NEW YORK STATE BAR ASSOCIATION

JOURNAL

TECHNOLOGY ISSUE

Who Is Minding the Bot? Human Oversight and AI

Also Inside:

Technology Takes Center Stage at the 2027 Annual Conference

150 Years NYSBA

FALL 2026
VOL. 98 | NO. 4


Clarity
starts at 8am™
8am solutions are trusted Member Benefits of the New York State Bar Association
8am.com/nysba
Run your business. Power your practice.
NYSBA
+
8am™
LawPay
MyCase
CasePeer
DocketWise

TECHNOLOGY ISSUE

CONTENTS

Departments

CONNECT WITH NYSBA | VISIT NYSBA.ORG

@nysba | @nysba | www.nysba.org/LinkedIn | @nystatebar | nysba

New York State Bar Association Journal welcomes articles from members of NYSBA on subjects of interest to New York State lawyers. Views expressed in articles or letters published are the authors' only and are not to be attributed to the NYSBA Journal, its editors or the New York State Bar Association unless expressly so stated. Authors are responsible for the correctness of all citations and quotations. For submissions guidelines: www.nysba.org/JournalSubmit. Material accepted may be published or made available through print, film, electronically and/or other media. Copyright ©2026 by the New York State Bar Association. Library subscription rate is $250 annually. New York State Bar Association Journal is published quarterly by the New York State Bar Association, One Elk Street, Albany, NY 12207. Print (ISSN 1529-3769), Online (ISSN 1934-2020). Periodicals postage paid at Albany, NY and additional mailing offices. POSTMASTER: Send address changes to: NYSBA, One Elk Street, Albany, NY 12207.

NEW YORK STATE BAR ASSOCIATION
JOURNAL

FALL 2026
VOL. 98 | NO. 4
NYSBA

EDITORIAL OFFICES
One Elk Street, Albany, NY 12207
518.463.3200 • FAX 518.463.8844
www.nysba.org

NYSBA ADVERTISING
Association Media Group
Nicola Tate, Vice President,
Media & Sponsorship Development
ntate@associationmediagroup.com
804.469.0324

SUBMISSIONS
Send articles to journal@nysba.org.
Review submission guidelines at
nysba.org/journalsubmit.

The New York Advantage: Preparing Lawyers for a Rapidly Changing Profession Through NYSBA's Tech Summit

Technology has always influenced the practice of law, but never at the velocity, scale or consequence we are experiencing today. Artificial intelligence is reshaping research and drafting. Automation is transforming workflows. Cybersecurity threats are escalating in sophistication. Courts are digitizing at an unprecedented speed. Clients expect seamless digital communication, data-driven insights and faster turnaround times. And regulators – especially in New York – are racing to keep pace with the ethical, privacy and professional responsibility implications of these shifts.

In this moment of profound change, the New York State Bar Association is stepping forward with a bold, future-focused program: **NYSBA Tech Summit**, a comprehensive program of CLEs, demonstrations and hands-on learning designed to equip New York licensed lawyers with the knowledge, tools and confidence to thrive in a technology-driven legal landscape.

Tech Summit is not simply CLE programming. It is a strategic investment in the future of the profession – and a reflection of NYSBA's commitment to ensuring that New York-licensed lawyers remain national leaders in legal innovation, ethical practice and client service.

Why Technology Is Now the Backbone of Legal Practice

For decades, technology was treated as an accessory to legal work – helpful, but not essential. That era is over. Today, technology is the infrastructure on which modern practice is built.

Consider just a few examples:

Generative AI is now capable of drafting documents, summarizing depositions, analyzing contracts and identifying patterns in large datasets.

Predictive analytics are informing litigation strategies and risk assessment.

Digital evidence – from smartphone data to surveillance footage to metadata – is central to both civil and criminal matters.

Cybersecurity obligations have become core components of ethical competence, especially in New York's highly regulated environment.

Remote and hybrid practice models require new approaches to confidentiality, communication and client engagement.

These tools are no longer optional. They are embedded in client expectations, judicial processes and the competitive realities of the marketplace. Lawyers who do not understand them risk falling behind – not only in efficiency, but in ethics, competence and professional responsibility.

Tech Summit is designed to meet this moment head-on.

