Ethics 3.0—Attorney Responsibility in the Age of Generative AI

Jon M. Goran

Originally published in The Business Lawyer
Winter 2023/2024 | Volume 79, Issue 1
Survey of the Law of Cyberspace

Ethics 3.0—Attorney Responsibility in the Age of Generative AI

*By Jon M. Garon**

"[A] lawyer without books would be like a workman without tools."[1]
– Thomas Jefferson

Introduction

The practice of law has gone digital. Technology has transformed the mechanics of practicing law through the remote access to one's office; reliance on smartphones to share data, email, and use social media to communicate with clients; machine learning to anticipate judicial decisions; cloud-based outsourcing to store records; artificial intelligence (AI) to conduct valuations; and legal practices existing only in the metaverse. Law is by no means alone, and to some extent, the profession saw the changes coming.

In 2009, the American Bar Association created the Commission on Ethics 20/20 (Commission) to "perform a thorough review of the ABA Model Rules of Professional Conduct [(MRPC or Model Rules)] and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments."[2] The Commission held hearings and developed draft statements regarding a number of topics, including the effect of technology on a lawyer's duty of confidentiality and client development.[3]

In 2012, the ABA House of Delegates adopted the Commission's recommendations. In the decade that followed, the introduction of the metaverse, cryptocurrencies, NFTs, and blockchain technologies, as well as challenges associated

* Professor of Law and Director of the Goodwin Program for Society, Technology, and the Law, NSU Shepard Broad College of Law.

1. Letter from Thomas Jefferson to Thomas Turpin (Feb. 5, 1769), https://founders.archives.gov/documents/Jefferson/01-01-02-0016.

2. *ABA Commission on Ethics 20/20: About Us*, Am. B. Association, https://www.americanbar.org/groups/professional_responsibility/committees_commissions/aba-commission-on–ethics-20-20/about_us/ (last visited Dec. 1, 2023); *see* ABA Commission on Ethics 20/20, Report to the House of Delegates on Outsourcing (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf.

3. *ABA Commission on Ethics 20/20*, Am. B. Association, https://www.americanbar.org/groups/professional_responsibility/committees_commissions/aba-commission-on–ethics-20-20/ (last visited Dec. 1, 2023).

with a worldwide pandemic, forced an ever-greater need for lawyers to address technological issues in their practice.

Through the Commission, the ABA embraced the importance of technological change as fundamental to the practice of law. The ABA adopted an amendment to MRPC Rule 1.1,[4] Comment [8] as follows:

> 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.[5]

In making this duty explicit, the ABA heightened the level of responsibility that law firms must address regarding the technological mediation of their services. Through the expanded understanding of competence, the expectation now includes an attorney's duty to understand the benefits and risks of technology available for the practice of law.

This article focuses on the obligations of client confidentiality, the duty to understand cybersecurity, the need to proceed with caution when exploiting the new technologies of generative AI and the metaverse, and the need to communicate in a permissible manner. These are all key obligations under the Model Rules related to the use of technology.

Still, the Model Rules are not necessarily binding law and the comments thereon are not the basis for attorney discipline.[6] Although many jurisdictions have adopted them in whole,[7] others have adopted (or updated) them on a rule-by-rule basis.[8] The ABA Center for Professional Responsibility reported that, as of April 4, 2023, "[t]hirty-nine (39) jurisdictions ha[d] adopted a statement on tech competence."[9] Other jurisdictions may have language that addresses these concerns more obliquely.[10] Nonetheless, the Model Rules provide a normative guideline that goes beyond the technical requirements for minimum competency and may provide standards for professional malpractice liability or other culpability.[11] As a result, the Model Rules provide a common baseline for

4. Model Rules Pro'l Conduct r. 1.1 (Am. B. Ass'n 2023) ("A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.").

5. ABA Comm. on Ethics & Prof'l Resp., Formal Op. 477R (2017).

6. Model Rules Prof'l Conduct pmbl. [14] (Am. B. Ass'n 2023) ("Comments do not add obligations to the Rules but provide guidance for practicing in compliance with the Rules."); *see* Daniel J. Siegel, *Revise the Rules of Professional Conduct for Technology*, Law Prac., Nov./Dec. 2021, at 24, 25, https://www.americanbar.org/groups/law_practice/publications/law_practice_magazine/2021/nd21/hb/?login (emphasizing same).

