WHITE PAPER

Legal Ethics in the Digital Age

The legal industry is in a period of transformation that is going to continue for years to come. Legal departments, law firms, service providers, and other legal professionals are being more strategic with tech investments and partnerships. In the midst of change, lawyers must not discount the ethical obligations owed to clients. It is crucial to factor ethics into any changes in workflows, practice habits, and tech usage. While change is necessary and beneficial, it must be done carefully to avoid ethical violations that could provide reputational harm not only to the lawyer, but also the organization.

Just like medical professionals, lawyers take an oath to behave ethically and are held to a high standard of care when it comes to their clients and offering legal advice. Before the world went digital, these obligations were more predictable. Take the duty of confidentiality. What did that require pre-digitization? 1) Physically secure hard copy documents containing sensitive information. 2) Do not discuss client matters with anyone outside the legal team. 3) Conduct client and case strategy meetings face-to-face or over the phone in a private setting. These were considered adequate measures to fulfill the duty of confidentiality before digital communication and storage became the norm.

Now, data security needs to be considered before sending that text over an app or investing in new tech to help with information governance or privacy initiatives. While decades have passed since digitization begun, lawyers need to be mindful of how ethics plays a role in their everyday operations more than ever before given the explosion of emerging technologies in business over the past few years.

Lawyers must remain informed on new American Bar Association (ABA) and state bar developments. Most states follow the ABA Model Rules closely and employ the same core principles. Even so, there are still supplementary directives guiding practice in each state. It is crucial to know the rules and opinions from the ABA and any state for which the lawyer practices in to remain compliant. Keep informed on best practices for remaining ethical when interacting or practicing digitally. While there is a good amount of guidance on digital practice, given the prevalence of remote culture in business along with legal's foray into modern law it is safe to anticipate updated guidance in the coming years.

KEY ETHICAL OBLIGATIONS

Remaining ethical is the cornerstone of legal practice, as lawyers take oaths to act in accordance with the law and represent their client's best interests. The legal industry is in the most dynamic phase it has ever been with modern technology continuing to enter the market and trend. This means that ethical duties will keep evolving to keep pace.

Here are the major ethical duties that are heightened in the digital age.

1. **Competence:** ABA Model Rule 1.1 states that attorneys must provide clients with competent representation. What qualifies as competence will depend on the field of law and scope of representation. In 2021, the rule was expanded to require attorneys to keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.[1] This includes understanding the basic features of technology commonly used in legal practice.[2] The expansion of competence has become critical as new technologies enter the scene.

   General consensus is that at minimum, lawyers must keep informed about innovative trending technologies and basic features to remain competent. Lawyers must diligently research new technology and/or the reputation of potential partner providers before bringing tools in house or outsourcing. Understanding benefits and risks also helps the legal team make educated decisions about where to allocate legal spend and confidently demonstrate these choices to leadership and increase buy-in potential.

[1] ABA Model Rule 1.1 - Comment 8, Competence
[2] ABA Formal Opinion 477R* (May 11, 2017; Revised May 22, 2017).

2. **Communication:** ABA Model Rule 1.4 requires transparent communication so clients can make informed decisions regarding representation.[3] Best practice is to provide clients with notice on tech usage relating to their case as needs evolve. Being transparent demonstrates value, fosters collaboration, and helps avoid billing disputes.

3. **Confidentiality:** ABA Model Rule 1.6 mandates that client information be kept confidential.[4] In a digital world, this requires an extra layer of vetting to ensure all tools used in-house and via third parties are secure and will protect sensitive client data.

4. **Oversight:** The rise in collaborative business models coupled with ethical legal duties makes it crucial for lawyers to oversee work performed by any outside partners. Several ABA rules[5] hold lawyers responsible for the work of their team, both internal support staff and external providers.

