings or deposition obligations. Consistent with California

[6] https://support.microsoft.com/en-us/help/4092060/windows-keep-your-computer-secure-at-home

[7] Title 204, Ch. 99 adopted Dec. 6, 2000, amended April 21, 2005, effective May 7, 2005.

> Rule of Professional Conduct 1.2(a), lawyers should also consult with their clients to seek authorization to extend such extensions or to stipulate to continuances in instances where the clients' authorization or consent may be required.
>
> While we expect further guidance from the court system will be forthcoming, lawyers must do their best to help mitigate stress and health risk to litigants, counsel and court personnel. Any sharp practices that increase risk or which seek to take advantage of the current health crisis must be avoided in every instance.

This Opinion agrees with the Los Angeles County Bar Association's statement and urges lawyers to comply with Pennsylvania's Code of Civility, and not take unfair advantage of any public health and safety crises.

IV. Conclusion

The COVID-19 pandemic has caused unprecedented disruption for attorneys and law firms, and has renewed the focus on what constitutes competent legal representation during a time when attorneys do not have access to their physical offices. In particular, working from home has become the new normal, forcing law offices to transform themselves into a remote workforce overnight. As a result, attorneys must be particularly cognizant of how they and their staff work remotely, how they access data, and how they prevent computer viruses and other cybersecurity risks.

In addition, lawyers working remotely must consider the security and confidentiality of their procedures and systems. This obligation includes protecting computer systems and physical files, and ensuring that the confidentiality of client telephone and other conversations and communications remain protected.

Although the pandemic created an unprecedented situation, the guidance provided applies equally to attorneys or persons performing client legal work on behalf of attorneys when the work is performed at home or at other locations outside of outside of their physical offices, including when performed at virtual law offices.

Hot Topics in Legal Ethics

David G. Ries
Clark Hill PLC
Pittsburgh, PA
412.394.7787
dries@clakhill.com

May 2020

Contents

Adapted from course materials prepared by the author for the Special Institute on Mineral Title Examination in September 2019 in Westminster, CO, cosponsored by the Rocky Mountain Mineral Law Foundation, the Energy and Mineral Law Foundation and the American Association of Professional Landmen.

This paper explores three current issues in legal ethics that are important for energy and mineral attorneys to understand and address. They include competence in technology, safeguarding client data, and multijurisdictional practice.

I. Competence in Technology

As the use of technology in the practice of law continues to grow at a rapid pace, attorney competence in technology and protection of electronic data and client information is more important than ever before. At the American Bar Association Annual Meeting in August 2012, the ABA Model Rules of Professional Conduct[1] ("Model Rules") were amended to add express requirements of competence in technology and reasonable measures to safeguard information relating to clients. Reactions to these amends have varied, ranging from viewing the amendments as a sea change, adding potentially onerous new duties, to seeing them as simply making more explicit what was already required. What do the amended rules actually require? How can attorneys comply with them? This section provides an overview of the duty of competence and what it requires. The next section explores the duty to safeguard information relating to clients.

This paper discusses the ABA Model Rules. It is important for attorneys to consult and comply with the ethics rules, court cases and ethics opinions in the relevant jurisdiction(s).

A. ABA Commission on Ethics 20/20

The ABA Commission on Ethics was appointed by the ABA President in 2009 to perform a thorough review of the Model Rules and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments. The Commission submitted its proposals for consideration at the ABA 2012 Annual Meeting, including Technology and Confidentiality, Technology and Client Development, Outsourcing, Practice Pending Admission, Admission by Motion, and Detection of Conflicts of Interest. These proposals were adopted and the Model Rules were amended in accordance with them.

Additional proposals were approved at the ABA 2013 Midyear Meeting, including Unauthorized Practice of Law; Multijurisdictional Practice of Law, Registration of In-House Counsel**,** Pro Hac Vice Admission, and Choice of Rule for ethics and discipline. The Commission referred fee division and nonlawyer ownership of law firms to the ABA Standing Committee on Ethics and Professional Responsibility for further consideration. The Commission's Introductions and Overviews and Reports and Resolutions, as well as detailed background information, are available on the Commission's website.[2]

B. The Ethics 20/20 Amendments: Competence and Confidentiality

The Commission found that technology has transformed how attorneys communicate with clients and how they process and store information relating to clients. This has created new issues about lawyers' obligations, including the duty to protect confidential information. The

---

[1] ABA Model Rules of Professional Conduct (2020).

[2] www.americanbar.org/groups/professional_responsibility/committees_commissions/aba-commission-on--ethics-20-20.

amendment to the Comment to Model Rule 1.1 requires attorneys to have and maintain competence in their use of technology. The amendments to Model Rules 1.1 and 1.6 together require attorneys to take competent and reasonable measures to protect client information. These rules and comments, as amended, provide (additions underlined):

> **Model Rule 1.1 - Competence**
>
> 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**
>
> ***
>
> **Maintaining Competence**
>
> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology,</u> engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.
>
> _____
>
> **Model Rule 1.6 - Confidentiality of Information:**
>
> (a) A lawyer shall not reveal information relating to the representation of a client unless…
>
> <u>(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.</u>
>
> _____
>
> **Model Rule 5.3 Responsibilities Regarding Nonlawyer Assistance**

The rule was amended to expand its scope. "Assistants" was expanded to "Assist<u>ance</u>," extending its coverage to all levels of staff and outsourced services, ranging from copying services, to cloud technology service providers, to outsourced legal services. This requires attorneys to employ reasonable safeguards, like due diligence, contractual requirements, supervision, and monitoring, to insure that nonlawyers, both inside and outside a law firm, provide services in compliance with an attorney's duty of confidentiality.

C. Existing Obligations, Not New Ones

The Ethics 20/20 Commission noted that the requirements for competence in technology and competent and reasonable measures to safeguard confidentiality were not new:

> <u>Rule 1.1 Comment [8]</u>: "The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should

> remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

ABA Commission on Ethics 20/20, *Report to Resolution 105A Revised* (2012). As of December 2019, 38 states have adopted this amendment or a variation of it.

> Rule 1.6 (c): "This duty is already described in several existing Comments, but the Commission concluded that, in light of the pervasive use of technology to store and transmit confidential client information, this existing obligation should be stated explicitly in the black letter of Model Rule 1.6."

ABA Commission on Ethics 20/20, *Report to Resolution 105A Revised*, Introduction (2012).

D. Competence in Technology – What Does It Require?

To comply with the duty of competence in technology, attorneys must: **know relevant technology, learn it, or get qualified assistance with it.**

1. Critical Competencies

Andrew Perlman, the Dean of Suffolk University Law School and a Reporter of the ABA Ethics 20/20 Commission," has summarized the duty of competence in technology as follows:[3]

> Just twenty years ago, lawyers were not expected to know how to protect confidential information from cybersecurity threats, use the Internet for marketing and investigations, employ cloud-based services to manage a practice and interact with clients, implement automated document assembly and expert systems to reduce costs, or engage in electronic discovery. Today, these skills are increasingly essential, and many lawyers want to know whether they are adapting quickly enough to satisfy their ethical duty of competence.

Dean Perlman's examples of critical competencies in technology include:

1. Cybersecurity
2. Internet Marketing and Investigations
3. Employing Cloud-Based Services (in the practice of law)
4. Leveraging New and Established Legal Technology / Innovation

Examples of this 4th category include: "automated document assembly, expert systems (e.g., automated processes that generate legal conclusions after users answer a series of branching questions), knowledge management (e.g., tools that enable lawyers to find information efficiently within a lawyer's own firm, such as by locating a pre-existing document addressing a legal issue or identifying a lawyer who is already expert in the subject), legal analytics (e.g., using "big data" to help forecast the outcome of cases and

[3] Andrew M. Perlman, "The Twenty-First Century Lawyer's Evolving Ethical Duty of Competence," The Professional Lawyer (December 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2532995.

determine their settlement value), virtual legal services, and cloud-based law practice management."

This article provides a good overview of the general requirements.

2. E-Discovery

E-Discovery is an area of practice in which technology has been rapidly developing. Attorneys who are involved in this practice area face continuing challenges in having and maintaining competence in the developing law and technology.

State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2015-193 analyzes the duty of competence for attorneys who engage in e-discovery. It includes the following:

Digest:

> An attorney's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law. Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a matter, and the nature of the ESI. Competency may require even a highly experienced attorney to seek assistance in some litigation matters involving ESI. An attorney lacking the required competence for e-discovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the representation. Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney's duty of confidentiality.

The opinion lists the following skills and resources that may be necessary for competent handling of e-discovery, depending on the complexity of e-discovery in the case. If they apply in the case, an attorney must either have or acquire the necessary skills or engage the resources to provide them - either competent co-counsel or expert consultants:

1. initially assess e-discovery needs and issues, if any;
2. implement/cause to implement appropriate ESI preservation procedures;
3. analyze and understand a client's ESI systems and storage;
4. advise the client on available options for collection and preservation of ESI;
5. identify custodians of potentially relevant ESI;
6. engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan;
7. perform data searches;

8. collect responsive ESI in a manner that preserves the integrity of that ESI; and
9. produce responsive non-privileged ESI in a recognized and appropriate manner.

Exterro, an e-discovery service provider, recently published the results of a its fifth annual survey of federal judges.[4] One of the statements on which judges were asked to comment was: "In the past 12 months, the lawyers appearing before you have shown an adequate level of knowledge and expertise in e-discovery matters." Only 4% of judges strongly agreed; 52% agreed; 26% were neutral, 15% disagreed; and 3% strongly disagreed.

Lack of competence in e-discovery can lead to disciplinary sanctions. Massachusetts Board of Bar Overseers, Public Reprimand No. 2013-21 (October 9, 2013) (competence in e-discovery) sanctioned an attorney for violation of duties of competence and communication for improper advice to client about the duty to preserve electronically stored information, resulting in court sanctions to client. The reprimand states:

> The respondent's advice to his client to scrub certain files from the hard drive of a laptop in contravention of a court order constituted unlawful obstruction of another party's access to evidence, in violation of Mass. R. Prof. C. 3.4(a). The respondent's failure to adequately communicate to his client his obligations under the court order and the potential prejudice of altering property subject to the court order was conduct in violation of Mass. R. Prof. C. 1.4. Finally, the respondent's conduct of handling a matter that he was not competent to handle without adequate research or associating with or conferring with experienced counsel, and without any attempt to confirm the nature and content of the proposed deletions, was conduct in violation of Mass. R. Prof. C. 1.1.

Developing technology in e-discovery can present a challenge to attorneys in maintaining competence in technology. Deduplication is an automated process that identifies and links duplicate and near-duplicate electronic documents and files, like e-mails. After duplicates have been identified and linked, a reviewer can review all of them at one time for relevance, responsiveness to a document request, privilege, etc. The process avoids repetitive review efforts, which can be substantial, and protects against inconsistent classification by multiple reviewers. Deduplication Technology has now been for a number of years.