7. *See* Cheryl B. Preston, *Lawyers' Abuse of Technology*, 103 Cornell L. Rev. 879, 884–86 (2018).

8. *See*, *e.g.*, *In re* Formal Advisory Op. No. 20-1, 872 S.E.2d 745, 747 n.6 (Ga. 2022) (per curiam) ("Georgia . . . has not adopted the ABA Rules or the comments to the ABA Rules wholesale.").

9. *Jurisdictional Rules Comparison Charts*, Am. B. Association, https://www.americanbar.org/groups/professional_responsibility/policy/rule_charts (last visited Dec. 1, 2023).

10. *See id.*

11. *See* Heidi Li Feldman, *Beyond the* Model Rules*: The Place of Examples in Legal Ethics*, 12 Geo. J. Legal Ethics 409, 432 (1999); George L. Hampton IV, *Toward an Expanded Use of the Model Rules of Professional Conduct*, 4 Geo. J. Legal Ethics 655, 656–58 (1991); Deborah L. Rhode, *Moral Character as a Professional Credential*, 94 Yale L.J. 491, 510 & n.85 (1985). *But see* Model Rules Prof'l Conduct pmbl. [20] (Am. B. Ass'n 2023) ("Violation of a Rule should not itself give rise to a cause of action

understanding the technological competence required of practicing attorneys.[12]

To fully understand the scope of a lawyer's duty regarding technology, the practitioner must go beyond the Model Rules. Examples abound. Under the Health Insurance Portability and Accountability Act (HIPAA),[13] data privacy and security rules occasionally apply to legal services, subjecting law firms to those strict privacy and security obligations.[14] The Export Administration Act and the International Traffic in Arms Regulations may render illegal certain digital distributions.[15] Similarly, while most law firms do not meet the threshold requirements of earning more than $25 million in annual revenue and holding the personal information for at least one hundred thousand California consumers or households, those firms that meet this standard must comply with the California Consumer Privacy Act.[16] Other states are enacting similar laws, each with its own threshold requirements, obligations, and operations.[17] Lawyers must also adhere to the truth-in-advertising obligations established by the Federal Trade Commission (FTC).[18] A lawyer's duty to remain competent and diligent in light of technological change begins with the Model Rules but other areas of substantive law may extend that duty.

I. The Expanded Obligations of Client Confidentiality

In 2012, the ABA amended the Model Rules by adopting Rule 1.6(c), which requires that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to

against a lawyer nor should it create any presumption in such a case that a legal duty has been breached.").

12. *See generally* ABA Comm. on Ethics & Prof'l Resp., Formal Op. 483 (2018) (Lawyers' Obligations After an Electronic Data Breach or Cyberattack); ABA Comm. on Ethics & Prof'l Resp., Formal Op. 477R (2017) (Securing Communication of Protected Client Information).

13. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

14. *See* 45 C.F.R. §§ 164.302–164.318 (2022) (addressing security standards for the protection of electronic health information); *id.* § 164.501 (defining "health care operations" to include "conducting or arranging for . . . legal services"); *id.* § 164.502(b) (regulating disclosure of protected health information by any covered entity or business associate); Aaron P. Sohaski & Jordan B. Segal, *Litigation in a HITECH World: Cybersecurity and the Importance of Maintaining HIPAA Security Compliance*, 95 Mich. B.J., Nov. 2016, at 52, 52–54 (discussing HIPAA and the risk of inadvertent disclosure).

15. Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 Wm. Mitchell L. Rev. 111, 138 (2011) (discussing the duty implicit in MRPC r. 1.1 prior to the proposed revision); *see* 50 U.S.C. §§ 2401–2411 (2018); 22 C.F.R. §§ 120.1–130.17 (2022).

