LEGAL ETHICS & MALPRACTICE REPORTER

TABLE OF CONTENTS

FEATURED TOPIC
LEGAL ETHICS AND ARTIFICIAL INTELLIGENCE

One of the areas in which technology is making increasing inroads into legal practice is in the use of artificial intelligence ("AI") algorithms. AI has been touted as providing a faster, cheaper way to accomplish certain legal tasks. But, as lawyers and law firms adopt AI into their daily practice to do tasks formerly done by human lawyers, they need to be aware of how the *Rules of Professional Conduct* may impact such use.

AI has been defined in a number of different ways. IBM, a pioneer in AI research provides this definition:

> In computer science, the term artificial intelligence (AI) refers to any human-like intelligence exhibited by a computer, robot, or other machine. In popular usage, artificial intelligence refers to the ability of a computer or machine to mimic the capabilities of the human mind—learning from examples and experience, recognizing objects, understanding and responding to language, making decisions, solving problems—and combining these and other capabilities to perform functions a human might perform, such as greeting a hotel guest or driving a car.[1]

Katherine Nunez, in her 2017 comment in the *Tulane Journal of Technology and Intellectual Property* explained further:

> AI is a method of technology that teaches a machine how to do a task originally thought to be carried out by humans. There are four main methods from which machines are being taught: (1) machine learning; (2) visual recognition; (3) speech recognition; and (4) natural language processing. Machine learning is the use of "algorithms that iteratively learn from data," allowing machines to learn through experience, such as their interactions with humans, rather than being programmed with the specific knowledge. Visual recognition is "the ability for machines to identify images" (e.g., Facebook's photo recognition tool). Speech recognition is a machine's ability to understand how humans communicate verbally then translate the human vocal tones into words (e.g., Apple's Dictation feature). Natural language refers to a human language. Thus, natural language processing (NLP) is the ability of machines to understand the relation between words

---

[1] Online at https://www.ibm.com/cloud/learn/what-is-artificial-intelligence.

and decipher the intent and meaning behind their usage by humans.[2]

Today, AI algorithms are used in a number of common legal practice areas such as electronic discovery, document assembly, and legal research. AI programs are already available that are specifically tailored to actually produce complete documents for many areas of legal practice. Rafael Baca reported the extent of this use in an article on the ABA's online "Law Practice Today" on 14 August 2020:

> At this time, AI algorithms allow commercial legal software to automatically generate legal documents from briefs to patent search results and judicial opinions. The economic and time-saving temptations of simply signing-off on AI-generated work products are great to legal practitioners, especially in private practice.[3]

Given the increasing use of AI, it is important for lawyers to understand how a number of the *Rules of Professional Responsibility* may apply to this.

Rule 1.1 as adopted in both Kansas and Missouri requires that lawyers be competent. Comment 8 to 1.1 states that a lawyer:

> 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.

(emphasis added). A reasonable interpretation of Comment 8 when applied to the use of AI is that lawyers must, at a minimum, understand the risks associated with its use. It does not required that lawyers understand the complex details of AI algorithms. But it does require that they understand enough about how such algorithms perform in practice to enable them to estimate where risks to clients, such as breaches of client confidentiality, may occur.

Rule 1.6 requires that a lawyer maintain client confidences unless a specific exception is met. AI algorithms often require substantial amounts of client data to function properly. This may put such data at risk of inadvertent disclosure. In their article "The Ethics of Artificial Intelligence," David L. Gordon and Rebecca L. Ambrose comment:

---

[2] Katherine Nunez, "Artificial Intelligence and Legal Ethics: Whether AI Lawyers Can Make Ethical Decisions," *Tulane Journal of Technology and Intellectual Property*, v. (2017), v. 20, 189- 203 at 191-192.

[3] Online at https://www.lawpracticetoday.org/article/model-ethics-rules-as-applied-to-artificial-intelligence/.

