Ethics and the Rise of AI

As Technology Evolves, So Will the Impact on Rules of Professional Conduct

By Hon. Heidi W. Currier, Jessica Lewis Kelly, Natalya Johnson and Robert Hille

Technology and the digital revolution have transformed the way we do things. While some say these advances have created greater efficiencies and brought the world closer together, they have also created new threats to our privacy and security.

The justice system is not immune to abuse and misuse of technology. Courts and lawyers can find it difficult to keep pace and embrace the benefits of rapidly advancing technological tools while avoiding harm.

The ongoing expansion of access to and use of artificial intelligence, especially generative AI, further complicates the ethical landscape for law professionals, both in and outside the courtroom.

Historically, cybersecurity efforts were primarily focused on how to prevent bad actors from accessing data and systems. Systems were constantly updated to detect and prevent unauthorized access while users were trained to recognize and avoid social engineering attempts at access by hackers. Theft of digital data and the information it contained as well as access to financial systems created new opportunities for criminals.

The acquisition of personal or proprietary information not only creates a large-scale risk of embarrassment through social media but identity theft also permits access to financial accounts and conversion of property. Correcting the consequences of identity theft places an enormous burden both on individuals and institutions.

Access to computer systems enabled control of those systems by a third party as well as the ability to shut them down entirely. Ransomware created large payouts for hackers. Additionally, such access through malware allowed for unauthorized access to information, alterations of data and the unfair and unknown competitive use of information causing substantial harm.

Without the proper framework, AI exacerbates these ongoing threats: (1) by expanding the pool of potential bad actors from highly skilled technologists to anyone with access to a smartphone or computer, (2) by improving the quality and believability of deepfakes, and (3) by increasing the frequency and level of cyber-attacks. For lawyers, AI might be the catalyst that transforms cybersecurity from nice-to-know to need-to-know, as suggested by the New Jersey Supreme Court's consideration of a possible new CLE requirement in "technology-related legal subjects" and a potential comment to RPC 1.1 ("Competence") regarding technology.[1]

Through a faster processing tool that draws from an enormous database, AI seeks to empower us to become more efficient, more understandable, and more creative. Viewed more cynically, AI seeks to become a better version of us.

Early stages of AI tools, still in use, examined what we and others said. It then tried to anticipate what we would say next. Constantly monitoring what we said, it strived for better predictions or to provide us with better alternatives. Examples can be seen with ubiquitous word processing programs including texting options for smartphones. When typing a text or email, the device offers choices on what it believes you want to say (or should say) next. Many emails come with pre-prepared suggested replies increasing the danger of unintended consequences due to rapid responses without time for reflection.

The evolution of AI technologies also presents evolving considerations. Generative AI seeks to go a step further. It seeks to create for us, in a fraction of the time, a work product that is better than what we could do ourselves. To do this, it accesses a vast universe of information and works in response to prompts from the user. The more detailed the prompt, the better the response. The goal of generative AI is to integrate the ability to touch, see, hear, smell and taste. In other words, AI seeks to become us, only a better version.

In exchange, AI also learns from its users. Each interaction and input of information improves AI's inferencing that allows it to compare what we did and want to do with other examples from its universal framework. Through this expanding universe or large language platform, AI is constantly seeking to improve. The larger its universe and

THE HON. HEIDI WILLIS CURRIER *is the Deputy Presiding Judge of Administration of the Appellate Division. Judge Currier sat in both the Civil and Family Divisions in Middlesex County Superior Court prior to her elevation to the Appellate Division. She is a member of the Supreme Court Committees on Artificial Intelligence and the New Jersey judicial team working with the National Courts and Sciences Institute initiative on Data Science and Artificial Intelligence.*

JESSICA LEWIS KELLY *serves as a Special Assistant to the Administrative Director of the New Jersey Courts. She is a member of the NJSBA Committee on Artificial Intelligence and supports the Supreme Court Committee on AI and the Courts, the Working Group on Judiciary Use of AI, and the New Jersey delegation to the National Courts and Sciences Institute Data Science and AI Initiative. Jessica routinely provides CLE instruction on AI and other topics, including well-being in the law and jury reforms.*