16. Cal. Civ. Code § 1798.140(d)(1) (West, Westlaw through ch. 1 of the 2023-24 1st Ex. Sess.) (defining regulated "business"); *see* Daniel A. Cotter, *The Increasingly Complex Landscape for Attorneys and Privacy*, 35 DCBA Brief 26, 31 (2022) (discussing obligations under the California Privacy Rights Act).

17. *See* Sanford P. Shatz & Paul J. Lysobey, *Privacy Laws Continue Their Spread Across the Country*, 78 Bus. Law. 551, 551 (2023) ("Since the beginning of 2022, the privacy landscape in the United States has continued to change and develop. Utah and Connecticut have enacted comprehensive consumer privacy legislation. . . . Virginia and Colorado are also preparing for their privacy laws previously enacted in 2021 to become effective . . . .").

18. *See* 16 C.F.R. § 255.1 (2022).

the representation of a client."[19] Subsection (c) addresses confidentiality concerns associated with electronic information and extends the affirmative duty to data privacy, security, and reliability.

The ABA adopted a "reasonable efforts" standard to apply to the lawyer's duty of confidentiality.[20] There are a number of common technologies that a law firm should address when determining its baseline technology risk. The law firm can then adjust those standards to provide heightened protection when the nature of the information warrants additional protection.

In the context of financial institutions, financial services regulators have created the FTC Safeguards Rule under the Gramm-Leach-Bliley Act that outlines the steps needed to protect customer information.[21] The Safeguards Rule as well as the HIPAA Security Rule use the same three-pronged model for data protection, requiring: "administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[22]

"When thinking about protecting personal information, most people begin with the technical safeguards. These are the basic steps that can reduce the risks from most identity theft and other forms of fraud."[23] Technical safeguards include firewalls; active software updating and patching to ensure that no outdated software is in operation; device encryption; strong unique passwords for each account; two-step verification of identity; internet encryption using HTTPS; and similar techniques.[24]

Law firms have a duty to manage themselves and their employees and agents to ensure that everyone with access to confidential information remains trustworthy and diligent. Law firms, for example, might consider disabling the "reply all" button to ensure that each recipient of an email is an intended recipient.[25] An attorney also can trigger an inadvertent disclosure from a lack of understanding about the tools being used. Attorneys who are unaware of the metadata in word processing documents may inadvertently leave confidential client information in the metadata associated with documents shared publicly.[26] Attorneys may not be aware of the geo-location information they provide to Google Maps and other apps when traveling. This data could be combined with other information to disclose the target of a corporate acquisition or of a future lawsuit. Law firms should

19. Model Rules Prof'l Conduct r. 1.6(c) (Am. B. Ass'n 2023).

20. *See* ABA Commission on Ethics 20/20, Report to the House of Delegates on Technology & Confidentiality 4 (2012) ("Rule 1.6(c) is intended to make clear that lawyers have an ethical obligation to make reasonable efforts to prevent these types of disclosures, such as by using reasonably available administrative, technical, and physical safeguards.").

21. 16 C.F.R. § 314.1 (2022).

22. *See id.* §§ 314.1–314.6 (implementing 15 U.S.C. §§ 6801(b), 6805(b)(2)).

23. Jon M. Garon, Parenting for the Digital Generation 211 (2022).

24. *Id.* at 211–13.

25. Disabling the "reply all" function should certainly be done for anyone who has confused the "reply" and "reply all" functions more than once.

26. *See* Model Rules Prof'l Conduct r. 4.4(b) (Am. B. Association 2023) ("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."); *id.* r. 4.4(b) cmt [2] (addressing metadata).

employ technical measures to reduce the likelihood of inadvertent disclosure of data by attorneys and staff.

"Physical safeguards are the physical measures, policies, and procedures to protect . . . systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusions."[27] Physical security focuses on buildings, offices, computer network server rooms, mechanical locks, and other physical steps that can be taken to protect files, computers, and storage devices.[28] Physical safeguards also include the steps taken to mitigate against natural disasters and other catastrophic events, such as off-site storage of backup files and the ability to operate remotely in the event that the firm's offices are closed.