The EDRM concisely summarized the importance of a lawyer's supervisory obligation: "In the realm of eDiscovery, this becomes particularly important because, as stated in Model Rule 5.4, any provider that is not 100 percent attorney owned and any employees that are not licensed in the jurisdiction in which they are employed are not authorized to practice law. Therefore, law firm and in-house attorneys must provide adequate oversight over any work done by litigation support and discovery service providers."[6] This rule of thumb should not only be followed for litigation partnerships, but when using a provider or consultant for any purpose – especially when client data is being transmitted or stored as a part of the project.

While all ethical duties are equally important to uphold, the legal industry must be cognizant of how digitization and technology influences certain obligations like those outlined above. An article highlighting the ABA's 2021 summit noted:

> "More and more states are adopting ethics rules that obligate attorneys to be competent in technology. Lawyers can no longer hide their heads in the sand when it comes to technological advancements. In most jurisdictions, computer literacy is a requirement. Courts have even sanctioned lawyers and clients who fail to use technology properly. But at the same time, advancing technology can create advancing ethical issues in litigation. Judges and lawyers will continue to grapple with the intersection between ambiguous ethics rules and ever-increasing technological capabilities."[7]

The article covered several areas where ethical obstacles surface and present unique challenges for legal professionals. This included AI, social media, and remote working.[8] It is necessary to have strategies around ethical compliance in these and other areas that have emerged in the digital age.

[3] ABA Model Rule 1.4
[4] ABA Model Rule 1.6
[5] See ABA Model Rules 5.1, 5.3, 5.4, and 5.5
[6] The Use of Artificial Intelligence in eDiscovery, p. 9-10 (Electronic Discovery Reference Model Feb. 2021).
[7] Nelson, Kip. Legal Ethics 2.0: How Emerging Technologies Are Creating Novel Ethical Dilemmas ABA (Feb. 4, 2022) https://www.americanbar.org/groups/judicial/publications/appellate_issues/2022/winter/legal-ethics-2/
[8] Nelson, Kip. Legal Ethics 2.0: How Emerging Technologies Are Creating Novel Ethical Dilemmas ABA (Feb. 4, 2022) https://www.americanbar.org/groups/judicial/publications/appellate_issues/2022/winter/legal-ethics-2/

DATA SECURITY

Data security is the optimal place to start, as keeping client communications and data safe is the cornerstone of legal ethics. The vulnerabilities and risks that are present in emerging technologies and digital business models must be a top concern. Understanding the importance of data security and how to implement effective practices is crucial. Data security essentially refers to the processes, policies, and programs that operate to protect vulnerable data from cyber-attacks. Since lawyers regularly handle sensitive information, such as personal client identifiers and trade secrets, it is very important to implement strong security systems and protocols. While there are laws and regulations that apply to data security and breaches, the separate ethical duties in the legal space add another layer to compliance and can result in disciplinary action when gone unfulfilled.

Keeping data secure goes hand in hand with technological competence, confidentiality, communication, and oversight obligations. Below are four key illustrations of how data security and legal ethics intertwine.

#1: Appropriately Securing Digital Communications

The duties of competence and confidentiality come into play with data security ethics, as lawyers should only use secure solutions and continuously monitor data security on a firm's network to protect sensitive client data from hackers or inadvertent disclosure. On May 22, 2017, the ABA issued an opinion about the security of digital communications involving protected client information. Six years later, this opinion is still relevant and acts as a guide for securing data when using emerging technologies to conduct business. Lawyers are required to take reasonable measures to prevent unauthorized or inadvertent access to the transmitted data.[9] The ABA had not comprehensively tackled this topic since 1999 when addressing email security[10], and the world is obviously a lot different now with the main form of communication and conducting business being through digital platforms. Here are some key points from that opinion:

[9] ABA Formal Opinion 477R* (May 11, 2017; Revised May 22, 2017)
[10] ABA Formal Opinion 99-413 (March 10, 1999)

- Lawyers must take reasonable efforts to safeguard client communications. Reasonableness will depend on the situation, as some communication may require a higher degree of protection than others such as when they involve a client's trade secrets or trial strategy. Other factors to consider include the type of digital mediums involved and available security measures, which can vary. The ABA commented that "the reasonable efforts standard 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."[11]