An article in 2010 discussed the ethical issues involved in attorneys' performing unnecessary review of electronic data because of their failure to use deduplication software.[5] The issues it addressed include conflicts of interest (from charging for unnecessary services) and competence (from lack of knowledge of these kinds of tools).

---

[4] Exterro, "Judges Survey 2019, A Survey of Industry Trends, Practices, and Challenges Faced."

[5] Patrick Oot, Joe Howie, and Anne Kershaw, "Ethics and Ediscovery Review," *ACC Docket* (January/February 2010).

3. Waiver of Privilege in Using a File Sharing Site

As the following example shows, improper use of technology can present a risk of waiver of privilege. In *Harleysville Ins. Co. v. Holding Funeral Home, Inc.,* 2017 WL 1041600 (W.D. Va. Feb. 9, 2017), the Magistrate Judge held that the placement of privileged information on Box, a file share service like Dropbox, and sharing of the hyperlink to access that information without additional protection (like password protection) constituted a failure to take reasonable steps to protect the information, resulting in waiver of attorney-client privilege and work-product protection.

The facts are somewhat complex. The case involved a fire loss with an allegation of arson and insurance fraud. Counsel for the insurer uploaded a claim file to the Box file sharing service and sent a link to the Box folder to the National Insurance Crime Bureau for an investigation. Defense counsel later served a subpoena on the National Insurance Crime Bureau, which produced the email containing the link. Defense counsel then used the link to access and download the investigation file and later produced it to the insurer's counsel in response to a request for production. The Magistrate Judge found that use of the link, without additional protection, was like leaving a file on a park bench and waived any applicable privilege and work product protection.

In *Harleysville Ins. Co. v. Holding Funeral Home, Inc.,* 2017 WL 4368617 (W.D. Va. Oct. 2, 2017), the District Judge reversed the Magistrate Judge's decision, holding that the disclosure was inadvertent and there was no waiver. The court also imposed sanctions on defense counsel for 1) failing to notify the insurer's counsel of the inadvertent production, as required by a Virginia rule and Virginia Legal Ethics Opinion 1702, requiring such notice, and 2) Federal Rule of Civil Procedure 45(e)(2)(B) for "failure to return, sequester or destroy the privileged material upon [the insurer's] counsel's request."

> Model Rule 4.4(b) provides:
>
> (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.
>
> _____
>
> Federal Rule of Civil Procedure 45(e)(2)(B), like Rule 26(b)(5)(B), provides:
>
> (B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who

produced the information must preserve the information until the claim is resolved.

Under the Virginia rule and ethics opinion, similar to Model Rule 4.4(b), the District Court held that defense counsel receiving the inadvertently produced information should have notified the insurer's counsel who produced it. It also held that under Fed. R. Civ. P. 45, defense counsel, upon request by insurer's counsel, should have returned or sequestered the information unless the court found that there was a waiver.

This case demonstrates both the risk of waiver in using technology and how the Magistrate Judge and District Judge viewed the same conduct differently; different judges may rule differently on the same facts.

A practical lesson from this case is the importance of understanding technology used a lawyer and using its available control and security tools to protect confidential and privileged information. The problem may have been avoided by using measures like removing the privileged file after it was downloaded, setting an expiration date on the recipient's access and/or password protecting (and sharing it with the recipient in a secure way; not in the email sharing the link).

4. Errors in Redaction

A recent, high profile example of an error in the use of technology by attorneys is the failed redaction of confidential information in a court filing by Paul Manafort's attorneys in January of 2019. Confidential information about the Mueller investigation, which was not to be made public, was covered by black bars in the PDF court filings. However, the information was not properly redacted and could be retrieved by copying and pasting it.[6] Technology tools are available to securely redact information in electronic documents.[7] There have been other similar incidents.[8] They present issues of competence in technology.

5. E-Filing and Missed Deadlines

The following cases are examples of how errors in electronic filing can have serious consequences.

U.S. v. Carelock, 459 F.3d 437 (3rd Cir. 2009)
(Error in electronic filing of a notice of appeal in a criminal case waived the right to appeal)

[6] Louise Matsakis, "Paul Manafort is Terrible With Technology," *Wired* (Jan. 9, 2019).

[7] E.g., Adobe, "How to remove sensitive information from PDF's," https://helpx.adobe.com/acrobat/how-to/redact-pdf.html; National Security Agency |Central Security Service, "Redaction of PDF File Using Adobe Acrobat Professional X," https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/redaction-of-pdf-files-using-adobe-acrobat-professional-x.cfm

[8] Judge Herbert B. Dixon, Jr., "Embarrassing Redaction Failures," *The Judge's Journal* (May 1, 2019).

The court observed:

> "To err is human, but to really foul things up requires a computer." Farmers' Almanac (1978). In parting, we note that the cause of this error was that Carelock's counsel had unfortunately failed to double-check the document he had electronically transmitted to the District Court. Although the modern use of the computer is a great time-saver, its ease of use should not assuage the almost obsessive attentiveness that is required when filing any document with a court. Otherwise, a scenario such as Carelock's may occur, which proves the adage that "a computer lets you make more mistakes faster than any invention in human history-with the possible exceptions of handguns and tequila." Mitch Ratcliffe (quoted in Herb Brody, The Pleasure Machine: Computers, Technology Review, Apr. 1992, at 31).

Two-Way Media LLC v. AT&T, Inc., 782 F.3d 1311 (Fed. Cir. 2015)

(Defendants were properly denied an extension of the time for filing an appeal of a $40 million judgment of patent infringement, even though court notices of electronic filings communicated an arguably incomplete description of the orders resolving post-trial motions, since counsels' failure to review the orders attached to the notices and failure to review the civil docket that contained a complete description of the orders did not constitute "excusable neglect.")

Official Comm. of Unsecured Creditors of Motors Liquidation Co. v. JP Morgan Chase Bank, N.A. (In re Motors Liquidation Co., 777 F.3d 100 (2nd Cir. 2015)

(Law firm associate tasked paralegal with organizing and filing UCC-3 termination statements to release security interest in debtor's property. Paralegal erroneously included one that terminated the security interest for a different $1.5 billion debt. Associate, other attorneys in associate's firm, and attorneys in another firm did not catch the error. Termination of main loan was effective – the UCC contains no requirement that a secured party that authorizes a filing subjectively intends or otherwise understands the effect of the plain terms of its own filing.)

E. Additional Information

ABA/Bloomberg Law Lawyer's Manual on Professional Conduct (print and online reference manual, with biweekly current reports)
www.americanbar.org/groups/professional_responsibility/publications/aba_bna_lawyers_manual_on_professional_conduct

American Bar Association*, ABA Compendium of Professional Responsibility Rules and Standards, 2018 Edition* (collection of professional responsibility rules, standards and selected ethics opinions)

American Bar Association, *Annotated Model Rules of Professional Conduct, Ninth Ed.* (2019)

American Bar Association, *Model Rules of Professional Conduct, 2020 Edition*

American Bar Association, Center for Professional Responsibility – (includes online version of the current Model Rules of Professional Conduct, copies of recent ABA ethics opinions and

headnotes to earlier ABA ethics opinion)
www.americanbar.org/groups/professional_responsibility.html

Geoffrey C. Hazard, Jr., W. William Hodes and Peter Jarvis *The Law of Lawyering, Fourth Edition*, (Wolters Kluwer, November 2019 Update)

Andrew M. Perlman, "The Twenty-First Century Lawyer's Evolving Ethical Duty of Competence," *The Professional Lawyer* (2014), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2532995.

Antigone Peyton, "Kill the Dinosaurs, and Other Tips for Achieving Technical Competence in Your Law Practice," *Richmond J. L. & Tech.* (March 2015)

Ronald D. Rotunda and John S. Dzienkowski, *Legal Ethics: The Lawyer's Deskbook on Professional Responsibility, 2018 – 2019 Ed.* (Thomson West 2018)

II. Safeguarding Client Data: Attorneys' Legal and Ethical Duties

Confidential data in computers and information systems, including those used by attorneys and law firms, faces greater security threats today than ever before. And they continue to grow! They take a variety of forms, ranging from e-mail phishing scams and social engineering attacks to sophisticated technical exploits resulting in long term intrusions into law firm networks. They also include lost or stolen laptops, tablets, smartphones, and USB drives, as well as inside threats - malicious, untrained, inattentive, and even bored personnel.

These threats are a particular concern to attorneys because of their duties of competence in technology and confidentiality. Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients. They also often have contractual and regulatory duties to protect client information and other types of confidential information.

Breaches have become, so prevalent that there is a new mantra in cybersecurity today – it's "when, not if" there will be a breach. Robert Mueller, then the FBI Director, put it this way in an address at a major information security conference in 2012:[9]

> I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.

This is true for attorneys and law firms as well as other businesses and enterprises. Consistent with this threat environment, New York Ethics Opinion 1019 warned attorneys in May 2014:

> Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including

[9] FBI Director, RSA Cybersecurity Conference (March 1, 2012) https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

> trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks.

ABA Formal Opinion 477R (May 2017) (discussed below), describes the same current threat environment:

> At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a … world where law enforcement discusses hacking and data loss in terms of "when," and not "if." Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.

The ABA's *2019 Legal Technology Survey Report* reports that law firms have been and continue to be victims of data breaches.[10] The *Survey* reports that about 26% of respondents overall reported that their firms had experienced a security breach at some point. The question is not limited to the past year, it's "ever." A breach broadly includes incidents like a lost/stolen computer or smartphone, hacker, break-in, or website exploit. This compares with 23% last year.

Law.com published a series of articles on law firm data breaches in October of 2019. It reported on over 100 breaches, based on its review of state websites and information requests to states about breaches reported to states by law firms under data breach notice laws. The first article started with:[11]

> A Law.com investigation finds that law firms are falling victim to data breaches at an alarming rate, exposing sensitive client and attorney information. These incidents—most unpublicized before now—may just be the tip of the iceberg.

---

[10] See, John G. Loughnane, ABA TECHREPORT 2019 Cybersecurity, www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019.

[11] Christine Simmons**,** Xiumei Dong and Ben Hancock**,** "More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse," Law.com (October 15, 2019), www.law.com/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-picture-is-getting-worse. See also, Christine Simmons**,** Xiumei Dong and Ben Hancock**, "**Law Firm Cybersecurity: See Which Firms Reported a Data Breach," Law.com (October 15, 2019), www.law.com/2019/10/15/here-are-law-firms-reporting-data-breaches, Christine Simmons**,** Xiumei Dong and Ben Hancock**,** "How Vendor Data Breaches Are Putting Law Firms at Risk," Law.com (October 17, 2019), www.law.com/2019/10/17/how-vendor-data-breaches-are-putting-law-firms-at-risk and Christine Simmons and Xiumei Dong, "As Hackers Get Smarter, Can Law Firms Keep Up?" Law.com (October 28, 2019), www.law.com/2019/10/28/as-hackers-get-smarter-can-law-firms-keep-up.