Tech Summit: A Program Built for the Modern New York Lawyer

Tech Summit's CLEs and workshops are curated specifically for New York practitioners – a distinction that matters. New York's legal ecosystem is uniquely complex, fast-moving and influential. Our courts are early adopters of digital systems. Our clients operate in industries where technology and regulation collide daily. And our bar has long been a national leader in shaping ethical and professional standards.

Tech Summit reflects that reality by offering programming that is both forward looking and practically grounded, including:

1. CLEs on the Law of Emerging Technology

These sessions explore the legal frameworks governing AI, data privacy, cybersecurity, digital evidence and technology-driven client services. They provide authoritative guidance on how New York law is evolving – and how attorneys can stay ahead of regulatory change.

2. Practical Instruction on Integrating Technology Into Daily Practice

Members will learn how to use new tools to streamline workflows, improve accuracy, enhance client communication and strengthen case strategy. These sessions translate abstract concepts into real world skills.

3. Ethics-Focused Programming

Tech Summit places ethics at the center of its curriculum. Sessions will address confidentiality, competence, bias, transparency and the responsible use of AI – all through the lens of New York's professional standards.

4. Hands-on Demonstrations and Workshops

The expo component of Tech Summit allows members to interact directly with technology vendors, test new tools and see demonstrations of platforms that can transform their practice. This is experiential learning at its best.

5. New York-Specific Insights

Because NYSBA is uniquely positioned to understand the realities of practicing in this state, Tech Summit offers guidance tailored to New York's courts, clients and regulatory environment. This is not generic national programming – it is built for the lawyers who practice in the nation's most dynamic legal market.

Why NYSBA Is the Right Organization To Lead This Work

Many organizations offer technology programming, but none bring the combination of **New York's legal complexity**, **national influence** and **professional diversity** that NYSBA does.

NYSBA's leadership in this space is rooted in a deep, statewide understanding of New York's legal landscape – one that spans solo practitioners, small and large firms, government attorneys and in-house counsel. Because the association maintains strong, longstanding relationships with courts, regulators and legal institutions, it can anticipate shifts in the profession before they reach most practitioners. That insight is paired with a firm commitment to ethical leadership, ensuring that emerging technologies are integrated responsibly and in alignment with professional standards. And with a membership that reflects the full spectrum of legal practice across the state, NYSBA is uniquely positioned to deliver programming that resonates with every corner of the profession. Tech Summit is a natural extension of that mission: to support New York lawyers, strengthen the profession and uphold the rule of law.

The Stakes for New York Lawyers

The consequences of technological change are not theoretical – they are already reshaping the profession.

Competitiveness

Clients increasingly expect their attorneys to use technology to deliver faster, more accurate and more cost-effective services. Firms that embrace technology gain a competitive edge; those that do not risk losing business.

Ethical Competence

The duty of competence now includes understanding the benefits and risks of relevant technology. Tech Summit helps attorneys meet that obligation.

Cybersecurity

New York lawyers handle sensitive information daily. Cybersecurity breaches can have devastating consequences for clients and firms alike. Tech Summit provides essential guidance on protecting data and meeting regulatory requirements.

Access to Justice

Technology can expand access to legal services, streamline court processes and reduce barriers for clients. New York lawyers have a responsibility to understand how these tools can support justice.

Professional Identity

As technology reshapes the profession, lawyers must adapt – not by abandoning the core values of legal practice, but by integrating new tools in ways that strengthen those values.

Tech Summit is designed to help members navigate these challenges with confidence.

Beyond Technology: Strengthening the Whole Lawyer

While Tech Summit is the centerpiece of this issue, NYSBA recognizes that the future of the profession requires more than technological competence. It requires civic awareness, personal resilience and a commitment to the values that define our work.

To support that broader vision, NYSBA will also host:

A Civics Convocation

This gathering reinforces the role of lawyers as guardians of democratic institutions and the rule of law. In a time of polarization and misinformation, the legal profession's commitment to civic education and constitutional principles is more important than ever.

A Wellness and Self-Care Expo

The demands of legal practice are intense, and technology – while helpful – can also contribute to burnout and information overload. The Wellness and Self-Care Expo offers resources to support mental health, resilience and sustainable practice. It recognizes that the future of the profession depends not only on technological skill, but on the well-being of the people who serve it.

These programs complement Tech Summit by strengthening the whole lawyer professionally, civically and personally.