- Consider the following factors before determining appropriate security measures: 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).[12] This will help determine whether strong measures like encryption or firewalls are necessary. Some communication is so sensitive that lawyers should just consider discussing the subject with the client in person to avoid any inadvertent disclosure. Conversely, low risk communication will require standard security measures that are generally less costly and easier to implement.
- Using multiple devices and incorporating emerging technologies can make it difficult to know where to start with securing digital client communications. The ABA provides lawyers with guidance on this topic by offering best practices for making data security decisions.[13] This includes understanding the nature of the threat; understanding how organizations transmit and store client confidential information; understanding and using electronic security measures; determining how to protect electronic communications about client matters; labeling client confidential information; training lawyers and nonlawyer assistants in technology and information security; and conducting due diligence on vendors providing communication technology.

The major takeaway here is that choosing appropriate security measures will be highly fact specific. It is crucial to balance the nature of communication or data being transmitted, breach risk, cost, and industry best practices. Remaining educated on trending attack methods is an important piece here, as threat actors switch this up frequently. Communicating over certain apps or from unsecure locations also increases the risk of data interception. Failure to consider these risks and discuss security measures with clients can lead to ethical consequences.[14] This will also feed into incident response programs, which more organizations are prioritizing in the digital age.

[11] ABA Formal Opinion 477R* p.4 (May 11, 2017; Revised May 22, 2017)
[12] ABA Formal Opinion 477R* p.4-5 (May 11, 2017; Revised May 22, 2017)
[13] ABA Formal Opinion 477R* p. 6-10 (May 11, 2017; Revised May 22, 2017)
[14] ABA Model Rule 1.4 requires lawyers to inform clients of risks associated with certain electronic transmission of confidential client data.

#2: Remote Working

Conducting business remotely is no longer a luxury, but instead the norm across several industries. With this brings extra security concerns to ensure work completed offsite remains protected. Communicating over public wi-fi or on devices that are not company owned raises data security issues.

When conducting business in a public location, the Wi-Fi available is often unsecure and breeding grounds for potential hackers. Several states have addressed this issue over the years and advise against conducting business over public Wi-Fi unless the lawyer takes extra steps to secure client data when conducting business. According to a California opinion issued back in 2010, necessary measures include encrypting files or using a virtual private network (VPN).[15] Even if a state has not specifically addressed this topic, it is still covered or implied by most states' rules and other opinions about competence, confidentiality, and general technology usage. Lawyers should also take extra steps to secure any mobile device containing client information. This includes implementing complex passwords, remote wiping, encryption, two-factor identification, inactivity timeouts, authorization before downloading applications, and automatic wiping after a few incorrect access attempts. [16]

Since the rise of remote work during the pandemic, there has been a new comprehensive opinion on this topic. The ABA explicitly permits virtual practice, defined as technologically enabled law practice beyond the traditional brick-and-mortar law firm. However, the opinion reminded practitioners not to discount the intersection of data security and legal ethics:

> "When practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies." [17]

Best practices for keeping data secure include but are not limited to careful review of software terms of service, installing security updates, creating strong passwords, encryption and VPNs. When using a virtual meeting platform or videoconferencing app, find out if a certain app or platform records conversations or creates a transcript so they can get client consent before conducting a meeting. Also, disable devices with listening features when communicating about client matters. Periodical assessment is necessary due to the quick rate technology is evolving. [18]

To carry out best practices across legal teams, it is crucial to implement policies that promote technological competence and provide mandatory training on these topics. Lawyers need to ensure that the subordinates they supervise keep up to date on new technologies and implement proper security measures because senior lawyers can face ethical violations for inadequate supervision that results in an ethical violation. In the remote working world, having checks and balances on device and tech usage is critical to maintaining an ethical practice.