Many of the AI programs that lawyers are using to provide their clients with legal services are supplied by third-party vendors who are not lawyers or otherwise associated with a law firm. As a result, lawyers must take steps, as required by Model Rule 1.6, to ensure that their clients' information is appropriately safeguarded. To ensure the confidentiality of the information, a lawyer contemplating the use of AI should consider discussing confidentiality concerns with the third-party provider and should inquire about, among other things, what type of information is going to be provided, how that information will be stored, what security measures are in place with respect to the storage of the information, and who is going to have access to the information. Only after concluding that the client confidential information that they provide will be reasonably safeguarded should a lawyer proceed with using AI in connection with the representation of a client.[4]

Rule 2.1 requires that a lawyer "shall exercise independent professional judgment" in representing a client. Advanced AI algorithms use machine learning so that their ability to make judgments will increase in sophistication and accuracy as they absorb more data and learn from it. This process, however, in effect permits the AI to make judgments in the place of a human lawyer. One must ask whether a lawyer who permits an AI to make judgments (e.g. as to the wording of a specific document or the formulation of an e-discovery request) is, in fact, exercising her own "professional judgment." Using an AI algorithm is different from using a word processing program.

The level of independent decision making by the AI is significant. A lawyer using an AI algorithm that makes significant decisions should inform her client that she is using AI and how it functions so that she complies with Rule 1.4. She might also obtain client consent to the use of the algorithm as a precautionary measure.[5]

Kansas and Missouri Rules 5.1 and 5.3 place responsibility upon lawyers to supervise non-lawyer assistants and, in the case of lawyers who manage a law firm, to establish rules and procedures so that non-lawyer assistance is rendered in compliance with the *Rules of Professional Conduct*. As a result of a 2012 change in the language of Rule 5.3 from "assistants" to "assistance" many commentators take the position that the obligation to supervise under rules 5.1 and 5.3 extends to **non-lawyer assistants such as AI**. Gordon and Ambrose remark:

Under Model Rules 5.1 and 5.3, lawyers have an express obligation to supervise the work of both the lawyers and nonlawyers that they engage to assist them in providing legal

---

[4] David L. Gordon & Rebecca L. Ambrose, "The Ethics of Artificial Intelligence," online at https://www.jacksonlewis.com/sites/default/files/docs/Final_The%20Ethics%20of%20Artificial%20Intelligence_Gordon%20and%20Ambrose.pdf.
[5] Gordon & Ambrose, p. 6.

services to ensure that their conduct complies with the Rules of Professional Conduct. While these rules are typically applied to humans, a 2012 adoption of an amendment to Model Rule 5.3 makes clear that these rules likely extend to AI as well. In 2012, the ABA approved the Ethics 20/20 Commission's recommendation to change the title of Rule 5.3 from "Responsibilities Regarding Nonlawyer Assistants" to "Responsibilities Regarding Nonlawyer Assistance." [6] This change shows that the rule is intended to have reach beyond human assistants, to other nonlawyers, human or not, involved in the representation of a client.

This, of course, opens the question of how a lawyer goes about "supervising" an AI to insure that its functions in compliance with the *Rules of Professional Responsibility*. This will require, at the very least, that a lawyer have a working knowledge of how the AI algorithm functions and confirm that the AI does not violate any Rules as it functions. This may not be a simple task and may well place an untenable burden on many lawyers who do not possess specialized knowledge of computer science.

There is a very strong likelihood that the advantages of using AI algorithms to replace human lawyers in accomplishing various tasks in law practice will increase their use considerably in coming years. Using AI for many tasks provides faster and less expensive services both to lawyers and to their clients. Increases in computing power and increased sophistication of AI algorithms will almost certainly lead to their wider use. But lawyers must recognize that the use of AI in their practices burdens them with new twists on traditional ethical responsibilities. And failure to realize this and take steps to meet these responsibilities could result in disciplinary or malpractice actions.