NATALYA G. JOHNSON *is senior director and senior counsel for Johnson & Johnson. She is a skilled corporate counsel with expertise in employment strategies, litigation, and impactful community leadership. She is the Chair of the Special In-House Committee and a member of the Task Force on Artificial Intelligence and the Law of the New Jersey State Bar Association. In 2024, she joined the Board of Trustees of Public Media NJ, the operator of NJ PBS.*

ROBERT HILLE *is a former NJSBA President and partner at Greenbaum, Rowe, Smith & Davis, LLP where he serves as trial and appellate counsel. Bob practices in the areas of ethics/professional liability, insurance and health care and is also a member of the firm's white collar practice team. Bob has also appeared as a guest analyst on* Law & Crime *and* Court TV *and is the author of several treatises and numerous articles.*

> There can...be a tendency for an AI tool to suggest how lawyers should approach a legal problem or brief. While this may be helpful, it may not be the best course in a particular case because its suggestion may not be compliant with our court or evidence rules or pertinent case law. It could also lead to a generalized response when the circumstances call for a particularized one.

the more information and specificity it receives from its users, theoretically, the better the final product.

These technological advances can similarly benefit the legal system and its participants. Yet with its potential benefits, AI and Generative AI add another layer to privacy and security risks and further threaten technological vulnerabilities.

As with any digital tool, AI is only as good as its programming, its database and what is inputted. An additional consideration is its programming capacity to learn from its accumulation of data and user interaction.

By now, we are familiar with AI hallucinations and briefs containing non-existent sources. In some of those circumstances, attorneys were sanctioned by the court. The error in the AI tool's output was no excuse for the attorney's failure to review and verify the accuracy of court submissions.

We are also familiar with potential inherent biases in AI programs. Because AI draws its learning from the past to the user's point in time, its inferences can be biased. Some examples of this could include the use of an AI hiring tool to find ideal employee candidates. However, the tool measured past employee backgrounds and performances. The result was the creation of a racial or gender bias in its hiring screening and recommendations.

There can also be a tendency for an AI tool to suggest how lawyers should approach a legal problem or brief. While this may be helpful, it may not be the best course in a particular case because its suggestion may not be compliant with our court or evidence rules or pertinent case law. It could also lead to a generalized response when the circumstances call for a particularized one. Another danger is AI could repeatedly direct a lawyer to a portion of its universe that is not where the lawyer wants to go or should go. The result could be a blind spot for the lawyer. Instead of boosting efficiency, the use of AI may result in the lawyer spending more time working around the tool's misplaced suggestions to locate relevant content.

Another area of concern is created by research vendors. Within these research tools, vendors also seek to improve their AI tools. They do this by bombarding lawyers with pop-ups directing them to click into AI programs. Ostensibly, their purpose is to entice lawyers to see how good their AI tool is. But this also can lead to inadvertently clicking into an AI program and potentially sharing confidential information without intending to do so.

Sometimes, AI-generated articles take on the appearance of a primary resource created by a person or reputable organization or entity. A tell-tale sign here is the absence of an identifiable author. Just as lawyers must locate and read any cited case law (whether suggested by AI or otherwise), so too they must check the sources referenced in any article offered by AI to confirm its existence and the accuracy of the referenced content.

Most importantly, AI exacerbates the risk of unauthorized disclosure of or unauthorized access to confidential information entrusted to the lawyer.

AI can obtain information from a lawyer when the lawyer has inputted information into the tool or gave the tool access to a database. Where the tool is only accessible to the lawyer or the firm, this may not be a problem, so long as appropriate security measures are established and routinely monitored. If the lawyer uses a vendor-based system, additional privacy concerns abound, requiring extensive vetting of AI vendors.

Similar risks exist for employees and members of the judiciary who use AI and Generative AI tools. Judges and court staff are prohibited from inputting any confidential or non-public information into public AI tools. The New Jersey Courts are cautiously exploring in-development retrieval augmented generation models that might in the future enable broader use of AI to improve court services. This work is guided by the Statement of Principles for the New Jersey Judiciary's Ongoing Use of Artificial Intelligence, as approved by the Supreme Court in January 2024.[2]

With the proliferation of AI technology, new laws and regulations have emerged. Currently, there is an absence of a single overriding federal law; however, a patchwork of state and even foreign regulations have emerged. Some states have reviewed Rules of Professional Conduct to help establish a uniform framework to help guide the responsible use and implementation of artificial intelligence technology related to the practice of law.