[15] See State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179, p. 7 (2010);
[16] Christie Jr., J.S. Ethics in a Digital World: What Should an Ethical Lawyer Know about Technology? ABA Section of Labor and Employment Law Employee Benefits Committee 2018 Midwinter Meeting, p. 11 (Feb. 9, 2018)
[17] ABA Formal Opinion 498 (March 10, 2021)
[18] ABA Formal Opinion 498 (March 10, 2021)

#3: Outsourcing

The concept of legal outsourcing tasks is not new, but the frequency and type of work being outsourced is changing in the new era of law centering around hybrid work models. This is an instance of where a lawyer's ethical duties extend to third-party oversight. The ABA formally authorizes outsourcing legal and nonlegal support services when attorneys maintain competent representation, comply with duties related to supervision and assistance, notify clients, and receive informed consent from clients if the provider will be handling confidential data.[19] It is crucial to review any state-specific opinions touching on provider partnerships. For example, most states have issued opinions authorizing partnerships with providers for cloud computing if the provider deploys appropriate security measures. This is a capability many organizations are expanding for various legal services, compliance, information management, and retention. The consensus is that cloud solutions are beneficial and appropriate if lawyers take reasonable care to maintain client confidentiality and data security when choosing a provider.

The ABA proclaimed: "Lawyers practicing virtually (even on short notice) must have reliable access to client contact information and client records. If the access to such "files is provided through a cloud service, the lawyer should (i) choose a reputable company, and (ii) take reasonable steps to ensure that the confidentiality of client information is preserved, and that the information is readily accessible to the lawyer." Lawyers must ensure that data is regularly backed up and that secure access to the backup data is readily available in the event of a data loss. In anticipation of data being lost or hacked, lawyers should have a data breach policy and a plan to communicate losses or breaches to the impacted clients." [20]

As an illustration at the state level, the Illinois State Bar Association takes the following stance on cloud computing involving a third-party when storing client data: "A lawyer may use cloud-based services in the delivery of legal services provided that the lawyer takes reasonable measures to ensure that the client information remains confidential and is protected from breaches. The lawyer's obligation to protect the client information does not end once the lawyer has selected a reputable provider."[21] While specifically addressing cloud services, this sentiment applies across the board when using an ALSP for various tasks – from eDiscovery to breach response and beyond. Organizations should vet and audit their provider partners and technology to ensure everything is above board. This is an important step regardless to monitor success for meeting legal transformation goals and lessen the risk of ethical complaints from clients or delayed matters due to insufficient processes.

#4: Cyber Education

Many state bars require lawyers to obtain continuing legal education credits each year. In 2022, the New York State Bar became the first to outwardly recognize the importance of cyber education. New CLE requirements for lawyers take effect on July 1, 2023. They must obtain one hour of credit to satisfy their CLE requirement from the newly created "Cybersecurity, Privacy and Data Protection" category.[22] This encompasses ethical obligations and general practice considerations that intertwine with these topics, providing a broad range of educational opportunities to explore.

[19] ABA Formal Opinion 08-451 (August 5, 2008).
[20] ABA Formal Opinion 498 (March 10, 2021)
[21] ISBA Op. 16-06 (2016).
[22] New CLE Requirement: Cybersecurity, Privacy and Data Protection, New York City Bar (Dec. 2, 2022) https://www.nycbar.org/media-listing/media/detail/new-cle-requirement-cybersecurity-privacy-and-data-protection