NEW AUTHORITY
ABA FORMAL OPINION 498: VIRTUAL PRACTICE

On March 10, 2021, the ABA Committee on Ethics and Professional Responsibility released Formal Opinion 498 on "Virtual Practice." The release of this opinion has been long expected, and it does not contain any significant surprises. As the opinion notes, lawyers had begun to do more and more work from home or away from the office over the past decade and the COVID-19 pandemic accelerated the emerging trend. It is also quite likely that this trend will continue for many lawyers even after the pandemic lessens and eventually ends.

The first part of the opinion is a reminder to lawyers about how the *Rules of Professional Responsibility* impact virtual law practice. First, of course, the opinion mentions Rule 1.1 on competence and Comment 18 to the Rule, which requires lawyers "to keep abreast of changes in

---

[6] Gordon & Ambrose, p. 7; see, also, Rafael Baca, n. 3, above, p. 3.

the law and its practice, including the benefits and risks associated with relevant technology." The opinion goes on to discuss that both Rules 1.3 and 1.4 continue to be requirements for virtual practice and to remind lawyers that, even though they may be practicing online, they must still remain diligent and communicate with their clients as Rules 1.3 and 1.4 require.

Importantly the opinion also reminds lawyers that Rule 1.6 on confidentiality applies to virtual practice and that such practice may well require special efforts by the lawyer. The opinion refers several times to Formal Opinion 477R regarding securing communication of protected client information:

> …depending on the circumstances, lawyers may need to take special precautions. Factors to consider to assist the lawyer in determining the reasonableness of the "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." As ABA Formal Op. 477R summarizes, "[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."

Finally, the first section of the opinion reminds lawyers of their supervisory responsibilities under Rules 5.1 and 5.3. These two rules require that lawyers adequately supervise both lawyers and non-legal assistants to ensure that all are aware of the *Rules of Professional Conduct* and comply with them. Supervision, like confidentiality, may require special efforts when it is not done in person.

The second part of Opinion 498 deals with some special aspects of using "virtual practice technologies." Those highlighted are "hardware/software systems," "accessing client files," "virtual meeting platforms and video conferencing," "virtual document and data exchange platforms," "smart speakers, virtual assistants, and other listening-enabled devices." Finally the opinion elaborates on the special problems with supervision mentioned in the first section. The underlying ethical concerns of all of these discussions is with confidentiality of client information when using these digital technologies.

The opinion, for example, warns lawyers that they must make special efforts when using virtual meetings:

> Lawyers should ensure that they have carefully reviewed the terms of service applicable to their hardware devices and software systems to assess whether confidentiality is protected. To protect confidential information from unauthorized access, lawyers should be diligent in installing any security-related updates and using strong passwords,

antivirus software, and encryption. When connecting over Wi-Fi, lawyers should ensure that the routers are secure and should consider using virtual private networks (VPNs).

The opinion applies the same considerations to the use of virtual document exchange. Interestingly, the opinion also discusses situations where lawyers in law firms supply their own devices to carry on their virtual practice. The opinion states that every law firm should have a policy about such use and that it should "ensure that security is tight." Law firms might well want to adopt a policy prohibiting lawyers from using their personal laptops or cell phones, thereby avoiding the risk that a personal device might not be sufficiently secure.

Another quite interesting aspect of the opinion is its discussion of smart speakers or "other listening-enabled devices." Many lawyers use such devices at home for a multitude of purposes such as accessing the web, streaming music, etc. Unfortunately, these devices are often insecure and may be accessed by the manufacturer or third parties. If lawyers are, in fact, working from home, they may not even realize that their listening-enabled devices are nearby or have the capacity to hear their discussions of client confidential information. The opinion proposes a simple and safe solution to this potential Rule 1.6 problem. Lawyers "should disable the listening capability" of all such devices in the workspace.

The opinion concludes with a section discussing "possible limitations on virtual practice." Lawyers will always have to perform certain tasks, such as writing checks and maintain trust accounts and records. They will have to receive "paper mail." Even when they are practicing virtually, if they continue to maintain a brick and mortar office they will have to be able to communicate to clients by appropriate signage whether they are in and how they can be contacted virtually.