A Call to Action: The Future Is Here

Tech Summit is more than an event. It is a turning point for the profession.

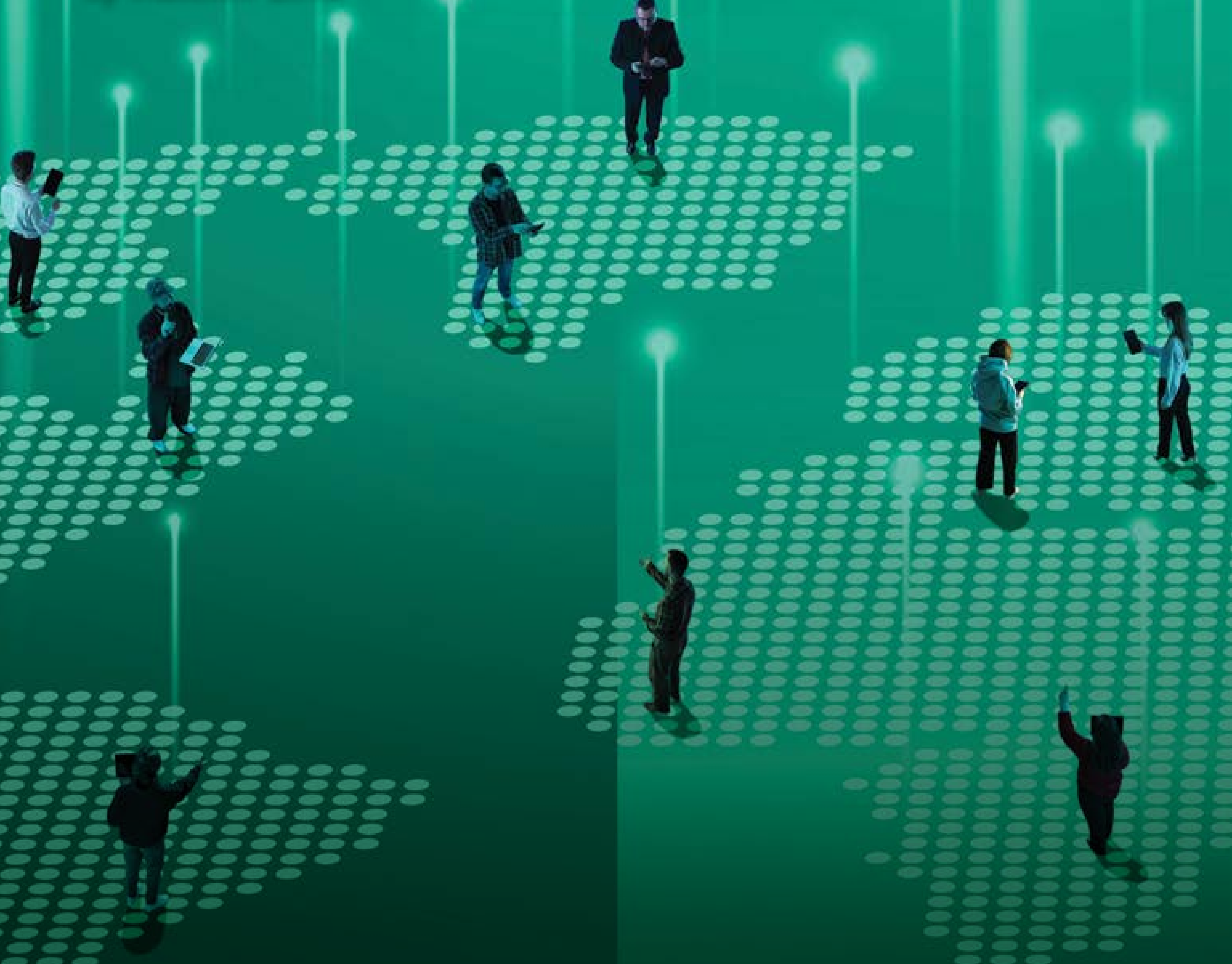
By attending, NYSBA members will gain essential knowledge about the technologies reshaping legal practice, learn practical skills they can apply immediately, and strengthen their ethical competence in an evolving professional landscape. They'll also connect with peers, innovators and leaders across the state, positioning themselves – and their clients – for success in a rapidly changing world. New York lawyers have always been at the forefront of legal innovation, and Tech Summit ensures we remain there. For more details, please see related story on page 61.