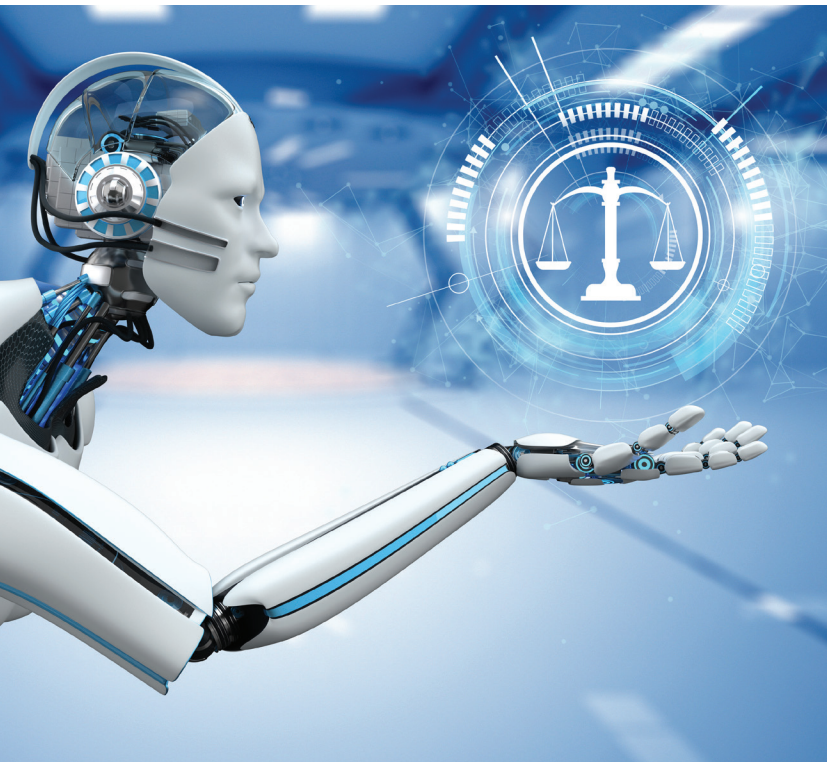
The reasoning behind this update was to shift focus to pressing issues in the legal industry relating to data protection, truly illustrating how integral good data hygiene is to ethical compliance. Law firms and other legal organizations house a significant amount of proprietary client information including communications, case strategy, financial data, trade secrets, and more. If a hacker obtains access to a legal organization's systems or email accounts, the fallout can be monumental. Accounting for applicable data privacy laws adds an extra layer of compliance duties relating to this information. Incorporating education on these topics is meant to help attorneys understand not only their obligations, but also the proper safeguarding of sensitive data and incident response best practices. This is important education for all layers, regardless of their state's CLE requirements.

EMERGING TECHNOLOGIES

Lawyers always have to account for their ethical obligations when dealing with emerging technologies. Confidentiality and competence are two major duties that surface with tech usage. Even if someone chooses not to utilize all the latest technologies, they still need to be aware of the tools other lawyers in the same practice area are using and understand the basics or obstacles that may surface. This trend has materialized over the year with AI usage in legal practice. Most litigators regularly use technology assisted review (TAR) for eDiscovery purposes or are at minimum educated about function, benefits, and risks.

It is also of the utmost importance to know how platforms, apps, and devices operate before using one for a client or other work-related matter and to ensure that there are no serious security risks present. Without competence in situations like these or holding onto the unwillingness to adopt emerging technologies, lawyers can put client data at risk and even inadvertently provide disadvantaged representation. This can result in serious ethical violations and all lawyers should review their current policies, procedures, and workflows to ensure they are meeting the duties of competence and confidentiality– especially when carrying out work functions virtually.

Two innovative technologies that lawyers should look out for are generative AI and the metaverse.



#1) Generative AI

Throughout the years the use cases for AI in legal practice have expanded. Predictive coding tools such as TAR are more often accepted for identifying key documents and themes early on in a matter and efficiently managing the assessment and review of data. These tools have matured since introduction, as now some can perform sentiment analysis and pattern processing. AI can assist with document review, settlement evaluation, litigation analysis, internal investigations, regulatory compliance, and strategy decisions. Legal teams have learned best practices for choosing secure predictive coding tools that can integrate into an organization's infrastructure or vetted through a provider partner. With generative AI entering the arena, it is crucial to understand the different risks that accompany using this technology and how to safely and integrate usage into legal practice.

Generative AI creates new content and chat answers based on prompts. A 2023 survey by LexisNexis demonstrated that 86 percent of lawyers were aware of generative AI and over half used or plan to use this tool for work purposes. Additionally, 84 percent of lawyers surveyed felt that generative AI would increase efficiency for their legal team.[23] There is no doubt that lawyers will use tools like ChatGPT in the future and ethics needs to factor into use case decisions.