Security threats to lawyers and law firms continue to be substantial, real, and growing – security incidents and data breaches have occurred and are occurring. It is critical for attorneys and law firms to recognize these threats and address them through comprehensive information security programs. **The greatest security threats to attorneys and law firms today are most likely spearphishing, ransomware, business email compromise, and lost and stolen laptops and mobile devices.**

A. Duty to Safeguard

Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients and also often have contractual and regulatory duties to protect confidential information.

1. Ethics Rules

Several Model Rules have particular application to protection of client information, including competence (Model Rule 1.1), communication (Model Rule 1.4), confidentiality of information (Model Rule 1.6), safeguarding property (Model Rule 1.15), and supervision (Model Rules 5.1, 5.2 and 5.3).

Model Rule 1.1: Competence covers the general duty of competence. It provides that "A lawyer shall provide competent representation to a client." This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." It includes competence in selecting and using technology, including cybersecurity. It requires attorneys who lack the necessary technical competence for security to learn it or to consult with qualified people who have the requisite expertise.

As discussed above, the ABA Commission on Ethics 20/20 conducted a review of the Model Rules and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments. One of its core areas of focus was technology and confidentiality. Its recommendations in this area were adopted by the ABA at its Annual Meeting in August of 2012.

The 2012 amendments include addition of the following underlined language to the Comment to Model Rule 1.1:

> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>…

As of December 2019, 38 states have adopted this addition to the comment to Model Rule 1.1, some with variations from the ABA language.

Model Rule 1.4: Communications also applies to attorneys' use of technology. It requires appropriate communications with clients "about the means by which the client's objectives are to be accomplished," including the use of technology. It requires keeping the client informed and, depending on the circumstances, may require obtaining "informed consent." It requires notice to a client of a compromise of confidential information relating to the client.

Model Rule 1.6: Confidentiality of Information generally defines the duty of confidentiality. It begins as follows:

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b). . .

Rule 1.6 broadly requires protection of "information relating to the representation of a client;" it is not limited to confidential communications and privileged information. Disclosure of covered information generally requires express or implied client consent (in the absence of special circumstances like misconduct by the client).

The 2012 amendments added the following new subsection (underlined) to Model Rule 1.6:

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

This requirement covers two areas – inadvertent disclosure and unauthorized access. Inadvertent disclosure includes threats like leaving a briefcase, laptop, or smartphone in a taxi or restaurant, sending a confidential e-mail to the wrong recipient, producing privileged documents or data in litigation, or exposing confidential metadata. Unauthorized access includes threats like hackers, criminals, malware, and insider threats.

The 2012 amendments also include additions to Comment [18] to Rule 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 and consideration of available safeguards. The analysis includes 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 require the lawyer to implement special security measures not required by the rule or may give informed consent to forego security measures that would otherwise be required by the rule. The amended Comment is as follows (with strikethrough for deletions and underlining for additions:

> **Comment**
>
> ***
>
> **Acting Competently to Preserve Confidentiality**
>
> [18] Paragraph (c) requires a ~~A~~ lawyer ~~must~~ to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the

> access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

Significantly, the Ethics 20/20 Commission noted that these revisions to Model Rules 1.1 and 1.6 make explicit what was already required rather than adding new requirements.

Model Rule 5.1: Responsibilities of Partners, Managers, and Supervisory Lawyers and Model Rule 5.2: Responsibilities of a Subordinate Lawyer include the duties of competence and confidentiality. Model Rule 5.3: Responsibilities Regarding Nonlawyer Assistants 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. This requires attorneys to employ reasonable safeguards, like due diligence, contractual requirements, supervision, and monitoring, to ensure that nonlawyers, both inside and outside a law firm, provide services in compliance with an attorney's ethical duties, including confidentiality.

Model Rule 1.15: Safeguarding Property requires attorneys to segregate and protect money and property of clients and third parties that is held by attorneys. Some ethics opinions and articles have applied it to electronic data held by attorneys.

In June 2012, while the Ethics 20/20 amendments were under consideration, the *Wall Street Journal* published "Client Secrets at Risk as Hackers Target Law Firms."[12] It started with:

> Think knowing how to draft a contract, file a motion on time and keep your mouth shut fulfills your lawyerly obligations of competence and confidentiality?

[12] Jennifer Smith, "Client Secrets at Risk as Hackers Target Law Firms," *Wall Street Journal Law Blog* (June 25, 2012), https://blogs.wsj.com/law/2012/06/25/dont-click-on-that-link-client-secrets-at-risk-as-hackers-target-law-firms.

> Not these days. Cyberattacks against law firms are on the rise, and that means attorneys who want to protect their clients' secrets are having to reboot their skills for the digital age.

2. Ethics Opinions

A number of state ethics opinions, for over a decade, have addressed professional responsibility issues related to security in attorneys' use of various technologies. Consistent with the Ethics 20/20 amendments, they generally require competent and reasonable safeguards.

Examples include State Bar of Arizona, Opinion No. 05-04 (July 2005), New Jersey Advisory Committee on Professional Ethics, Opinion 701, "Electronic Storage and Access of Client Files" (April, 2006), State Bar of Arizona, Opinion No. 09-04 (December, 2009): "Confidentiality; Maintaining Client Files; Electronic Storage; Internet" (Formal Opinion of the Committee on the Rules of Professional Conduct); State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179; and New York State Bar Association Ethics Opinion 1019, "Confidentiality; Remote Access to Firm's Electronic Files," (August, 2014).

Significantly, California Formal Opinion No. 2010-179 advises attorneys that they must consider security **before** using a particular technology in the course of representing a client. Depending on the circumstances, an attorney may be required to avoid using a particular technology or to advise a client of the risks and seek informed consent if appropriate safeguards cannot be employed.

There are now multiple ethics opinions on attorneys' use of cloud computing services like online file storage and software as a service (SaaS).[13] For example, New York Bar Association Committee on Professional Ethics Opinion 842 "Using an outside online storage provider to store client confidential information" (September, 2010), consistent with the general requirements of the ethics opinions above, concludes: "[a] lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's obligations under Rule 1.6."

Another opinion on safeguarding client data is ABA Formal Opinion 477R, "Securing Communication of Protected Client Information" (May 2017). While focusing on electronic communications, it also explores the general duties to safeguard information relating to clients in light of current threats and the Ethics 20/20 technology amendments to the Model Rules. Its conclusion includes:

> Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the

[13]The ABA Legal Technology Resource Center has published a summary with links, "Cloud Ethics Opinions around the U.S.," available at www.americanbar.org/content/dam/aba/images/legal_technology_resources/CloudEthicsOpinions2019/cloudethicsopinions2019.pdf.

> benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

More recently, the ABA issued Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018). The opinion reviews lawyers' duties of competence, confidentiality and supervision in safeguarding confidential data and in responding to data breaches. It discusses the obligations to monitor for a data breach, stopping a breach and restoring systems, and determining what occurred. It finds that Model Rule 1.15: Safeguarding Property applies to electronic client files as well as paper client files and requires the care required of a professional fiduciary.

The opinion concludes:

> Even lawyers who, (i) under Model Rule 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 Rule 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 Rule 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."

Most recently, addressing work-at-home issues arising from the COVID-19 pandemic, the Pennsylvania Bar Association issued Formal Opinion 2020-300, "Ethical Obligations for Lawyers' Working Remotely" (April 2020). The opinion reviews attorneys' ethical duties to employ competent and reasonable measures to safeguard information relating to clients and provides best practices for attorneys performing legal work and communications remotely.

The opinion concludes:

> The COVID-19 pandemic has caused unprecedented disruption for attorneys and law firms, and has renewed the focus on what constitutes competent legal representation during a time when attorneys do not have access to their physical offices. In particular, working from home has become the new normal, forcing law offices to transform themselves into a remote workforce overnight. As a result, attorneys must be particularly cognizant of how they and their staff work remotely, how they access data, and how they prevent computer viruses and other cybersecurity risks.
>
> In addition, lawyers working remotely must consider the security and confidentiality of their procedures and systems. This obligation includes protecting computer systems and physical files, and ensuring that the confidentiality of client telephone and other conversations and communications remain protected.

> Although the pandemic created an unprecedented situation, the guidance provided applies equally to attorneys or persons performing client legal work on behalf of attorneys when the work is performed at home or at other locations outside of outside of their physical offices, including when performed at virtual law offices.

The key professional responsibility requirements from these various opinions on attorneys' use of technology are competent and reasonable measures to safeguard client data, including an understanding of limitations in attorneys' knowledge, obtaining appropriate assistance, continuing security awareness, appropriate supervision, and ongoing review as technology, threats, and available safeguards evolve. They also require obtaining clients' informed consent, in some circumstances, and notifying clients of a breach or compromise. It is important for attorneys to consult the rules, comments, and ethics opinions in the relevant jurisdiction(s).

3. Ethics Rules – Electronic Communications

E-mail and electronic communications have become everyday communications forms for attorneys and other professionals. They are fast, convenient, and inexpensive, but also present serious risks to confidentiality. It is important for attorneys to understand and address these risks.

The Ethics 2000 revisions to the Model Rules, over 15 years ago, added Comment [17] (now 19]) to Model Rule 1.6. For electronic communications, it requires "reasonable precautions to prevent the information from coming into the hands of unintended recipients." It provides:

> …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…

This Comment requires attorneys to take "reasonable precautions" to protect the confidentiality of electronic communications. Its language about "special security measures" has often been viewed by attorneys as providing that they never need to use "special security 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."

There are, however, questions about whether unencrypted Internet e-mail affords a reasonable expectation of privacy. Respected security professionals for years have compared the security of unencrypted e-mail to postcards or postcards written in pencil.[14] A June 2014 post by Google on

[14] E.g., Bruce Schneier, *E-Mail Security - How to Keep Your Electronic Messages Private*, (John Wiley & Sons, Inc. 1995) p. 3, Bruce Schneier, *Secrets & Lies: Digital Security in a Networked Work*, (John Wiley &

the *Google Official Blog*[15] and a July 2014 *New York Times* article[16] use the same analogy – comparing the security of unencrypted e-mails to postcards and comparing encryption to envelopes.

Comment [19] to Rule 1.6 also lists "the extent to which the privacy of the communication is protected by law" as a factor to be considered. The federal Electronic Communications Privacy Act[17] and similar state laws make unauthorized interception of electronic communications a crime. Some observers have expressed the view that this should be determinative and attorneys should not be required to use encryption. The better view is to treat legal protection as only one of the factors to be considered. As discussed below, some of the newer ethics opinions conclude that encryption may be a reasonable measure that should be used, particularly for highly sensitive information.

4. Ethics Opinions – Electronic Communications

An ABA ethics opinion in 1999 and several state ethics opinions concluded that special security measures, like encryption, are not generally required for confidential attorney e-mail.[18] However, these opinions, like Comment [19], contain qualifications that limit their general conclusions.