Prior to the rise of AI, the Court placed the ethical burden on counsel in RPC 1.6(f) "to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of or unauthorized access to information relating to the representation of the client." RPC 1.0 defines "reasonable" as "the conduct of a reasonably prudent and competent lawyer."

The Official Comment to that RPC requires a lawyer to safeguard "electronically stored information" in the lawyer's control from access by third persons, including a vendor. Additionally, RPC 5.3 makes a lawyer responsible for failures of vendors and other entities or persons the lawyer contracts with to protect confidential information.

Where third persons improperly access confidential information entrusted to the lawyer, the Official Comment to RPC 1.6(f) lists a number of factors to consider in deciding whether the lawyer's conduct breached the rule. The list is not exhaustive.

Identified factors are (1) the information's sensitivity; (2) likelihood safeguards would have prevented disclosure; (3) the cost of additional safeguards; (4) the difficulty of implementing additional safeguards; and (5) the extent such safeguards impair the lawyer's ability to represent clients. Clients may require specific safeguards or give informed consent to forgo security measures otherwise required.

We see that many of the concepts surrounding ethical and responsible artificial intelligence principles coincide with the underlying tenets of our RPCs. For example, frequently when exploring AI and ethics, terms such as explainability, transparency, fairness and mitigation of bias are implicated. These concepts relate to and connect with RPCs governing competence, confidentiality, and candor.

In addition to the New Jersey Supreme Court Committee on Artificial Intelligence and the Courts, an AI task force set up by the New Jersey State Bar Association established New Jersey as one of the first states to explore the responsible integration of artificial intelligence into legal practice and adherence to ethical standards. The task force evaluated the rules at play to assess and determine whether the RPCs were sufficiently flexible to relate to the rise of AI use and to cover professional conduct with legal practice when leveraging AI. That task force became a formal committee of the Association after submitting its report and continues its work in this field. Other jurisdictions also engaged in this exercise, including states such as New York and Pennsylvania.

In 2024, the American Bar Association issued its Formal Opinion 512 entitled Ethics Guidance and Lawyers Use of AI tools. The ABA and jurisdictions around the country have reached similar conclusions about the broad applicability and flexibility of RPCs to cover AI use. Some of the specific rules at play include the ABA Model Rules of Professional Conduct: Competence (Rule 1.1), Confidentiality (Rule 1.6), Communication (Rule 1.4) and more. Ultimately, attorneys are responsible for work product and output regardless of how it is generated.

The standards regarding confidential information as expressed in the RPCs also impose the potential for civil liability on lawyers.

In *Baxt v. Liloia*, 155 N.J. 190 (1996), the Court held that a breach of the RPCs could not form the basis of a civil action against a lawyer. However, the RPCs are conduct standards for lawyers. That is, they are evidence of the standard a lawyer is required to follow. Where a breach of a particular RPC standard contributes to some harm, a lawyer can be held liable for legal malpractice. This is now grafted into the language of the Model Jury Charge on Legal Malpractice.[3]

As noted, AI is designed to outpace humans. To do that, it must constantly learn. That can only be done by feeding

In addition to the New Jersey Supreme Court Committee on Artificial Intelligence and the Courts, an AI task force set up by the New Jersey State Bar Association established New Jersey as one of the first states to explore the responsible integration of artificial intelligence into legal practice and adherence to ethical standards.

on what the user gives it. This is why research AI financial stakeholders want to direct us to constantly use AI.

A common goal for creator and user may be availability of and access to a perfect and helpful legal product. However, financial stakeholders are primarily driven by profit, not ethics. Lawyers' interests must always be guided by ethics and their fiduciary duties.

In a proactive effort to address risks imposed by AI, the Court formed a ommittee on Artificial Intelligence and the Courts. That committee preliminarily recommended that the risks posed by AI use were adequately addressed in the RPCs as currently configured and did not require amendment or supplementation. But the Court also recognized additional considerations AI use presented in the ethics context and the need for guidance to the Bench and Bar in that regard.