Client confidentiality, security and privacy are some considerations that surface with tech usage. Putting confidential client information into a large language model like ChatGPT can open the door to waive privilege and can violate the attorney-client relationship. Any information included in a prompt will not be deleted and can be used for training purposes. Consider these factors before using for document review, contracting, language translation, and other use cases that involve confidential information. Client consent is also crucial when using any new technology and lawyers need to remain informed about the benefits and risks in order to provide competent representation.

The Florida Bar released an article in 2023 regarding considerations lawyers should make before using generative AI for practice tasks such as drafting briefs. The article noted that state opinions on e-filing, cloud computing, online research tools, metadata, and similar topics provide some useful instruction. One pointer that will ring true for lawyers practicing in any state pertained to the creation of facts for a legal document. AI services may create untrue facts or leave out citations. This can result in violation of a lawyer's ethical duty to not make false statements to the tribunal or third parties.[24] While this is not barring use of generative AI for brief or memo drafting, best practice dictates review of the facts to ensure they are accurate before filing with the court or transmitting to opposing counsel.

[23] 2023 Generative AI & The Legal Profession: Generative AI Captures Imagination of Lawyers, Law Students, Consumers, LexisNexis (2023)
[24] Grabb, Jonathan. Lawyers and AI: How Lawyers' Use of Artificial Intelligence Could Implicate the Rules of Professional Conduct, The Florida Bar (Mar. 13, 2023) https://www.floridabar.org/the-florida-bar-news/lawyers-and-ai-how-lawyers-use-of-artificial-intelligence-could-implicate-the-rules-of-professional-conduct/

#2) The Metaverse

The metaverse is on a journey to positioning itself as the next iteration of the Internet and in the process of evolving into a standalone digital economy. As of 2021, the global value of the metaverse was $58.5 billion and this figure is projected to climb to $1.5 trillion by 2030.[25] Currently there are several digital spaces that make up the metaverse. Progress has been made on the business front, but it is still in the very early stages. It will be years before it is used regularly across industries because trust takes time to build. In the legal space, several law firms have opened up but lawyers are not really advising clients yet. As with any new digital endeavor, anticipating potential use cases is crucial as they can materialize amongst competitors and clients. Future use cases include client consultations and meetings, internal collaboration, metaverse courtrooms, depositions, ALSP partnerships, data storage, and document review.

The legal community will be faced with new eDiscovery challenges and ethical obligations. Lawyers, legal service providers, and review teams should anticipate unique collection and review obstacles when data relevant to litigation or investigations resides in the metaverse. Challenges to prepare for include the need to use virtual reality headsets to view and analyze data, custodian identification, preservation mechanisms, and increased spoliation claims. Court decisions in this area will be instructive but it will be years before meaningful case law trends emerge.

The first obvious place where metaverse and ethics intersect is with competence. Best practices include metaverse and VR headset education and training, monitoring modern technologies used to power the metaverse, competitor analysis, and paying close attention to early case decisions. Also update pertinent trainings and policies regarding business use in the metaverse to align expectations across the legal teams and any outside partners.

How eDiscovery and information governance processes are carried out in the metaverse goes hand in hand with a lawyer's ethical obligations. Privileged information and data subject to regulatory compliance needs to be safeguarded. If venturing into the metaverse, legal organizations must have coherent policies about what us allowed to be stored in the metaverse and any unique instructions around collection or preservation. Failure to do so could increase spoliation or breach risk.

#3: Other Considerations

In addition to the more innovative areas discussed above, lawyers must not forget how simple communication channels used daily such as email and text can inadvertently open the door for unethical behavior.