Administrative safeguards can be understood as the "administrative actions, policies, and procedures [that] manage the selection, development, implementation, and maintenance of security measures."[29] "[T]he purpose of creating cybersecurity regulations with administrative safeguard policies [is] to ensure that senior management [is] paying attention to privacy and security."[30]

A firm's plan should identify the individuals responsible for cybersecurity, privacy, and confidentiality by job title, so the plan remains valid notwithstanding employee turnover. Senior firm leadership must be directly responsible for implementing the plan. The specifications of the technical and physical safeguards listed above should be detailed in the plan.

A meaningful plan includes training of all individuals and entities that have any access to confidential information, from senior partners to student interns. Training should be tailored to the role of the individual. Attorneys who have supervisory responsibility need training to ensure that those being supervised also meet their obligations.

Another important aspect of the program is data minimization or access control.[31] If (or when) a cybersecurity breach occurs, the damage can be largely mitigated if each person's access to confidential information is limited to that information the person needs to provide legal services. If, instead, any attorney can troll through all the legal files of the law firm without restriction, then a breach of any attorney's account lays open every client file for theft and disclosure.

The plan should require end-to-end encryption of all confidential records, limit use of unencrypted email,[32] enforce stronger password policies and establish a set of standards and contractual requirements for all vendors of the law

27. 45 C.F.R. § 164.304 (2022) (addressing electronic protected health information).

28. For example, whether in paper or electronic form, confidential information should not be easy to purloin from offices unlocked every evening for routine cleaning. *See* Garon, *supra* note 23, at 210.

29. 45 C.F.R. § 164.304 (2022) (addressing electronic protected health information).

30. Garon, *supra* note 23, at 215.

31. *See* Teresa Matich, *2023 Law Firm Data Security Guide: How to Keep Your Law Firm Secure*, Clio (2023), https://www.clio.com/blog/data-security-law-firms/.

32. *See*, *e.g.*, Tex. Prof'l Ethics Comm., Op. 648 (2015) (identifying six areas where encrypted email should be considered). As email encryption becomes increasingly available, it becomes less reasonable to send unencrypted emails when the risk of interception is significant, as suggested by these six categories. *See* ABA Comm. on Ethics & Prof'l Resp., Formal Op. 477R (2017).

firm.[33] As noted by the FTC, an appropriate plan includes strategies to mitigate cyber risks, as well as risks associated with natural disasters and other catastrophic events.[34] Every plan should include provisions for off-site storage of backup data along with testing of the restoration of the backup data.

Finally, the plan should include the operational response for a data breach, emergency, or natural disaster. The plan should identify who is to be contacted; the steps to address data breach notification obligations of both clients and of individuals protected by various data breach notification regimes; any law enforcement agencies to be engaged; any vendors to be involved; and anything else that reflects a decision-point that could slow the response.

II. The Intersection Between Privacy and Generative AI

Beginning in 2022, one decade after the Commission made its recommendations, the stock market became giddy with the cultural phenomenon unleashed by the public launch of OpenAI's ChatGPT.[35] Generative AI systems can produce data that mimics the content of human creativity.[36] These neural networks can generate content in the form of text, voice, pictures, videos, software, physical and molecular designs, audiovisual works combining these features, and more.[37]

Generative AI services are far more than search engines because they do not merely find published content: They evaluate, combine, and synthesize the known information to provide an answer of their own. Trained on the data with which they are provided, they develop their own responses to the questions presented. Certain generative AI services can be integrated with an "extractive" or "abstractive" process that produces a shortened or summarized version of texts or documents.[38] "Extractive AI is all about taking existing information and using it to answer specific questions or generate new content, while generative AI is all about creating new information from scratch."[39]

33. *See* Matich, *supra* note 31.

34. *See* 16 C.F.R. § 314.4(b) (2022) (referencing the identification of "reasonably foreseeable internal and external risks").

35. *See* Bern Elliott, *Why Is ChatGPT Making Waves in the AI Market?*, Gartner (Dec. 8, 2022), https://www.gartner.com/en/newsroom/press-releases/2022-12-08-why-is-chatgpt-making-waves-in-the-ai-market.