As to the Judiciary, the Court issued the public-facing Statement of Principles, which articulate how AI will be used in alignment with the Judiciary's core principles of Independence, Integrity, Fairness, and Quality Service. The statement includes a promise to "engage in ongoing oversight to ensure that AI technologies are Transparent, Explainable, Accurate, Reliable, and Secure."

Judges are permitted and encouraged to use AI, as guided by the Code of Judicial Conduct, Rule 1:38 and judiciary policies. AI is a useful tool for research, and the drafting or refining of non-legal communications, such as speeches and remarks. However, decision-making and judicial writing remain in the sole province of a human judicial mind.

Although a litigant is not required to reveal the use of AI in writing briefs or making arguments in New Jersey, judges are learning to detect the use of AI in cases and in the courtroom. This will be particularly prevalent in expert opinion and testimony as the technology evolves and litigants' use of it expands.

Lawyers and judges will need to work together to identify the AI work product and resolve issues surrounding it.

As to lawyers, the Court issued Preliminary Guidelines on the Use of Artificial Intelligence by New Jersey Lawyers in a Jan. 24, 2024, Notice to the Bar and authorized a survey distributed to more than 75,000 attorneys regarding their views of and experiences with generative AI technologies. Guided by the thousands of responses to that outreach, the Judiciary committed to provide no-cost CLE programs regarding AI. To date, those programs include a July 24, 2024, webinar, with leaders of the Office of Attorney Ethics, focusing on the ethical implications of AI use, and a Dec. 19, 2024 webinar regarding AI implications for cybersecurity.

In noting some of the problems lawyers and the courts have experienced with AI, the Court in its Preliminary Guidelines warned lawyers that their core ethical responsibilities remain unchanged when using AI tools. They must employ the same commitment to diligence, confidentiality, honesty and client advocacy as with traditional methods of legal practice.

In this regard, the Court began by noting a lawyer's responsibility for accuracy and truthfulness. It then identified the requirements in RPC 3.1 Meritorious Claims and Contentions; RPC 4.1(a)(1) Truthfulness in Statements to Others (not making false statements of fact or law to third persons); and RPC 8.4(c) Misconduct (conduct involving fraud deceit or misrepresentation).

The Court then cautioned that where AI generated false information, the use of that information may result in those rules being violated because of the lawyer's duty to check and verify the accuracy of all AI generated information.

Next, the Court referenced the lawyer's responsibilities for honesty, candor and communication. As already required, a lawyer is responsible for ensuring the validity of AI-generated information contained in pleadings, arguments or evidence filed or submitted to a tribunal.

Where that information contains false, fake or misleading content, the lawyer may be in violation of RPC 3.3(a)(1) Candor Toward Tribunal (making a false statement of fact or law) or RPC 3.3(a)(4) (offering evidence the lawyer knows to be false). Because of the lawyer's duty to verify, knowledge will apparently be presumed. This requirement is also present in Rule 1:4-8(a) Frivolous Litigation (effect of signing legal court documents).

The failure to ensure accuracy might also be a violation of RPC 8.4(d) (conduct prejudicial to the administration of justice) and RPC 8.4(g) (conduct involving discrimination). The latter could occur where an inherent bias in a tool results in a discriminatory impact to the groups identified in RPC 8.4(g) or where a tool is used to advance a discriminatory use.

The Court also reinforced that a lawyer cannot use AI to manipulate or create false evidence, or to allow a client to engage in such conduct. Such impermissible actions can support violations of RPC 1.2(d) Scope of Representation and Allocation of Authority Between Client and Lawyer (cannot counsel or assist a client in conduct that is illegal, criminal or fraudulent); RPC 1.4(d) Communication (failure to advise a client of the inability to assist in conduct not permitted by the RPCs); and RPC 3.4(b) (falsify evidence, counsel a witness to testify falsely or offer a witness an illegal inducement).

In disclosing the lawyer's use of AI to a client, the Court noted that a lawyer did not have an affirmative duty to disclose the use of AI under RPC 1.2 (lawyer must abide by a client's decisions concerning the scope and objectives of representation after consulting with the client about the means to pursue them); 1.4(b) (lawyer must promptly comply with a client's reasonable request for information); and RPC 1.4(c) (lawyer must provide sufficient information for a client to make informed decisions regarding the representation).