This is the moment to invest in your future. This is the moment to lead. NYSBA is ready to guide you – with the expertise, perspective and commitment that only New York can provide.

TAA GRAYS can be reached at tgrays@nysba.org.

Who Is Minding the Bot? Human Oversight and AI

By Matthew Lowe



Since the launch of ChatGPT in 2023, the use of artificial intelligence to do research, take over customer service functions and streamline tasks promises to radically change how people interact with the world. At the same time, we've also seen some of the perils of using AI uncritically: hallucinations in legal briefs, uninformed chatbots that help prepare a case pro se, students using AI to draft essays or in even more life-threatening situations such as recent reports of people following directions from chatbots to do harm to themselves and self-driving cars causing accidents.[1]

It's become clear that AI is not yet at the point where it can be trusted to always do the right thing. Any person or company using AI needs to be aware of the risks. Even more important, there needs to be a reliable framework for its use that includes human oversight. New laws, regulations and organizational policies are increasingly requiring that actual human beings oversee the AI programs they put into place. The EU AI Act, for example, employs human oversight as a necessary component of responsible AI governance. A term that has become popular in referring to the use of human oversight in AI systems is human-in-the-loop, suggesting that people are integral to any system using AI.

Yet organizations often struggle to put effective human oversight into practice. Simply placing a human somewhere in a workflow does not necessarily reduce risk or satisfy the underlying purpose of preventing bad outcomes or harm. Meaningful human oversight requires a person who can identify problems, exercise independent judgment and intervene before harm or injury occurs.

AI Incidents on the Rise

According to the AI Incident Database, which collects and indexes various types of incidents that cause harm due to AI, the number of such reports have doubled each year between 2022 and 2025. By October 2025, the number had already increased beyond the previous year.[2]

Nor have regulations kept pace with AI use. This is for three main reasons. First is the speed at which AI has been adopted. According to Tom Wheeler, a visiting fellow at the Brookings Institute's Center for Technology Innovation, "existing rules are insufficiently agile to deal with the velocity of AI development."[3] Second is the technology's multifaceted nature. Varying types, responses to prompts and unexpected applications make AI technology difficult to categorize neatly. Guidelines for attorneys using AI for research are going to be different from laws to prevent children from using bots to plan self-harm. Finally, the regulatory landscape is complex and fragmented. This is evident in the U.S.'s state-by-state approach and more so on a global level with major jurisdictions like the U.S. and EU employing different regulatory strategies.[4]

Still, regardless of the industry, regulation or framework, one piece of guidance is relatively common, and that is human oversight. The goal is straightforward: To ensure that an AI solution, an application that uses AI to address specific problems, such as a retail company deploying an AI-recommendation tool that analyzes customer purchase history to suggest products, operates safely and as expected, a human should be part of the decision-making process at critical points to monitor outputs. Human feedback and/or intervention is vital. However, questions tend to arise around when and how exactly human oversight ought to be implemented as a governance mechanism.

We must therefore explore how to meaningfully implement human oversight rather than superficially document instances of what is merely acceptable from a compliance standpoint in order to mitigate harm and liability.

Defining Human-in-the-Loop

While some prefer terms like human-in-the-loop, human-over-the-loop, human-out-of-the-loop, etc., such terms can sometimes be used inaccurately and/or interchangeably. They all refer to:

> AI systems that include human feedback or intervention as part of their operation. In these systems, humans may provide guidance, correct errors, or make final decisions to improve the accuracy and reliability of AI. This approach combines the strengths of both humans and machines, ensuring that complex or high-stakes tasks benefit from human judgment and oversight.[5]

Human-in-the-loop is mentioned by name or alluded to in almost every playbook providing guidance to groups using AI, especially in the context of systems that have the potential to cause material harm. To summarize a few areas where we see this concept:

- New York City's Local 144 prohibits employers or employment agencies from using an automated employment decision tool to make an employment decision unless the tool is audited for bias annually. The employer publishes a public summary of the audit and provides certain notices to applicants and employees who are subject to screening by the tool. According to labor and employment attorneys at Littler, the "threshold question is whether an employer is using an automated employment decision tool to make a covered employment decision and thus subject to the audit and notice requirements of the law," where a "covered employment decision" is one that involves hiring or promotion.[6] Here, while human-in the loop is not explicitly prescribed, it does serve as a tool to counteract bias.