Opinion 498 is a useful, basic guide to the ethical issues raised by virtual practice. All lawyers and law firms engaged in such practice should ensure that they are aware of these issues and take appropriate steps to comply with all of the applicable *Rules of Professional Conduct*.

TECH TIP
GUARDING AGAINST AN ATTACK
by Matthew Beal, JD, MCSE, MCP, A+, SEC+

Over the past several weeks there have been multiple high-profile attacks on both public and private sector computer networks and systems. These include the SolarWinds attack on Microsoft and multiple government entities, the Microsoft Exchange Server self-propagating virus, and multiple reported attacks on Android and Apple devices. When hackers perpetrate attacks like these, the victims remain completely unaware of ongoing nefarious activity. For example, SolarWinds is a company that works with clients to monitor and control

network activities, virus and malware threats, and network traffic. Yet, unbeknownst to the company, its own systems were under attack for a period of months. Significantly, SolarWinds did not discover the breach until after it had propagated updates containing corrupted code to its clients. By the time the breach was discovered, the hackers had infiltrated multiple systems of SolarWinds's clients.

No business wants hackers gaining access to its electronically stored information. But attorneys have an ethical obligation to protect the client-related information on their computer systems. Specifically, Rule of Professional Conduct 1.6 requires that attorneys maintain all "information relating to the representation of a client" in a confidential manner. To that end, attorneys must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Knowing that cyber-attacks are a reality, your law office should be prepared to: (1) guard against an attack; and (2) respond should your office fall victim.

Your office can guard against an attack with relatively basic protections. Institute and maintain administrative permissions and do regular patch maintenance. Ensure your organization's devices and applications are updated to their most current versions. Operating systems that are no longer supported (and, therefore, no longer updated) should not be used. If you have an application that requires an outdated operating system, do not allow that computer to access the internet. And, because simply changing passwords with regularity can make the data those passwords protect more secure, an ageing guideline (one that requires all users to update their passwords at specifically timed intervals) can be extremely helpful. Of course, keep those passwords unique by following the password guidance we have discussed previously.

Should your office become the victim of a hack, it will be best able to respond if you keep and maintain a back-up of your office infrastructure data, including, as needed, device configuration settings for essential systems such as user credential repositories, major organization applications such as email servers, and other essential applications. Separately, you should also be maintaining a backup copy of your electronic client files. These backups need to be kept updated on a frequent basis. If feasible, keep a temporally current copy offsite.

By taking these precautions, you will protect your computing environment from basic intrusion attempts and maintain a basis to recover data that could be lost during an attack.

ETHICS & MALPRACTICE RESEARCH TIP
ARTIFICIAL INTELLIGENCE RESOURCES AND RESEARCH TIPS

The following books and articles provide a more detailed discussion of artificial intelligence in general and how it affects the law and legal ethics, as discussed in this month's lead article.

General Articles about AI:

Mariya Yao et al., *Applied Artificial Intelligence: A Handbook for Business Leader* (2018).

Max Tegmark*, Life 3.0 Being Human in the Age of Artificial Intelligence* (2018).

Binto George et al., *Artificial Intelligence Simplified: Understanding Basic Concepts* (2021).

Articles about AI and the law:

Harry Surden, *Artificial Intelligence and Law: An Overview*, 35 Ga. St. U. L. Rev. 1305 (2019).

Daniel Faggella*, AI in Law and Legal Practice – A Comprehensive View of 35 Current Applications*, EMERJ (last updated Mar. 14, 2020), available at https://emerj.com/ai-sector-overviews/ai-in-law-legal-practice-current-applications/.

Lauri Donahue, *A Primer on Using Artificial Intelligence in the Legal Profession*, JOLT Digest (Jan. 3, 2018), available at https://jolt.law.harvard.edu/digest/a-primer-on-using-artificial-intelligence-in-the-legal-profession.

BLAST FROM THE PAST
JUSTICE POTTER STEWART: ETHICS IS

This month's quote is from Justice Potter Stewart and requires not comment or interpretation:

"Ethics is knowing the difference between what you have a right to do and what is right to do."