Consistent with the questions raised by security experts about the security of unencrypted e-mail, some ethics opinions express a stronger view that encryption may sometimes be required. For example, New Jersey Opinion 701 (April, 2006), discussed above, notes at the end: "where a document is transmitted to [the attorney] … by email over the Internet, the lawyer should password a confidential document (as is now possible in all common electronic formats,

---

Sons, Inc. 2000) p. 200, and Larry Rogers, "Email – A Postcard Written in Pencil, Special Report," (Software Engineering Institute, Carnegie Mellon University 2001).

[15] "Transparency Report: Protecting Emails as They Travel Across the Web," Google Official Blog (June 3, 2014) http://googleblog.blogspot.com/2014/06/transparency-report-protecting-emails.html.

[16] Molly Wood, "Easier Ways to Protect Email from Unwanted Prying Eyes," *New York Times* (July 16, 2014) www.nytimes.com/2014/07/17/technology/personaltech/ways-to-protect-your-email-after-you-send-it.html?_r=0.

[17] 18 U.S.C. §§ 2510-2522.

[18] For example, ABA Formal Opinion No. 99-413, Protecting the Confidentiality of Unencrypted E-Mail (March 10, 1999) ("based upon current technology and law as we are informed of it …a lawyer sending confidential client information by unencrypted e-mail does not violate Model Rule 1.6(a)…" "…this opinion does not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.") and District of Columbia Bar Opinion 281, "Transmission of Confidential Information by Electronic Mail," (February, 1998), ("In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security.").

including PDF), since it is not possible to secure the Internet itself against third party access."[19] This was over ten years ago.

California Formal Opinion No. 2010-179, Pennsylvania Formal Opinion 2011-200 and Texas Ethics Opinion 648 (2015) provide that encryption may sometimes be required. A July, 2015 ABA article notes **"**The potential for unauthorized receipt of electronic data has caused some experts to revisit the topic and issue [ethics] opinions suggesting that in some circumstances, encryption or other safeguards for certain email communications may be required."[20]

In May 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R, "Securing Communication of Protected Client Information." The Opinion revisits attorneys' duty to use encryption and other safeguards to protect e-mail and electronic communications in light of evolving threats, developing technology, and available safeguards. It suggests a fact-based analysis and finds that "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."

Opinion 477R, consistent with these newer opinions and the article, concludes:

> A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, **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.** (Emphasis added.)

The Opinion references the Ethics 20/20 amendments to Comment [18] to Model Rule 1.6 and its discussion of factors to be considered in determining reasonable and competent efforts. It provides general guidance and leaves details of their application to attorneys and law firms, based on a fact-based analysis on a case-by-case basis.

In addition to complying with any applicable ethics and legal requirements, the most prudent approach to the ethical duty of protecting electronic communications is to have an express understanding with clients (preferably 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. It has now reached the point where all attorneys should have encryption available for use in appropriate circumstances.

---

[19] File password protection in some software, like current versions of Microsoft Office, Adobe Acrobat, and WinZip uses encryption to protect security. It is generally easier to use than encryption of e-mail and attachments. However, the protection can be limited by use of weak passwords that are easy to break or "crack."

[20] Peter Geraghty and Susan Michmerhuizen, "Encryption Conniption," Eye on Ethics, *Your ABA* (July 2015).

5. Common Law and Contractual Duties

Along with the ethical duties, there are parallel common law duties defined by case law in the various states. The Restatement (3rd) of the Law Governing Lawyers (2000) summarizes this area of the law, including Section 16(2) on competence and diligence, Section 16(3) on complying with obligations concerning client's confidences, and Chapter 5, "Confidential Client Information." Breach of these duties can result in a malpractice action.

There are also increasing instances when lawyers have contractual duties to protect client data, particularly for clients in regulated industries, such as health care and financial services that have regulatory requirements to protect privacy and security.

For example, the Association of Corporate Counsel has adopted *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information* that companies can use for security requirements for outside counsel.[21]

6. Regulatory Duties

Attorneys and law firms that have specified personal information about their employees, clients, clients' employees or customers, opposing parties and their employees, or even witnesses may also be covered by federal and state laws that variously require reasonable safeguards for covered information and notice in the event of a data breach.[22]

B. Complying with the Duties

Understanding all of the applicable duties is the first step, before moving to the challenges of compliance by designing, implementing and maintaining an appropriate risk-based information security program. It should address people, policies and procedures, and technology and be appropriately scaled to the size of the practice and the sensitivity of the information.

1. Information Security Overview

Information security is a process to protect the confidentiality, integrity, and availability of information. Comprehensive security must address people, policies and procedures, and technology. While technology is a critical component of effective security, the other aspects must also be addressed. As explained by Bruce Schneier, a highly-respected security professional, "[i]f you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."[23] The best technical security is likely to fail without

---

[21] www.acc.com/resource-library/model-information-protection-and-security-controls-outside-counsel-possessing-0.

[22] For example, Internal Revenue Code, 26 U.S.C. § 6713, Internal Revenue Procedure 2007-40, Gramm-Leach-Bliley Act, 15. U.S.C. §§ 6801-6809 and National Conference of State Legislatures -State Data Security Laws (www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx) and State Security Breach Notification Laws (www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

[23] Bruce Schneier, *Secrets and Lies - Digital Security in a Networked World* (John Wiley & Sons, Inc. 2000) at p. xii.

adequate attention to people and policies and procedures. Many attorneys incorrectly think that security is just for the Information Technology department or consultants. While IT has a critical role, everyone, including management, all attorneys, and all support personnel, must be involved for effective security.

An equally important concept is that security requires training and ongoing attention. It must go beyond a onetime "set it and forget it" approach. A critical component of a law firm security program is constant vigilance and security awareness by all users of technology. As an ABA report aptly put it:[24]

> Lawyers must commit to understanding the security threats that they face, they must educate themselves about the best practices to address those threats, and **they must be diligent in implementing those practices every single day**.
>
> (Emphasis added.)

Information security is best viewed as a part of the information governance process. Information governance manages documents and data from creation to final disposition – including security and privacy.[25]

At the ABA Annual Meeting in August, 2014, the ABA adopted a resolution on cybersecurity that is consistent with this general approach:[26]

> **RESOLVED,** That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected.

This resolution recommends an **appropriate cybersecurity program** for all private and public sector organizations, which includes law firms.

Cybersecurity is best viewed as a part of the information governance process, which manages documents and data from creation to final disposition – including security and privacy.[27] Managing data is a critical part of information governance, including security, privacy, and records and information management. Effective management includes a current inventory,

---

[24] Joshua Poje, "Security Snapshot: Threats and Opportunities," TECHREPORT 2013 (ABA Legal Technology Resource Center 2013).

[25] See the Information Governance Reference Model, published by EDRM, an organization operated by Duke Law School that publishes resources for e-discovery and information governance. www.edrm.net/frameworks-and-standards/information-governance-reference-model.

[26] Available at www.americanbar.org/content/dam/aba/images/abanews/2014am_hodres/109.pdf.

[27] See the Information Governance Reference Model (IGRM), published by EDRM, an organization that publishes resources for e-discovery and information governance (www.edrm.net/frameworks-and-standards/information-governance-reference-model) and ARMA International, Information Governance (www.arma.org/page/Information_Governance).

classification, safeguarding, managing from creation to final disposition, and secure disposition where appropriate. Effective management requires minimization of data – collection and retention of only what is necessary and secure disposition of data that is no longer required or needed. **Management and minimization of data is an essential part of an effective security program.**

The first step for a security program is assigning responsibility for security. This includes defining who is in charge of security and defining everyone's role, including management, attorneys and support personnel.

Security starts with an inventory of information assets to determine what needs to be protected and then a risk assessment to identify anticipated threats to the information assets. The next step is development, implementation, and maintenance of a comprehensive information security program to employ reasonable physical, administrative, and technical safeguards to protect against identified risks. This is generally the most difficult part of the process. It must address people, policies and procedures, and technology and include assignment of responsibility for security, policies and procedures, controls, training, ongoing security awareness, monitoring for compliance, and periodic review and updating.

A cybersecurity program should cover the core security functions: identify, protect, detect, respond and recover. While detection, response, and recovery have always been important parts of security, they have too often taken a back seat to protection. Since security incidents and data breaches are increasingly viewed as sometimes being inevitable, these other functions have taken on increased importance. Gartner, a leading technology consulting firm, has predicted that by 2020, 60% of enterprises' information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2014.[28]

The requirement for lawyers is reasonable security, not absolute security. For example, New Jersey Ethics Opinion 701 states "'[r]easonable care,' however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible…" Recognizing this concept, the Ethics 20/20 amendments to the Comment to Model Rule 1.6 include "…[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure."

Security involves thorough analysis and often requires balancing and trade-offs to determine what risks and safeguards are reasonable under the circumstances. There is frequently a trade-off between security and usability. Strong security often makes technology very difficult to use, while easy to use technology is frequently insecure. The challenge is striking the correct balance among all of these often-competing factors.

---

[28] http://blogs.gartner.com/anton-chuvakin/2014/02/24/new-research-on-dealing-with-advanced-threats.

The Ethics 20/20 amendments to Comment 18 to Rule 1.6 provide some high-level guidance. As discussed above, the following factors are applied for determining reasonable and competent safeguards:

> Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

This is a risk-based approach that is now standard in information security.

A comprehensive security program should be based on a standard or framework. Examples include the National Institute for Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,* (April 2018), other more comprehensive NIST standards, like NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) and standards referenced in it (a comprehensive catalog of controls and a process for selection and implementation of them through a risk management process) (designed for government agencies and large organizations), and the International Organization for Standardization's (ISO), ISO/IEC 27000 family of standards, (consensus international standards for comprehensive Information Security Management Systems (ISMS) and elements of them). (See NIST and ISO references in Additional Information below for references to these standards and frameworks.)

These standards can be a challenge for small and mid-size firms. In October of 2018, the Federal Trade Commission launched a new website, Cybersecurity for Small Business, which includes links to a number of security resources that are tailored to small businesses.[29] It is a joint project of the FTC, NIST, the U.S. Small Business Administration, and the U.S. Department of Homeland Security. NIST's *Small Business Information Security: The Fundamentals, NISTR 7621, Revision 1* (November 2016) provides NIST's recommendations for small businesses based on the *Framework*.[30] In March of 2019, NIST launched its Small Business Cybersecurity Corner website.[31]

The ABA Cybersecurity Legal Task Force serves as a clearinghouse regarding cybersecurity activities, policy proposals, advocacy, publications, and resources, tailored to lawyers and the legal profession. Its website contains a wealth of information and links to resources.[32] The Task Force maintains a web page that includes these and additional resources for small law firms and

---

[29] www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity.

[30] https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

[31] www.nist.gov/itl/smallbusinesscyber.