36. *See* Rob Toews, *The Next Generation of Large Language Models*, Forbes (Feb. 7, 2023, 11:00 AM), https://www.forbes.com/sites/robtoews/2023/02/07/the-next-generation-of-large-language-models/?sh=a6a71bd18dbc.

37. *See id.*; Atin Gupta & Geoffrey G. Parker, *How Will Generative AI Disrupt Video Platforms?*, Harv. Bus. Rev. (Mar. 13, 2023), https://hbr.org/2023/03/how-will-generative-ai-disrupt-video-platforms.

38. Stefano Ferilli, Andrea Pazienza, Sergio Angelastro & Allesandro Suglia, *A Similarity-Based Abstract Argumentation Approach to Extractive Text Summarization*, *in* AI*IA Advances in Artificial Intelligence 87, 87 (Floriana Esposito et al. eds., 2017) (collecting articles presented at the XVIth International Conference of the Italian Association for Artificial Intelligence).

39. *Extractive AI vs Generative AI*, Nowigence, https://nowigence.com/blog/extractive-ai-vs-generative-ai/ ("It's like the difference between copy-pasting a Wikipedia article and writing a completely original one.") (last visited Dec. 1, 2023).

Because generative AI is trained to see patterns and provide pleasing patterns to the user, it is excellent at providing text with an air of authority. But unless the system also uses some form of extractive AI to validate its response against known sources and limit its identification of facts to those found in external, verified information sets, generative AI is simply non-factual. Although the AI industry has labeled the failure to be accurate as "hallucinations," this term hides the structure of generative AI.[40] Generative AI output is only accurate to the extent that the pleasing patterns of information normatively correlate with the user's general understanding of the truth.

A district court reminded the profession of this simple truth in *Mata v. Avianca*,[41] where a law firm used generative AI to write portions of a brief.

> Peter LoDuca, Steven A. Schwartz and the law firm of Levidow, Levidow & Oberman P.C. (the 'Levidow Firm') (collectively, 'Respondents') abandoned their responsibilities when they submitted non-existent judicial opinions with fake quotes and citations created by the artificial intelligence tool ChatGPT, then continued to stand by the fake opinions after judicial orders called their existence into question.[42]

The Respondents had little experience with ChatGPT. They did not conduct ordinary legal research in writing their brief. Schwartz testified that he was "operating under the false . . . disbelief that [ChatGPT] could produce completely fabricated cases."[43] He further claimed, "I still could not fathom that ChatGPT could produce multiple fictitious cases, all of which had various indicia of reliability, such as case captions, the names of the judges from the correct locations, and detailed fact patterns and legal analysis that sounded authentic."[44] There is little evidence that Schwartz actually checked the quality of the source material, but he provided an explanation as to why he used the AI-generated materials: "My reaction was, ChatGPT is finding that case somewhere. Maybe it's unpublished. Maybe it was appealed. Maybe access is difficult to get. I just never thought it could be made up."[45] Even if true, none of those justifications seems to permit the use of the cases. The apparent reality was fiction; ChatGPT generated plausible but non-existent case materials.

Mata feels apocryphal, a campfire story for legal writing faculty to scare first-year law students to properly check their sources and Shepardize their cases before submitting their work to any professor or court. But the concern is real and growing.

Judge Brantley Starr of the Northern District of Texas responded to these concerns by issuing a standing order restricting the use of generative AI:

40. *See* Towes, *supra* note 36.
41. Opinion Order and Sanctions, Mata v. Avianca, Inc., No. 22-cv-1461 (S.D.N.Y. June 22, 2022).
42. *Id.* at 1.
43. *Id.* at 6.
44. *Id.* at 20.
45. *Id.* at 6.