For example, consider how communicating over modern technologies can create risk for violating Model Rule 4.2. This rule proscribes that a lawyer may not communicate about the subject of the representation with a represented person absent the consent of that person's lawyer unless the law or court order authorizes the communication. The ABA recently addressed the question of copying clients on group communication (email, texts, and other chat apps) with opposing counsel in a case. The issue of implied consent has been risen in a handful of states regarding when opposing counsel "replies all" because

[25] Metaverse Statistics 2023: All the Facts & Figures You Need to Know, ByBit Learn (Feb. 21, 2023) https://learn.bybit.com/metaverse/metaverse-statistics/

this would effectively be an instance of communicating with the other lawyer's client. The ABA took a different stance from several states on this topic, concluding the following:

> Absent special circumstances, lawyers who copy their clients on emails or other forms of electronic communication to counsel representing another person in the matter impliedly consent to a "reply all" response from the receiving counsel. Accordingly, the reply all communication would not violate Model Rule 4.2. Lawyers who would like to avoid consenting to such communication should forward the email or text to the client separately or inform the receiving counsel in advance that including the client on the electronic communication does not constitute consent to a reply all communication.[26]

This is something to keep in mind when communicating about a case, as it is often a routine practice to add all case members to an email or click "reply all" without considering who will receive subsequent discussions. To cover all bases, lawyers should communicate this with their clients before including them on any electronic communications involving other parties to a case.

SOCIAL MEDIA

When thinking about legal practice in the digital age, social media cannot be discounted as it is a massive part of everyday life for a large majority of society. Many lawyers and law firms use social media for business purposes to advertise services and employment opportunities, network with other legal professionals, share compelling legal news, communicate with clients, and attract new business. While this is not considered unethical, it should be completed with caution. The duty of competence is forefront here, as the social media universe keeps expanding.

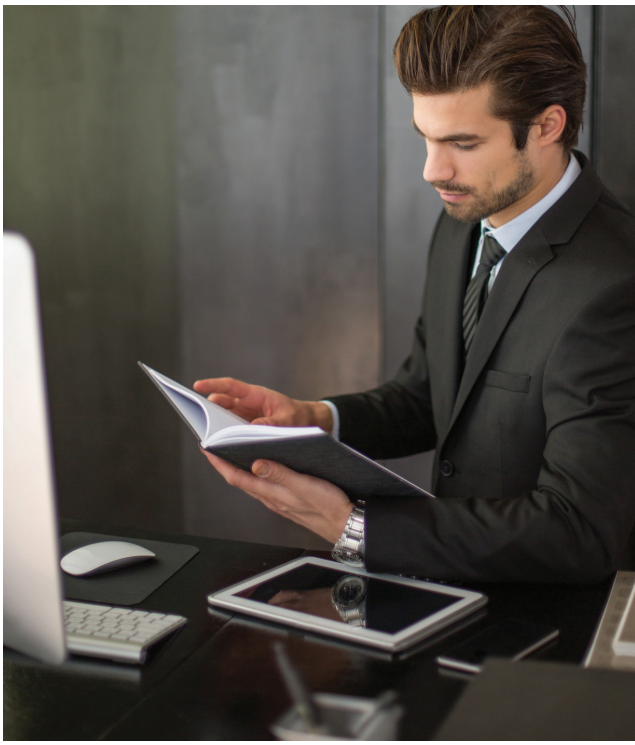
Jurisdictional Considerations

Social media posts have the potential to reach individuals in any area of the country. This may be problematic if a lawyer shares information outside of their practicing jurisdiction. Under American Bar Association ("ABA") Model Rule 5.5(b)(2), lawyers are prohibited from sharing information that would make the public believe that they are admitted to practice law in a jurisdiction where they are not licensed. Because of this, lawyers need to be mindful of what content they post and where it is shared. It is of the utmost importance to be transparent about licensing status and make a disclaimer stating that their content is not meant to form an attorney-client relationship or provide legal advice. This is especially ideal for lawyers who blog or post on an interactive platform.