[32] www.americanbar.org/groups/cybersecurity.

sole practitioners.[33] During 2018, The *ABA Journal* and the Task Force jointly produced a series of articles, "Digital Dangers – Cybersecurity and the law" that provide a variety of information on digital threats to attorneys and ways of addressing them.[34]

The ABA now offers as a member benefit a variety of free live and on demand webinars, including a number of webinars on cybersecurity and privacy. They're a great resource – and free.[35] Recent examples include "Working Remotely: Ethical Considerations During and After COVID-19" (May 14, 2020; will be available on demand,)[36] "The ABA Speaks on the Ethics of Disaster Recovery and Data Breaches" (December 10, 2019 and on demand)[37] and "Best of ABA TECHSHOW: Anatomy of a Data Breach: Analyzing Past Breaches to Minimize Risk" (February 4, 2020 and on demand).[38]

A comprehensive information security program should include:

- **Assignment of responsibility for security,**
- **Manage and minimize data,**
- **An inventory of information assets and data,**
- **A risk assessment,**
- **Appropriate administrative, technical and physical safeguards to address identified risks,**
- **Managing new hires, current employees and departing employees**
- **Training,**
- **An incident response plan,**
- **A backup and disaster recovery program,**
- **Managing third-party security risks, and**
- **Periodic review and updating.**

Attorneys and law firms will often need assistance in developing, implementing, and maintaining information security programs because they do not have the requisite knowledge and experience. For those who need assistance, it is important to find an IT consultant with

---

[33] www.americanbar.org/groups/cybersecurity/small-solo-resources/aba-cybersecurity-resources-for-small-solo-law-firms.

[34] Summaries of the articles and links to them are available at www.abajournal.com/magazine/cyber.

[35] www.americanbar.org/cle-marketplace/cle-library.

[36] www.americanbar.org/events-cle/mtg/web/399544145.

[37] www.americanbar.org/events-cle/ecd/ondemand/389385161.

[38] www.americanbar.org/events-cle/ecd/ondemand/392937589.

knowledge and experience in security or a qualified security consultant. Qualified consultants can provide valuable assistance in this process. An increasing number of law firms are using service providers for assistance with developing and implementing security programs, for third-party review of security, and for services like security scans and penetration testing to identify vulnerabilities. A growing trend is to outsource **part** of the security function by using a managed security service provider for functions such as remote administration of security devices like firewalls, remote updating of security software, and 24 X 7 X 365 remote monitoring of network security.

2. Cyber Insurance

Law firms are increasingly obtaining cyber insurance to transfer some of the risks to confidentiality, integrity, and availability of data in their computers and information systems. This emerging form of insurance can cover gaps in more traditional forms of insurance, covering areas like restoration of data, incident response costs, and liability for data breaches. Because cyber insurance is an emerging area of coverage and policies differ, it is critical to understand what is and is not covered by policies and how they fit with other insurance. The ABA Center for Professional Responsibility has published *Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber-Liability Insurance Policy* that provides guidance in this area.[39]

C. Conclusion

Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients and often have contractual and regulatory duties. These duties provide minimum standards with which attorneys are required to comply. Attorneys should aim for even stronger safeguards as a matter of sound professional practice and client service. The safeguards should be included in a risk-based, comprehensive security program.

Attorneys have three options for complying with these duties: know the requirements, threats and relevant safeguards, learn them, or get qualified assistance. For most attorneys, it will be a combination of all three.

D. Additional Information

American Bar Association, Cybersecurity Resources, provides links to cybersecurity materials and publications by various ABA sections, divisions and committees www.americanbar.org/groups/cybersecurity/resources,

American Bar Association, Cybersecurity Legal Task Force, serves as a clearinghouse regarding cybersecurity activities, policy proposals, advocacy, publications, and resources, tailored to lawyers and the legal profession. Its website contains a wealth of information and links to

---

[39] Eileen R. Garczynski, *Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber-Liability Insurance Policy* (American Bar Association 2016) and Eileen R. Garczynski, "Protecting Firm Assets with Cyber Liability Insurance," *Business Law Today* (September 2016), www.americanbar.org/publications/blt/2016/09/05_garczynski.html.

resources, including ones for small law firms and sole practitioners, www.americanbar.org/groups/cybersecurity

American Bar Association, *Model Rules of Professional Conduct, 2020 Edition*

John T. Bandler, *Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security* (American Bar Association 2017)

Center for Internet Security, a leading security organization that publishes consensus-based best security practices like the *CIS Controls* and *Secure Configuration Benchmarks*, www.cisecurity.org

Daniel Garrie and Bill Spernow, *Law Firm Cybersecurity* (American Bar Association 2017)

Federal Trade Commission (FTC), Data Security Resources for Business, www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security, Small Business Cybersecurity, www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

ILTA (International Legal Technology Association) LegalSEC, , provides the legal community with guidelines for risk-based information security programs, including publications, the LegalSEC security initiative, peer group discussions, webinars, an annual LegalSEC Summit conference and other live programs; some materials are publicly available while others are available only to members, http://connect.iltanet.org/resources/legalsec?ssopc=1

International Organization for Standardization (ISO), publishes the ISO/IEC 27000 family of standards, consensus international standards for comprehensive Information Security Management Systems (ISMS) and elements of them, www.iso.org/isoiec-27001-information-security.html

National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications, publishes numerous standards and publications, including the *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,* (April 2018) and *Small Business Information Security: The Fundamentals, NISTR 7621, Revision 1* (November 2016) and Small Business Cybersecurity Corner website, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf and www.nist.gov/itl/smallbusinesscyber

SANS Institute, www.sans.org, a leading information research, education, and certification provider, includes resources like the *SANS Reading Room*, the *Critical Security Controls*, *Securing the Human*, and OUCH! (a monthly security newsletter for end users)

Sharon D. Nelson, David G. Ries and John W. Simek, *Encryption Made Simple for Lawyers* (American Bar Association 2015)

Sharon D. Nelson, David G. Ries and John W. Simek, *Locked Down: Practical Information Security for Lawyers, Second Edition* (American Bar Association 2016)

Jill D. Rhodes and Robert S. Litt, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition* (American Bar Association 2017)

The Sedona Conference, *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers* (November 2015)

US-CERT, part of the U.S. Department of Homeland Security, www.us-cert.gov, includes resources for implementing the NIST Framework (businesses www.us-cert.gov/ccubedvp/getting-started-business) and (small and midsize businesses www.us-cert.gov/ccubedvp/getting-started-smb)

III. Multijurisdictional Practice

A. Introduction

The practice of law for most attorneys in the United States today, driven by technology, mobility, and a global economy, is increasingly national and international. Within the U. S., practice for most attorneys is truly multijurisdictional, with both legal services and their impacts in multiple states. The term "multijurisdictional practice" ("MJP") is used to describe legal services by a lawyer across state lines or in a jurisdiction in which he or she is not admitted to practice. It includes services performed in the other jurisdiction through physical presence or through virtual presence (phone, teleconference, email, Internet, etc.). The state in which the lawyer is admitted is called "the home state." The state in which the services are performed is called "the host state." MJP raises significant issues like potential unauthorized practice of law, potential violation of ethics rules, and choice of law for ethics rules and disciplinary proceedings. It is important for lawyers whose practice may cross state lines (most lawyers today) to understand and address MJP issues.

MJP includes practice in another U.S. jurisdiction or a foreign jurisdiction by attorneys admitted in a U.S. jurisdiction and practice in the U.S. by attorneys admitted in foreign jurisdictions. This paper focuses on domestic MJP by attorneys admitted to practice in the U.S.

B. Overview of Multijurisdictional Practice Issues

There have been ongoing MJP issues for attorneys representing clients in the United States for years and they will certainly continue. The general practice of law in the United States is regulated by the states and each state has its own requirements for admission to practice. All U.S. jurisdictions have laws that restrict practice to authorized persons. States laws prohibiting the unauthorized practice of law generally provide for civil or criminal sanctions, including injunctions, fines, contempt, and even imprisonment.

An example is South Carolina's law that makes unauthorized practice a felony:

> No person may either practice law or solicit the legal cause of another person or entity in this State unless he is enrolled as a member of the South Carolina Bar pursuant to applicable court rules, or otherwise authorized to perform prescribed legal activities by action of the Supreme Court of South Carolina. The type of conduct that is the subject of any charge filed pursuant to this section must have been defined as the unauthorized practice of law by the Supreme Court of South Carolina prior to any charge being filed. A person who violates this section is guilty

> of a felony and, upon conviction, must be fined not more than five thousand dollars or imprisoned not more than five years, or both.[40]

MJP started to receive growing attention during the 1990s as some states started to take action against out of state attorneys who were not licensed to practice in the state.[41]

Another example is Pennsylvania's unauthorized practice law, which provides:

> Penalty for unauthorized practice of law
>
> (a) GENERAL RULE.-- Except as provided in subsection (b), any person, including, but not limited to, a paralegal or legal assistant, who within this Commonwealth shall practice law, or who shall hold himself out to the public as being entitled to practice law, or use or advertise the title of lawyer, attorney at law, attorney and counselor at law, counselor, or the equivalent in any language, in such a manner as to convey the impression that he is a practitioner of the law of any jurisdiction, without being an attorney at law or a corporation complying with 15 Pa.C.S. Ch. 29 (relating to professional corporations), commits a misdemeanor of the third degree upon a first violation. A second or subsequent violation of this subsection constitutes a misdemeanor of the first degree.[42]

These laws have historically been applied to lay persons who perform legal services and to disbarred or suspended lawyers who continue to practice. Starting in the late 1990s, unauthorized practice laws have also been applied to lawyers who perform legal services in a state in which they are not admitted to practice. *E.g.*, *Birbrower, Montalbano, Condon & Frank, P.C. v. Superior Court,* 949 P.2d 1 (Cal. 1998), *cert. denied,* 119 S. Ct. 291 (1998); *Koscove v. Bolte, Colo.,* 30 P.3d 784 (Colo. Ct. App. 2001), *cert. denied*, 534 U.S. 1128 (2002); *In Re Ferry*, 774 A.2d 62 (R.I. 2001) and *Florida Bar v. Rapoport,* 845 So.2d 874 (Fla. Feb. 20, 2003), *reh. denied*, 2003 Fla. LEXIS 793 (May 6, 2003).

At the time when these cases were decided, "[l]iterally, the law in most jurisdictions [was] highly restrictive, with no real allowance for multi-state matters except the possibility for admission pro hac vice in litigation matters."[43] There were particular concerns for MJP by transactional and in-house attorneys.

Birbrower was an early, high profile case in this area, in which the California Supreme Court held that a New York law firm engaged in unauthorized practice of law in California. The firm had performed substantial work in California for a California client (a subsidiary of a New York client), including meetings with the client's accountants, participating in strategy discussions, meeting with the opposing party, making a settlement demand, and filing a demand for arbitration. The

---

[40] S.C. Code Ann. § 40-5-310.