> All attorneys and pro se litigants appearing before the Court must, together with their notice of appearance, file on the docket a certificate attesting either that no portion of any filing will be drafted by generative artificial intelligence (such as ChatGPT, Harvey.AI, or Google Bard) or that any language drafted by generative artificial intelligence will be checked for accuracy, using print reporters or traditional legal databases, by a human being. These platforms are incredibly powerful and have many uses in the law: form divorces, discovery requests, suggested errors in documents, anticipated questions at oral argument. But legal briefing is not one of them. Here's why. These platforms in their current states are prone to hallucinations and bias.[46]

Judge Starr's order provides flexibility to allow generative AI to be used as part of a human-reviewed research process. Judge Starr emphasizes the importance of addressing bias in one's writing and points to obligations to adhere to candor to the tribunal, duties to uphold the Constitution and law, and more general ethics obligations.[47]

While data providers are generally enthusiastic about the potential for generative AI services, those in the legal sector understand that extractive AI is the core of legal research. Within the legal industry, providers understand they must combine extractive AI tools as "guardrails" to limit the generative AI output. Each of the two largest legal research services, RELX's Lexis and Thomson Reuters' Westlaw, entered the AI arms race, as have their parent companies more generally.[48] The race between these two legal and business giants heated up when Thomson Reuters spent $650 million to acquire Casetext, which has been innovating through its early access to ChatGPT-4.[49]

The widespread proliferation of generative AI content and platforms comes only a year after the metaverse, another Silicon Valley darling, took the industry by storm. Although the metaverse is often described as complex, the idea is actually quite simple: It is a virtual Mall of America, a state fair, or a Renaissance festival. Like each of these gathering spaces, Roblox and the other metaverse platforms offer games, amusements, and social events, while building a virtual economy. People participate to interact with others and to share their common experiences.

46. Mandatory Certification Regarding Generative Artificial Intelligence (N.D. Tex. May 30, 2023) (Starr, J.), https://www.txnd.uscourts.gov/judge/judge-brantley-starr.

47. *See id.* ("[Generative AI] systems hold no allegiance to any client, the rule of law, or the laws and Constitution of the United States (or, as addressed above, the truth). Unbound by any sense of duty, honor, or justice, such programs act according to computer code rather than conviction, based on programming rather than principle.").

48. *See* Jake Nelson, *Combining Extractive and Generative AI for New Possibilities*, LexisNexis Legal Insights (June 6, 2023), https://www.lexisnexis.com/community/insights/legal/b/thought-leadership/posts/combining-extractive-and-generative-ai-for-new-possibilities; *Not All Legal AI Is Created Equal*, Thomson Reuters, https://legal.thomsonreuters.com/en/insights/white-papers/5-things-to-consider-when-evaluating-legal-ai-solutions (last visited Dec. 1, 2023).

49. *See* Kyle Wiggers, *Thomson Reuters Buys Casetext, an AI Legal Tech Startup, for $650M in Cash*, TechCrunch (June 26, 2023, 10:09 PM), https://techcrunch.com/2023/06/26/thomson-reuters-buys-casetext-an-ai-legal-tech-startup-for-650m-in-cash/; *Thomson Reuters to Acquire Legal AI Firm Casetext for $650 Million*, Reuters (June 27, 2023, 12:59 PM), https://www.reuters.com/markets/deals/thomson-reuters-acquire-legal-tech-provider-casetext-650-mln-2023-06-27/.

Attorneys already practice via virtual offices that exist solely in metaverse environments. To remain compliant with the applicable ethics rules and privacy obligations, such attorneys should use end-to-end encryption of their communications. Those offices should have technical measures to restrict access to their confidential client information both from third-party hackers but also from the platform operator, plug-in vendors, and related service providers. The metaverse does not have conference rooms; it has virtualized "Zoom-like" chat rooms. As such, the attorneys must assure that those online environments are not subject to eavesdropping, whether a live conversation or a digitally preserved one.

In addition to technical measures, attorneys should follow the administrative and physical measures of the Safeguards Rule to ensure confidentiality, data integrity, and protection from eavesdropping. Physical security for the metaverse means that the attorney is paying attention to the environment in which the legal services take place and that all vendors meet their privacy and security requirements. In other words, a crowded coffee shop creates only an illusion of privacy. If a laptop's screen is observed by another person, or the customer at the next booth listens to a conversation, then privilege does not exist, and security has not been maintained.