[26] ABA Formal Opinion 503 (Nov. 2, 2022)

Litigation

During discovery, lawyers have ethical duties to preserve and disclose all information that is relevant to a lawsuit. Under ABA Model Rule 3.4(a), lawyers are prohibited from unlawfully obstructing another party's access to evidence or unlawfully altering, destroying, or concealing a document with potential evidentiary value. Additionally, ABA Model Rule 3.3 requires that lawyers act with candor towards the court. As such, during discovery lawyers must disclose all relevant documents not subject to privilege in their original format to avoid violating these rules. For example, Rule 3.4 applies to situations where a lawyer advises a client to delete or alter social media content that is relevant to a lawsuit. The general consensus is that lawyers can do this but must be careful when instructing clients about their past and future social media activity. Failure to preserve significant evidence can result in sanctions, license suspension, or an unfavorable litigation outcome. The Sedona Conference noted that "attorneys may advise clients regarding changing privacy settings or removing content, as long as they also satisfy preservation obligations and do not obstruct another party's access to evidence."[27]



Other pointers to note include the following:

- Merely taking a screenshot or printing out a social media webpage may not be an accurate reflection of the content because it may not include certain metadata, videos, or other embedded information. This could be a potential Rule 3.4 violation if the missing data holds evidentiary value. For social media data containing relevant evidence, lawyers must provide proper authentication and include all key data in the production. More technically involved collection methods include dynamic capture and content downloading from the provider.[28]
- Lawyers cannot friend request a party, witness, or juror on a social media website in order to gain access to their private information for purposes of collecting data to use in litigation. This could potentially violate several ABA rules, including Rule 4.2 (communication with represented person), Rule 4.3 (communication with unrepresented person), and Rule 8.4(c) (conduct involving dishonesty, fraud, deceit or misrepresentation).[29] It is also unethical to advise clients to friend request someone for this purpose. However, data that is publicly available for viewing is fair game.
- While the ABA has not issued an opinion on the ethical dilemmas accompanying social media that has ephemeral messaging capabilities, it has spoken out on the topic. In an article reviewing case law guidance on ephemeral messaging applications (EMAs), the ABA noted:

> While EMAs offer substantial benefits for their corporate and individual users, they present unique discovery challenges that are inconsistent with the duty to preserve evidence because of their ephemeral features. Often, EMAs are associated—rightly or wrongly—with the appearance of impropriety because relevant information disappears by design and may hide damaging evidence or wrongful conduct. Their use is likely to place many organizations at risk for failure to satisfy

[27] The Sedona Conference, Primer on Social Media, 20 SEDONA CONF. J. 88 (2019).
[28] The Sedona Conference, Primer on Social Media, 20 SEDONA CONF. J. (2019).
[29] The Sedona Conference, Primer on Social Media, 20 SEDONA CONF. J. 91-92 (2019).
[30] Hoover, Dalila. Ephemeral Messaging Apps Users: Use Caution During Anticipated or Ongoing Litigation, ABA (Feb. 28, 2020). https://www.americanbar.org/groups/litigation/committees/pretrial-practice-discovery/practice/2020/ephemeral-messaging-apps-users-use-caution-during-anticipated-or-ongoing-litigation/

> electronically stored information (ESI) preservation considering that a large portion of their workforce uses EMAs for business-related communications.

Attorneys have an ongoing ethical duty to educate themselves and their clients about the uses and implications of EMAs. Because they raise to the appearance of impropriety due to their ephemeral features by design, best practice commands the implementation of corporate policies specifically tailored to EMAs including retention and legal holds in place sooner than later. Reminding clients to refrain from using EMAs during anticipated or ongoing litigation seems like good advice after all.[30]

Lawyers should monitor whether the ABA or state bars update any guidance on the use of social media that incorporates EMAs or newer platforms such as TikTok in the near future.

CONCLUSION

Legal ethics in the digital age is an ever-evolving topic. The areas discussed above are only a snapshot of key duties lawyers must be mindful of when incorporating digital processes and emerging technologies into their practice. As always, lawyers must know the ABA's stance on hot topics as well as state bar or court opinions applicable to any state they hold a law license. Failure to uphold these standards can result in discipline, disbarment, court sanctions, reputational harm, and client distrust. It is also crucial that other members of the internal legal team and external partners conduct business ethically. This makes regular communication and education on the topics discussed in this white paper an integral component of practicing law today.