[41] ABA, "Client Representation in the 21st Century - Report of the Commission on Multijurisdictional Practice" (August 2002), available on the MJP Commission's website, see note 1, supra.

[42] 42 PA. CONS. STAT. ANN. § 2524.

[43] William T. Barker, "Extrajurisdictional Practice by Lawyers," 56 *Bus. Law.* 1501, 1505 (2001).

California UPL statute[44] provided that only members of the California bar may "practice law" "in California." The court explored the meaning of "in California:"

> Section 6125 has generated numerous opinions on the meaning of "practice law" but none on the meaning of "in California." In our view, the practice of law "in California" entails sufficient contact with the California client to render the nature of the legal service a clear legal representation. In addition to a quantitative analysis, we must consider the nature of the unlicensed lawyer's activities in the state. Mere fortuitous or attenuated contacts will not sustain a finding that the unlicensed lawyer practiced law "in California." The primary inquiry is whether the unlicensed lawyer engaged in sufficient activities in the state, or created a continuing relationship with the California client that included legal duties and obligations.

The court found that physical presence is one factor to be considered in the location of practice, but is not exclusive, and that one may engage in unauthorized practice without being physically present. Unauthorized practice can include services while present "in California," physically or "virtually:"

> Our definition does not necessarily depend on or require the unlicensed lawyer's physical presence in the state. Physical presence here is one factor we may consider in deciding whether the unlicensed lawyer has violated section 6125, but it is by no means exclusive. For example, one may practice law in the state in violation of section 6125 although not physically present here by advising a California client on California law in connection with a California legal dispute by telephone, fax, computer, or other modern technological means. Conversely, although we decline to provide a comprehensive list of what activities constitute sufficient contact with the state, we do reject the notion that a person *automatically* practices law "in California" whenever that person practices California law anywhere, or "virtually" enters the state by telephone, fax, e-mail, or satellite. (Citations omitted.)

The court held that the law firm could not recover fees for services performed "in California" under its definition, but could recover fees for services performed elsewhere.

The leading manual on attorney professional conduct explains the context of *Birbrower* as follows:[45]

> Few attorneys have ever refused to represent a client because the representation required occasional travel, letters, phone calls, faxes, or e-mails into jurisdictions in which they are not admitted. And, for the most part, authorities paid little

[44] CAL. BUS. AND PROF. CODE § 6125.

[45] *Lawyers' Manual on Professional Conduct* (ABA/Bloomberg Law), "Multijurisdictional Practice," p. 21:2107 (2009).

attention to these occasional intrusions or implemented formal methods to make allowance for attorneys' limited cross-border presence.

***

Birbrower set off a shock wave in the legal community.
(Emphasis added.)

C. Practice in Federal Courts and Before Federal Agencies

Practice of law that is *exclusively* in federal courts and before federal agencies is governed by federal law and is preempted from state regulation. For federal courts, long established case law holds that admission to practice is exclusively a federal issue. For example, the Ninth Circuit held in *In re Poole,* 222 F. 3d 618, 620-22 (9th Cir. 2000), that an attorney admitted to practice in bankruptcy court could recover fees despite the fact that he was not admitted to the state bar of Arizona where the bankruptcy court was located. Practice before federal agencies is governed by statute, 5 U.S.C. §500. In, *Sperry v. Florida, ex rel. Florida Bar,* 373 U.S. 379, 116 S. Ct. 1322 (1963) the Supreme Court held that Florida could not enjoin a nonlawyer who was registered to practice before the U.S. Patent Office from preparing and prosecuting patent applications in Florida because a federal statute[46] and regulations under it authorized the practice.

Admission to practice before the U.S. Supreme Court is governed by Supreme Court Rule 5, which provides:

> **Rule 5. Admission to the Bar**
>
> 1. To qualify for admission to the Bar of this Court, an applicant must have been admitted to practice in the highest court of a State, Commonwealth, Territory or Possession, or the District of Columbia for a period of at least three years immediately before the date of application; must not have been the subject of any adverse disciplinary action pronounced or in effect during that 3 year period; and must appear to the Court to be of good moral and professional character. …

Admission to practice before U.S. Courts or Appeals, for all circuits, is governed by Federal Rule of Appellate Procedure 45:

> **Rule 46. Attorneys**
>
> (a) Admission to the Bar.
>
> (1) *Eligibility.* An attorney is eligible for admission to the bar of a court of appeals if that attorney is of good moral and professional character and is admitted to practice before the Supreme Court of the United States, the highest court of a state, another United States court of appeals, or a United States district court

[46] 35 U.S.C. §112, giving the Commissioner of Patents authority to prescribe regulations governing practice by agents, attorneys and other persons.

(including the district courts for Guam, the Northern Mariana Islands, and the Virgin Islands).

Requirements for admission to practice before U. S. District Courts are governed by local rules of each court and are not uniform. Some districts, for full admission, require attorneys to be members of the bar of the highest court of the state (or U.S. jurisdiction) in which the district court is located. E.g., U.S. District Court for the Eastern District of Pennsylvania Local Rule 83.5. Others provide for full admission for attorneys admitted in the state in which the court is located, the U.S. Supreme Court, or any other U.S. District Court. E.g., U.S. District Court for the Western District of Pennsylvania LCvR 83.2.

While practice that is *exclusively* before federal courts or agencies is preempted and beyond state regulation, there is uncertainty as to the permissible bounds of such practice. In some practice areas, it may not be possible to operate an office exclusively for federal practice, with no practice of state law. For example, a bankruptcy attorney may advise clients about contract and state credit and property laws and an immigration attorney may deal with state contract, employment and licensing laws. *See. e.g., In the Matter of the Reinstatement of Diana Lynn Mooreland-Rucker,* 237 P.3d 784 (Ok. 2010), the dissent in *Rittenhouse v. Delta Home Improvements, Inc.,* 291 F.3d 925 (6th Cir. 2002), and *In re Marcone,* 2008 WL 6041371 at *7 (E.D. Pa. 2008).

D. ABA Commission on Multijurisdictional Practice

The ABA Commission on Multijurisdictional Practice was appointed in July of 2000 to study the application of current ethics and bar admission rules to the multijurisdictional practice of law.

The Commission issued its Final Report, *Client Representation in the 21st Century,* in June of 2002, which included nine recommendations:

1. Support the principle of state judicial regulation of the practice of law,

2. Amend Model Rule 5.5 to cover multijurisdictional practice,

3. Amend Model Rule 8.5 to clarify disciplinary jurisdiction over lawyers licensed in another jurisdiction,

4. Provide for effective disciplinary enforcement in a multijurisdictional context,

5. Use a national disciplinary data bank and reciprocal discipline,

6. Adopt a Model Rule on Pro Hac Vice admission,

7. Adopt a Model Rule on Admission by Motion,

8. Adopt a Model Rule for Licensing of Legal Consultants, and

9. Adopt a Model Rule on Temporary Practice by Foreign Lawyers.

All nine of the Commission's final recommendations were adopted by the ABA House of Delegates on August 12, 2002 and Model Rules 5.5 and 8.5 and the Model Bar Admission Rules were amended in accordance with them.

E. MJP Amendments to the ABA Model Rules

To implement the MJP Commission's recommendations, the ABA amended Model Rules 5.5 and 8.5 and the Model Bar Admission Rules.

1. ABA Model Rule 5.5 Unauthorized Practice of Law; Multijurisdictional Practice of Law[47]

First, the amendments expanded the first part of the rule, which prohibits attorneys admitted in the home jurisdiction ("outbound attorneys") from violating the rules in a host jurisdiction:

> (a) A lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction, or assist another in doing so.

It previously prohibited the unauthorized practice of law in another jurisdiction. It was expanded to cover rules regulating the practice of law in the other jurisdiction.

Next, it added (b), which covers practice in the jurisdiction by attorneys admitted elsewhere ("inbound attorneys").

> (b) A lawyer who is not admitted to practice in this jurisdiction shall not:
>
> (1) except as authorized by these Rules or other law, establish an office or other systematic and continuous presence in this jurisdiction for the practice of law; or
>
> (2) hold out to the public or otherwise represent that the lawyer is admitted to practice law in this jurisdiction.

The amendment added two provisions authorizing MJP, one on a temporary basis only and one on a temporary or continuous basis. These are the core of permitting MJP.

New subsection (c) permits MJP on **a temporary basis only**, in four circumstances:

> (c) A lawyer admitted 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:
>
> (1) are undertaken in association with a lawyer who is admitted to practice in this jurisdiction and who actively participates in the matter;
>
> (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;
>
> (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

[47] For later amendments to Model Rule 5.5 relating to limited practice by foreign in-house counsel, see Section 7 below.

> jurisdiction in which the lawyer is admitted to practice and are not services for which the forum requires pro hac vice admission; or
>
> (4) are not within paragraphs (c)(2) or (c)(3) and arise out of or are reasonably related to the lawyer's practice in a jurisdiction in which the lawyer is admitted to practice.

In addition to these new provisions for temporary MJP, new subsection (d) to Model Rule 5.5 permits MJP in two defined circumstances, whether it is **temporary or continuous**:

> (d) A lawyer admitted in another United States jurisdiction, and not disbarred or suspended from practice in any jurisdiction, may provide legal services in this jurisdiction that:
>
> (1) 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
>
> (2) are services that the lawyer is authorized to provide by federal law or other law of this jurisdiction.

The limits of a "temporary basis" and what is "continuous" are not entirely clear, resulting in uncertainty and risk following this amendment. For example, in a newsletter following adoption of Pennsylvania's version of Rule 5.5, the Disciplinary Board of the Supreme Court of Pennsylvania observed: "It should be emphasized that these are permitted only on a temporary basis. The lawyer who casually dispenses advice to and performs services for clients outside the jurisdiction where she or he is licensed runs a very serious risk of being charged with unauthorized practice of law, and may be subject to severe discipline. Attorney E-Newsletter (March 2007).

The Comment to Rule 5.5 provides some additional detail, but there is still much uncertainty:

> [4] Other than as authorized by law or this Rule, a lawyer who is not admitted to practice generally in this jurisdiction violates paragraph (b)(1) if the lawyer establishes an office or other systematic and continuous presence in this jurisdiction for the practice of law. Presence may be systematic and continuous even if the lawyer is not physically present here. Such a lawyer must not hold out to the public or otherwise represent that the lawyer is admitted to practice law in this jurisdiction. See also Rules 7.1(a) and 7.5(b).
>
> ***
>
> [6] There is no single test to determine whether a lawyer's services are provided on a "temporary basis" in this jurisdiction, and may therefore be permissible under paragraph (c). Services may be "temporary" even though the lawyer provides services in this jurisdiction on a recurring basis, or for an extended period of time, as when the lawyer is representing a client in a single lengthy negotiation or litigation. …

2. ABA Model Rule 8.5 Disciplinary Authority; Choice of Law

Model Rule 8.5 provides that a home state has jurisdiction over admitted attorneys, whether the conduct takes place in the home state or elsewhere, and a host state has jurisdiction over attorneys admitted elsewhere for conduct in the host state. Attorneys may accordingly be subject to discipline in both their home state and a host state for conduct committed in a host state. The Rule also provides for choice of law for disciplinary proceedings, looking at practice before tribunals, place of lawyer's conduct, and place of predominant effect.