As to the administrative requirements, the Safeguards Rule focuses on contractual obligations to ensure the necessary privacy and security to maintain confidentiality and privilege. The metaverse vendor agreements must be sufficiently robust so that the vendor stands behind the security it is providing. The agreement must also specify that the data gleaned from the parties' interactions on the generative AI platform or metaverse environment is not collected and exploited in a manner that could interfere with the firm's duty of confidentiality to its clients. Names, unique identifiers, geolocation data, and similar information could reveal confidential information to third parties in violation of the firm's ethical or legal obligations.

Finally, because both AI services and metaverse services are provided through third-party vendors, these technologies highlight the addition of Comment [3] to MPRC 5.3, which requires that, "[w]hen using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations."[50] To meet the reasonableness test, an attorney should make confidentiality requirements, data-retention obligations, and data-breach-notification obligations express contractual terms. The agreement should also include the ability to assess or audit compliance with those contractual obligations. As an ever-increasing number of legal services are conducted through third-party technologies, lawyers should contractually impose their confidentiality and privacy obligations on to their vendors.

50. Model Rules Prof'l Conduct r. 5.3 cmt. [3] (Am. B. Ass'n 2023).

III. The Ethical Lawyer's Digital Presence

The ubiquity of the Internet has required that lawyers engage their clients where the clients expect to get services, namely in the online environment.[51] When considering the ethical obligations regarding online legal services, the starting point has not changed. MRPC Rule 7.1 requires truthfulness and accuracy about the lawyer and the lawyer's services.[52] This requirement extends to all communication and necessarily includes electronic and online communications.[53] Comment [3] was modified slightly so that the duty is owed to the public generally, rather than to just prospective clients.[54]

This affirmative duty to the public has certain unique consequences in the social media and public space. For example, a lawyer should refrain from overstating the nature of the lawyer's practice or presence. Online tools can easily create an illusion of a national or global presence when, in reality, a firm has only a local or regional presence. Content on a lawyer's website or blog could lead to confusion if the disclosure misstated or falsely implied that non-attorney content had been prepared by an attorney within the firm. Simple attribution would generally resolve this issue.

The Commission codified an earlier ethics opinion regarding the conditions upon which a person can become a prospective client.[55] The ABA amended the text of MRPC Rule 1.18 to define a "prospective client" as "a person who consults with a lawyer about the possibility of forming a client-lawyer relationship," rather than merely someone who "discusses" the possibility.[56] The change clarifies that a "prospective client" is a person who has a "reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship."[57]

The District of Columbia Bar Association issued a pair of ethics opinions involving social media that aid in understanding the parameters of a lawyer's obligations regarding advertising and client communications. Opinion 370 addresses "Social Media I: Marketing and Personal Use,"[58] while Opinion 371 covers "Social Media II: Use of Social Media in Providing Legal Services."[59] The DC Bar's Committee on Legal Ethics (Committee) began Opinion 370 with a note of caution: "Increas-

51. Stephanie L. Kimbro, Virtual Law Practice: How to Deliver Legal Services Online 1 (2010).

52. Model Rules Prof'l Conduct r. 7.1 (Am. B. Ass'n 2023) ("A lawyer shall not make a false or misleading communication about the lawyer or the lawyer's services. A communication is false or misleading if it contains a material misrepresentation of fact or law, or omits a fact necessary to make the statement considered as a whole not materially misleading.").

53. ABA Commission on Ethics 20/20, Report to the House of Delegates on Technology & Client Development 1 (2012) ("[T]he Commission concluded that Model Rule 7.1's prohibition against false and misleading communications is readily applicable to online advertising and other forms of electronic communications that are used to attract new clients.").

54. *Id.* at 3 ("The inclusion of an appropriate disclaimer or qualifying language may preclude a finding that a statement is likely to create unjustified expectations or otherwise mislead the public a prospective client.").

55. *See* ABA Comm. on Ethics & Prof'l Resp., Formal Op. 10-457 (2010).