However, a lawyer must inform a client about the use of AI if the client asks or if the client cannot make an informed decision regarding the representation without knowing that the lawyer is using AI. An attorney can use AI to explain issues to the client but the lawyer is still charged with ensuring the accuracy of information generated by AI.

The Court addressed privacy and security under RPC 1.6 Confidentiality. That rule covers all information relating to the representation of the client. This includes the client's identity. N.J.R.E. 504, Attorney Client Privilege includes a subset of that information relating to attorney-client communications with the expectation of confidentiality. In both instances, the client, not the lawyer, possesses the privilege.

As discussed above, RPC 1.6(f) specifically burdens the lawyer with the duty to make reasonable efforts to avoid unauthorized access or disclosure. The Court, in noting the array of AI tools including those designed for lawyers and those "in development for use by Law firms," views the ultimate responsibility to be the lawyers to ensure the security of an AI system where a lawyer enters non-public client information. The consequences of such a security breach by the tool could form a basis for an RPC 1.6(f) violation regardless of any fault of the AI program's creator or vendor.

It should also be noted that reasonable efforts under RPC 1.6(f) and the Official Comment to that section include the lawyer's obligation to become familiar with such tools and mechanisms to avoid security breaches of confidential information and employ such protective measures.

Where these RPC violations occur through AI use, the Court also reminded the Bar of its oversight responsibilities.

RPC 5.1 imposes on law firm principals and supervising attorneys the responsibility and liability for RPC violations by subordinates including the misuse of AI. Correspondingly, RPC 5.2 makes subordinates responsible for their violations even when directed by another unless in accordance with a supervising lawyer's reasonable resolution of an arguable question of a professional duty. In the risks of AI misuse identified by the court above, an arguable question of duty may be a difficult burden to meet.

In terms of AI use and arrangements with non-lawyers in the use of such tools, the Court specifically referenced RPC 5.3 and its requirements that lawyers remain responsible to ensure that the conduct of those retained or employed shall adopt and maintain reasonable efforts to comply with the lawyer's professional obligation. Consequently, the failure of a third party resulting in an ethics violation from the use of its tool, will not excuse a lawyer from potential discipline.

Finally, in its guidelines to the Bar, the Court says that its references to potential RPC violations are illustrative and not exhaustive. By way of example, the Court noted that the use of AI will likely affect lawyer billing "RPC 1.5 (Fees)" and advertising practices "RPC 7.2 Advertising." These and other specific applications may be addressed in future guidelines if and as needed.

The road map that the Court has given in navigating the use of AI in compliance with a lawyer's ethical responsibilities stresses how important it is for lawyers to stay familiar with technology, to use care in uses of new technology, and vigilant in upholding existing standards of professionalism.

The following references can serve as guides to attorneys as they navigate this ever-changing landscape of generative AI.

Our review and assessment of the legal and regulatory landscape governing AI will continue and so will the cases and circumstances that call into question the Rules of Professional Conduct and other guidelines. New Jersey has taken a leading role across sectors in preparing our government, the public, business entities, and legal professionals to foster innovation while simultaneously regulating the application of artificial intelligence tools in both business and society at large.

As to the Court's guidelines and its Jan. 24, 2024 Notice to the Bar, it can be found at njcourts.gov/sites/default/files/notices/2024/01/n240125a.pdf?cb=aac0e368. The New Jersey State Bar Association's Task Force recommendations and findings can be viewed at https://njsba.com/wp-content/uploads/2024/05/NJSBA-TASK-FORCE-ON-AI-AND-THE-LAW-REPORT-final.pdf. The Attorney Ethics Hotline can be reached at 609-815-2924. Suggestions for issues to be considered by the New Jersey Supreme Court Committee on AI can be emailed to COURT-USE-of-AI.mbx@njcourts.gov. ■

Endnotes

1. November 21, 2024 notice to the bar ("Attorney Responsibilities as to Cybersecurity & Emerging Technologies—(1) Proposed CLE Requirement and (2) Proposed Comment to the RPCs—Request for Comments") (njcourts.gov/sites/default/files/notices/2024/11/n241121e.pdf?cb=eec32cf0)
2. njcourts.gov/sites/default/files/courts/supreme/statement-ai.pdf?c=t2v
3. Model Jury Charges (Civil), 5.51A, "legal Malpractice" (rev. Oct. 2022)