The amendments clarified that attorneys not admitted in the jurisdiction are subject to discipline for practice in it and clarified choice of law for disciplinary proceedings. The amended rule provides:

> *Maintaining The Integrity Of The Profession*
> Rule 8.5 Disciplinary Authority; Choice Of Law
>
> (a) Disciplinary Authority. A lawyer admitted to practice in this jurisdiction is subject to the disciplinary authority of this jurisdiction, regardless of where the lawyer's conduct occurs. A lawyer not admitted in this jurisdiction is also subject to the disciplinary authority of this jurisdiction if the lawyer provides or offers to provide any legal services in this jurisdiction. A lawyer may be subject to the disciplinary authority of both this jurisdiction and another jurisdiction for the same conduct.
>
> (b) Choice of Law. In any exercise of the disciplinary authority of this jurisdiction, the rules of professional conduct to be applied shall be as follows:
>
> (1) for conduct in connection with a matter pending before a tribunal, the rules of the jurisdiction in which the tribunal sits, unless the rules of the tribunal provide otherwise; and
>
> (2) for any other conduct, the rules of the jurisdiction in which the lawyer's conduct occurred, or, if the predominant effect of the conduct is in a different jurisdiction, the rules of that jurisdiction shall be applied to the conduct. A lawyer shall not be subject to discipline if the lawyer's conduct conforms to the rules of a jurisdiction in which the lawyer reasonably believes the predominant effect of the lawyer's conduct will occur.

3. ABA Model Bar Admission Rules

The MJP Commission also recommended and the ABA approved model bar admission rules for In-house counsel, admission by motion, *pro hac vice* admission, and practice by foreign legal consultants.

Caution: In addition to complying with the host state's MJP rules, practice may require compliance with the host state's court or agency rules, bar admission rules, and other rules.

F. Implementation by the States

The ABA Model Rules of Professional Conduct, as their name indicates, are models for adoption by state ethics authorities. They are amended periodically by the ABA, like these MJP amendments, and it takes time after amendment for the various states to consider them and to adopt, partially adopt, or reject amendments. For example, Arizona and New York adopted MJP rules in 2015 and Kansas, Washington, and West Virginia adopted MJP rules in 2014 – all over a decade after adoption of the ABA MJP amendments.

As of May 16, 2016, 13 states had adopted rules identical to amended Model Rule 5.5 and 33 states and the District of Columbia had adopted rules similar to it.[48] This leaves only Hawaii, Mississippi, Montana, and Texas as the only states without similar rules.

As of October 6, 2014, 25 states had adopted rules identical to amended Model Rule 8.5 and 20 states plus the District of Columbia had adopted rules similar to it.[49] This leaves Alabama, Hawaii, Kansas, Mississippi, and Texas as the only states without similar rules.

Details on state adoption of the Model Rules on MJP, practice by in-house counsel, admission by motion, *pro hac vice* admission, and practice by foreign legal consultants are reported in charts available on the MJP Commission's website.[50]

Caution: Some states have more restrictive rules for permitted MJP and some have additional requirements for MJP beyond those in the Model Rules, like registration and payment of fees. It is critical to understand and comply with the relevant state(s)' rules.

G. Challenges to Bar Admission Requirements

A number of constitutional challenges have been brought over the years to state bar admission requirements and to more restrictive rules for practice before some U.S. District Courts. They have been based on theories like the Privileges and Immunities Clause, Equal Protection, and the Commerce Clause. A number of them have been brought by the National Association for the Advancement of Multijurisdiction Practice (NAAMJP).[51] Except for some challenges to state residency requirements, they have been unsuccessful.

During the 1980s the Supreme Court held that state residency requirements for bar admission were unconstitutional under the Privileges and Immunities Clause: *Supreme Court of New Hampshire v. Piper,* 470 U.S. 274 (1985) (residency requirement for admission to New Hampshire Bar is unconstitutional under the Privileges and Immunities Clause – the right to practice law is a fundamental right and the state did not establish that the requirement bears a close relationship to a state objective) and *Supreme Court of Virginia v. Friedman,* 108 S. Ct. 2260 (1988) (Virginia

---

[48] See, ABA Quick Guide Chart on State Adoption of Rule, 5.5, (link on the ABA Commission on Multijurisdictional Practice website, Note 1 above).

[49] See, ABA Quick Guide Chart on State Adoption of Rule, 8.5, (link on the ABA Commission on Multijurisdictional Practice website, Note 1 above).

[50] ABA Commission on Multijurisdictional Practice website, Note 1 above.

[51] www.mjplaw.org/about_us.html.

residency requirement for admission by motion is unconstitutional under the Privileges and Immunities Clause).

In *Schoenefeld v. New York*, 907 F. Supp. 2d 252 (N.D. N.Y. 2011), the court held that a New York bar admission law requiring nonresident attorneys to have an office in New York is unconstitutional. In *Schoenefeld v. Schneiderman*, 821 F.3rd 273 (2nd Cir. 2015), after certification of a question of interpretation to the New York Court of Appeals, the Second Circuit reversed the district court's decision. The court of appeals held that the law does not violate the Privileges and Immunities Clause since it was enacted to eliminate a service of process concern and not for the protectionist purpose of favoring New York residents in their ability to practice law.

Most states have provisions for attorneys admitted and in good standing in other states to be admitted on motion if they meet requirements like a set number of years of full time practice.[52] Many of them require reciprocity – providing admission on motion only for attorneys admitted in states that offer reciprocal admission on motion. The constitutionality of reciprocity has been upheld. *E.g., Nat'l Ass'n for the Advancement of Multijurisdiction Practice (NAAMJP) v. Castile,* 799 F.3d 216 (3rd Cir. 2015) (Pennsylvania bar admission rule that allows admission on motion only for attorneys admitted in reciprocal states is constitutional) and *N.A. for the Advancement of Multijurisdiction Practice v. Berch,* 773 F.3d 1037 (9th Cir. 2014) (Arizona bar admission rule that allows admission on motion only for attorneys admitted in reciprocal states is constitutional.)

As discussed above, some federal districts, for full admission to practice, require attorneys to be members of the bar of the state in which the court is located while others have more permissive rules. The validity of the state bar admission requirement has been upheld. *E.g., NAAMJP v. Simandle,* 2015 U.S. Dist. LEXIS 115865 (D. N.J. Sept. 1, 2015), *aff'd,* 2016 U.S. App. LEXIS 12930, (3rd Cir. July 14, 2016) (District of New Jersey local rule requiring attorneys to be members of the New Jersey Bar for full admission is valid.) The court noted:

> To my knowledge, in none of these cases has NAAMJP been successful. I mention this history only to put this case in context, and not in criticism of NAAMJP for pursuing its cause.

H. The Colorado "Driver's License" Approach

For a number of years, Colorado has taken a very permissive approach to MJP that generally allows lawyers admitted and in good standing in other states to practice in Colorado as long as they do not establish residences in Colorado or open offices in there.[53] Pro hac vice admission is required for practice before Colorado courts and agencies.[54] Lawyers practicing under this rule

---

[52] www.BarReciprocity.com is a website that "summarizes and consolidates attorney admissions information relating to the bar exam, score transfers, bar reciprocity, and bar admission exemptions."

[53] Col. R. C. P. 220(1).

[54] Col. R. C.P. 220(2).

are subject to the Colorado Rules of Professional Conduct and are deemed to have obtained licenses in Colorado.[55] This MJP approach has been called the "driver's license" rule since it operates much the same way as laws covering driver's licenses that are broadly valid in other states, subject to each state's vehicle and traffic laws.[56]

I. The ABA Commission on Ethics 20/20

Review of MJP issues at the ABA has continued. In 2010, the ABA President appointed the ABA Commission on Ethics 20/20 "to perform a thorough review of the ABA Model Rules of Professional Conduct and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments."[57]

In 2012, the 20/20 Commission recommended and the ABA adopted (1) an amendment to the Model Rule on Admission by Motion to reduce the required time of practice in another jurisdiction from five years to three years and (2) adoption of a new model rule to permit practice for up to one year while a lawyer admitted elsewhere is seeking admission by motion.

In early 2013, the Commission also referred to the Standing Committee on Ethics and Professional Responsibility, for a formal ethics opinion, issues of the meaning of "systematic and continuous presence" of a lawyer in the context of "virtual presence." This is likely to be an important issue, as attorneys continue to become increasingly mobile and continue to use developing technologies. The Commission explained the issue as follows:

> …technology now enables lawyers to be physically present in one jurisdiction, yet have a substantial virtual practice in another. The problem is that it is not always clear when this virtual practice in a jurisdiction is sufficiently "systematic and continuous" to require a license in that jurisdiction. Currently, Comment [4] to Model Rule 5.5 identifies these issues, but provides limited guidance as to how to resolve them. The Comment states that a lawyer's "[p]resence may be systematic and continuous even if the lawyer is not physically present" in the jurisdiction. Neither the Rule nor the Comment provides any clarity as to when a lawyer who is "not physically present" in a jurisdiction nevertheless has a systematic and continuous presence there.[27]
>
> ---
>
> [27] Conversely, a lawyer may be licensed in one jurisdiction, but live in a jurisdiction where the lawyer is not licensed. If the lawyer conducts a virtual practice from the latter jurisdiction and serves clients only in the jurisdiction where the lawyer

---

[55] Col. R.C.P. 220(3) and (4).

[56] James Geoffrey Durham, "Is the ABA Ready for the Driver's License Rule?" Probate & Property, 54-60 (November/December 2011).

[57] See, the ABA Commission on Ethics 20/20 website, hwww.americanbar.org/groups/professional_responsibility/committees_commissions/standingcommitteeonprofessionalism2/resources/ethics2020hompeage .

> is actually licensed, there is a question of whether the lawyer has a "systematic and continuous" presence in the jurisdiction where the lawyer is living and thus violates Rule 5.5(b) in that jurisdiction. The Rule is unclear in this regard as well.

In early 2013, the Ethics 20/20 Commission recommended and the ABA adopted an amendment to Model Rule 5.5 that permits limited practice by foreign in-house counsel and a Model Rule for Registration of In-House Counsel to implement it. At the 2016 Midyear Meeting, the ABA expanded the definition of "foreign lawyer" in Model Rule 5.5 and the Model Rule for Registration of In-House Counsel to include some foreign lawyers who were not covered in the prior definition.

J. Continuing Multijurisdictional Issues

After the MJP Commission's work and the adoption of its recommendations in 2002, MJP issues have continued in practice. This is due to factors like differing state definitions of "unauthorized practice," uncertainty about what is "temporary," "continuous," and virtual presence," and lack of specificity in the amended Model Rules and state variations in adopting them.