56. ABA Commission on Ethics 20/20, *supra* note 53, at 1.

57. Model Rules Prof'l Conduct r. 1.18 cmt. [3] (Am. Bar Ass'n 2023).

58. D.C. Bar Ass'n Comm. on Legal Ethics, Op. 370 (2016).

59. D.C. Bar Ass'n Comm. on Legal Ethics, Op. 371 (2016).

ingly, attorneys are using social media for business and personal reasons. . . . The Committee notes that any social media presence, even a personal page, could be considered advertising or marketing, and lawyers are cautioned to consider the Rules applicable to attorney advertising . . . ."[60]

The Committee noted that ethical rules and interpretation of those rules vary from state to state; the tools of social media do not respect the geographic boundaries that are required of law licensure; there are many ways to use social media that may exceed personal or social communications that are not being addressed by the Committee's opinions.[61]

Summarizing the concerns regarding personal use of social media, the Committee highlighted areas in which an attorney could inadvertently overstep the activities permitted under the rules:

- "Communications via social media are inherently less formal than more traditional or established forms of communication."
- "Content contained on a lawyer's social media pages must be truthful and not misleading."
- "[I]f an attorney connects with, or otherwise communicates with, clients on social networking sites, then the attorney must continue to adhere to the Rules and maintain an appropriate relationship with clients."
- "[S]tatements on social media could expose a lawyer to civil liability for defamation, libel or other torts."
- "[The Committee recommended that] all law firms have a policy in place regarding employees' use of social networks [as lawyers in law firms] have an ethical duty to supervise subordinate lawyers and non-lawyer staff to ensure that their conduct complies with the applicable Rules, including the duty of confidentiality."[62]

To address the inadvertent formation of client relationships, the Committee suggested disclaimers. "Disclaimers are advisable on social media sites, especially if the lawyer is posting legal content or if the lawyer may be engaged in sending or receiving messages from 'friends,' . . . when those messages relate, or may relate, to legal issues."[63]

In Opinion 371, the Committee emphasized that competent representation may require the attorney to review the content of the client's social media activities in both a transactional and litigation setting. "In litigation, client social media postings could be inconsistent with claims, defenses, pleadings, filings,

60. D.C. Bar Ass'n Comm. on Legal Ethics, Op. 370 (2016).
61. *Id.*
62. *Id.*
63. *Id.* (citing D.C. Bar Ass'n Comm. on Legal Ethics, Op. 302 (2000) (addressing the solicitation of clients through the internet)).

or litigation/regulatory positions."[64] The opinion highlighted the obligation "to ensure that claims and positions are meritorious under Rule 3.1, which requires a non-frivolous basis in law and fact, and that misrepresentations are not made to courts or agencies in violation of Rules 3.3 and 8.4."[65] The opinion emphasized that, in the transactional context, "review of client social media for their consistency with representations, warranties, covenants, conditions, restrictions, and other terms or proposed terms of agreements could be important because inconsistency could create rights or remedies for counterparties."[66]

At the same time, lawyers must not entirely shun social media. On the contrary, lawyers conducting appropriate investigations have an obligation to review the social media postings of adverse parties as part of their factual review of ongoing matters.[67] In addition, to the extent that an attorney's client is itself subject to regulatory oversight of its online and social media activities, the attorney must be competent and engaged to ensure that these obligations are met.[68] In contrast, it is not acceptable to "friend," or connect online with another person involved in litigation, particularly an unrepresented opposing party or juror.[69]

Conclusion

The evolution of technology has affected every facet of legal practice. Lawyers have recognized this, and the profession has worked diligently to keep itself apprised of the changes to law and technology within each area of practice. A decade after the Commission's recommendations, however, the modifications to the MRPC highlight the changes affecting not just clients but lawyers themselves. Technology should serve the client and the relationship. The technological lawyer remains, first and foremost, a client-centered lawyer. This is the heart of ethical lawyering and the fundamental principle underlying the rules of technological competence.

64. D.C. Bar Ass'n Comm. on Legal Ethics, Op. 371 (2016).
65. *Id.* (footnotes omitted).
66. *Id.*
67. *Id.*
68. *Id.*
69. *See id.*