A law review note in 2009, seven years after adoption of the ABA MJP Model Rules, summarized it this way:

> Scholars generally agree that the current MJP rules are unnecessarily complicated, opaque, and varied, leading to confusion amongst even the best-intentioned attorneys over what is a violation.[58]

Several ethics opinions and court opinions have addressed MJP issues in the years following the 2002 amendments of the ABA rules. The following are some examples.

For an ethics opinion that address MJP issues under an amended state rule that follows the ABA approach (with some variation and additional registration requirements), see New Jersey Committee on the Unauthorized Practice of Law Opinion 49, "Multijurisdicational or Crossborder Practice" (October 2012). It discusses the general issues and concludes that an out-of-state lawyer, representing an out-of-state buyer, may prepare a contract for purchase of New Jersey real estate if the requirements of the MJP rule and registration requirements are satisfied.[59]

In Opinion No 12-09, the Illinois State Bar Association decided that a lawyer not admitted in Illinois could not work primarily in Illinois - even in an association with an Illinois licensed partner who would act in all Illinois matters and supervise the non-admitted lawyer, who would concentrate his practice in that lawyer's admitting jurisdiction. The activity under review constituted "systematic and continuous" presence, in violation of Illinois RPC Rule 5.5(b). In Opinion No 13-08, the Association concluded that "An out-of-state lawyer may practice

---

[58] Sara J. Lewis, "Note: Charting the 'Middle' Way: Liberalizing Multijurisdictional Practice Rules for Lawyers Representing Sophisticated Clients," 22 Geo. J. Legal Ethics 631, 643 (2009).

[59] Available at www.judiciary.state.nj.us/notices/2012/n121004c.pdf.

immigration law in Illinois with the use of a properly supervised nonlawyer in Illinois who collects information to be used by the lawyer in filling out immigration forms."[60]

The Arizona UPL Committee determined in UPL Advisory Opinion 10-02 that an out-of-state lawyer not admitted in Arizona could not practice law while in Arizona, even if limited to the law of the lawyer's licensed jurisdiction, other than on the temporary basis allowed under Arizona RPC Rule 5.5.[61]

In *Gould v. Florida Bar,* 259 F. App'x 208 (11th Cir. 2007) the Second Circuit upheld a determination by the Florida Bar that an attorney had engaged in unauthorized practice there. An attorney who was a member of the New York bar opened an office in Florida, and advertised that from that location he would counsel persons about New York legal matters only. The court agreed with the Florida Bar that such activity was unlawful under a Florida statute that made it unlawful for anyone not licensed in Florida to practice law in the state. This opinion stands for the proposition that practicing *any* law is subject to law practice regulation of the jurisdiction in which the "activity" occurs, even if practice is limited to the law of a jurisdiction where the lawyer is admitted.

The Oklahoma Supreme Court reviewed a bar applicant's potential unauthorized practice in another state in *In re Mooreland-Rucker*, 237 P.3d 784 (OK 2010). A lawyer admitted to practice in Oklahoma had moved to Texas to work in the U.S. Trustee's office, and was admitted in the federal courts in Texas. After leaving her employment, she practiced bankruptcy law in Texas, but was not admitted to the Texas bar. She allowed her Oklahoma bar membership to lapse. On application for reinstatement, the Supreme Court of Oklahoma granted reinstatement, but found that her practice in Texas violated Oklahoma Rule 5.5(a) and constituted UPL in Oklahoma – even if it was not determined to be unauthorized under Texas rules.

In *In re Carlton*, 708 F. Supp. 2d 524 (D. Md. 2010), the court explored the location of the principal law office of a telecommuting attorney. A member of the District of Columbia bar, also admitted to practice in the District Court for the District of Maryland, worked for a DC law firm. She lived in Massachusetts, and did most of her work from home or an office space in Boston, but met with clients in the DC office. She was not a member of the Massachusetts Bar, and did not hold herself out as a Massachusetts lawyer. The district court's rule required that a lawyer admitted to its bar must be a member in good standing of the highest court in a state (or District of Columbia) in which the attorney maintains his or her principal law office, or of the Maryland bar. In addressing the apparent failure to satisfy this requirement, it was argued that the lawyer's office was not where she was physically but where she practiced by telecommuting - DC. She received her mail at the DC office and it was forwarded to her in Massachusetts and she used the DC phone number to place and receive calls. She sent and received electronic communications wherever she was. This satisfied the court, which pointed to her nexus to the DC firm as her home for purposes of malpractice coverage, tax obligations, client trust fund obligations and the database (files,

[60] Both available at www.isba.org/ethics.

[61] Available at http://www.azbar.org/media/75280/upl10-02.pdf.

accounting records, research) and technology on which she relied was in the DC office although she reached them by telecommuting.

The Minnesota Supreme Court, with three justices dissenting, affirmed a sanction of a private admonition of a Colorado attorney for unauthorized virtual practice in Minnesota in *In re Charges of Unprofessional Conduct in Panel File No. 39302*, 884 N.W.2d 661 (Minn. 2016). The Colorado attorney negotiated by e-mail from Colorado with a Minnesota attorney to attempt to resolve a Minnesota judgment against his in-laws who resided in Minnesota. He also communicated with his clients from Colorado. The Minnesota attorney filed an unauthorized practice complaint about the Connecticut attorney.

The court first found that the Appellant had practiced law in Minnesota:

> The reasoning in *Birbrower* is persuasive. Based on that reasoning, we conclude that the Panel did not clearly err by finding that appellant practiced law *in* Minnesota, in violation of Minn. R. Prof. Conduct 5.5(a). Appellant contacted D.R., a Minnesota lawyer, and stated that he represented Minnesota clients in a Minnesota legal dispute. This legal dispute was not interjurisdictional; instead, it involved only Minnesota residents and a debt arising from a judgment entered by a Minnesota court. Appellant instructed D.R. to refer all future correspondence to him, and he continued to engage in correspondence and negotiations with D.R. over the course of several months. Appellant requested and received financial documents from his Minnesota clients and advised them on their legal options. By multiple e-mails sent over several months, appellant advised Minnesota clients on Minnesota law in connection with a Minnesota legal dispute and attempted to negotiate a resolution of that dispute with a Minnesota attorney. Appellant had a clear, ongoing attorney-client relationship with his Minnesota clients, and his contacts with Minnesota were not fortuitous or attenuated. Thus, there is ample support for the Panel's finding that appellant practiced law in Minnesota.

After finding that that the attorney had practiced law *in* Minnesota, the court held that none of the authorized exceptions for multijurisdictional practice in the Minnesota Rules of Professional Conduct (based on the ABA Model Rules) authorized this remote practice. The court accordingly affirmed the finding of misconduct and the sanction of a private admonition. It agreed that the nature of the misconduct was non-serious.

In a recent application of updated rules on multijurisdictional practice, the Ohio Supreme Court held that an attorney engaged in authorized temporary multijurisdictional practice in Ohio. *In re Application of Jones*, 123 N.E.3d 877 (Ohio 2018). The attorney was admitted to practice in Kentucky and practiced with a firm there. Her firm merged with an Ohio-based firm and she moved to Ohio to work in one of the firm’s Ohio offices. She applied for admission to the Ohio bar and continued to do legal work for Kentucky clients from the Ohio office while her application was pending. She also continued to maintain a Kentucky office and travelled to Kentucky. The Ohio Board of Commissioners on Character and fitness recommended disapproval of attorney's application based on a determination she engaged in unauthorized practice of law by practicing Kentucky law from an Ohio office during pendency of the application.

The Ohio Supreme Court approved the application, holding:

> A lawyer admitted to practice law in another jurisdiction who provides legal services exclusively in that jurisdiction from an office in Ohio pending resolution of an application for admission to the Ohio bar without examination and who otherwise complies with the provisions of Prof.Cond.R. 5.5(c) is providing legal services on a temporary basis and therefore has not engaged in the unauthorized practice of law.
>
> *Id.* at 878.

One justice, concurring in the judgment only, concluded that the attorney's practice violated the Ohio UPL rules, but found the rules to be unconstitutional as applied to her practice. He concluded:

> I would conclude that as applied to an out-of-state attorney who is not practicing in Ohio courts or providing Ohio legal services, Prof.Cond.R. 5.5(b)(1) violates Article I, Section 1 of the Ohio Constitution and the Due Process Clause of the Fourteenth Amendment to the United States Constitution. As applied to such an attorney, the rule violates Article I, Section 1 both because it does not "bear[ ] a real and substantial relation to the public health, safety, morals, or general welfare" and because it is "arbitrary" and "unreasonable," Similarly, applying the rule to such an attorney violates the Fourteenth Amendment because it does not bear a rational relationship to any discernable state interest.
>
> *Id.* at 886-887 (citations omitted)

This case demonstrates the continuing uncertainty in the application of the updated MJP rules, including potential constitutional considerations. If the Board's decision had been final, the attorney would have been denied admission to practice in Ohio.

The consequences of failing to understand and comply with MJP and UPL rules can be serious or even devastating. For example, in March, 2004, a grand jury in North Carolina indicted two Georgia lawyers and their law firm for unauthorized practice of law in North Carolina. The services at issue were in a grade-fixing investigation for a North Carolina college, including witness interviews, review of college records, correspondence with the community, and issuance of a report.[62]

K. Conclusion

It is critical for attorneys who are engaging in or contemplating engaging in MJP to carefully review and address unauthorized practice laws, ethics rules, bar admission rules, and any applicable court or agency rules in their home jurisdiction and relevant host jurisdiction(s).

---

[62] 20 *Lawyers Manual on Professional Conduct* (ABA/Bloomberg Law) 203 (Apr. 24, 2004).

L. Additional Information

American Bar Association Commission on Multijurisdictional Practice website, www.americanbar.org/groups/professional_responsibility/committees_commissions/commission-on-multijurisdictional-practice

American Bar Association, *Model Rules of Professional Conduct, 2020 Edition*

Lawyers' Manual on Professional Conduct (ABA/Bloomberg Law), "Multijurisdictional Practice," pp. 21:2101 et seq. (2009)

Stephen Gillers, "A Profession If You Can Keep It: How Information Technology and Fading Borders Are Reshaping the Law Marketplace and What We Should Do About It," *Hastings L.J.* (2012)

Geoffrey C. Hazard, Jr., W. William Hodes and Peter R. Jarvis, *The Law of Lawyering, Fourth Edition* (Wolters Kluwer November 2019 update), Chp. 46, "Unauthorized Practice of Law," and Chp. 66, "Multijurisdictional Lawyering: The Jurisdictional Reach of Disciplinary Authorities and Choice of Law Issues in Lawyer Discipline"

David G. Ries, "Multijurisdictional Practice: the Ethics of Lawyering Here, There and Anywhere," *58 Rocky Mtn. Min. L. Inst. 13-1* (2012)