- The EU AI Act, Art. XIV ("Human Oversight") requires that high-risk AI systems be designed so humans can effectively monitor, understand and override them. Its goal is to prevent harm to health, safety and fundamental rights by keeping algorithms under meaningful control. The AI system must also enable overseers to understand AI's limits, recognize bad outputs and safely intervene or stop the system before harm occurs.
- The National Institute of Standards and Technology AI Risk Management Framework recognizes that humans need to be more involved in some decisions made by AI than others:

> Human-AI configurations can span from fully autonomous to fully manual. AI systems can autonomously make decisions, defer decision-making to a human expert or be used by a human decision maker as an additional opinion. Some AI systems may not require human oversight, such as models used to improve video compression. Other systems may specifically require human oversight.[7]

This, of course, is a non-exhaustive list. Organizations like the International Organization for Standardization and the International Electrotechnical Commission's international standard for creating an AI management system, the Organization for Economic Cooperation and Development's AI Principles and states like Colorado also make recommendations for some aspects of human involvement. However, it does effectively demonstrate the range of ways in which human-in-the-loop is a vital part of AI oversight

Ultimately, a simple litmus test should leverage an ethical, commonsense approach to compliance: If a system is reasonably deemed capable of materially harming an individual, a higher level of human involvement should be required in an organization's governance process. The next question then is what is meant by "material harm"? And then, what is meant by "proportional human involvement"?

Less Than Effective Examples of Human Oversight

Across industries and different types of systems, a number of people and organizations are not quite getting compliance right when it comes to human oversight, as shown by examples mentioned above and below. It could be that those in charge may not be doing enough to anticipate and prevent harm. This is not to suggest that these entities are unethical, only that when laws and regulations are overly burdensome or poorly tailored. the process can turn into a bureaucratic checklist rather than meaningful reforms. This approach can lead to a hyperfocus on parts of the process and miss the bigger picture or lose sight of the AI tool's broader purpose. The hallucination of legal citations illustrates this problem: A user may focus narrowly on whether AI has produced citations that appear responsive to a research request, rather than whether those authorities actually exist and support the proposition for which they are being cited. In doing so, the user loses sight of the broader purpose of the tool, which should be to assist – rather than replace – the attorney's independent research, judgment and responsibility for the final work product.

Meaningful human oversight can be especially difficult to design, as it – as a control – is susceptible to a range of well-documented cognitive biases. For example, a reviewer looking at a 50-page AI-generated report of a generated model might assume that the report's conclusions are likely accurate because the report was produced by a sophisticated system. Similarly, when multiple reviewers are involved and there is no clarity about who should be checking what, each may assume someone else has already performed a detailed review. In both cases, oversight exists on paper but may be ineffective in practice because of user bias or assumptions. Collectively, blind spots like these can reduce reviewers from active decision-makers to passive monitors, undermining the very safeguards that human oversight is intended to provide. Essentially, the diligence an individual applies may diminish when that person believes someone or something else is also responsible for the output, especially when it's done by a nonhuman tool seen as infallible. This varies depending on the extent to which one perceives authority or expertise. In other words, whether it is a group project or an AI output, the need one feels to contribute diminishes since some individuals might consciously or unconsciously believe that "the rest of the group won't allow us to fail, so I can do a little less" or "the likelihood of the AI getting it wrong is probably low, so I don't need to review too closely."

Weaknesses in the System: The Example of Michael Cohen

Shortly after the first mainstream generative AI models became prevalent, instances of misuse by attorneys began to appear. Arguably the most famous of these cases involves Michael Cohen, President Trump's former lawyer, and Cohen's counsel. In 2023, Cohen was in the process of securing an early end to a 2018 court-ordered supervised release after serving for charges ranging from campaign finance fraud to tax evasion. Cohen passed along AI-generated, hallucinated case citations to David Schwartz, his attorney at the time, who then submitted them to the judge as part of their filings, who subsequently discovered the hallucinations.

There are a few notable takeaways from this incident. One comes from Cohen blaming Schwartz for failing to check the validity of his citations before submitting them to the judge after stating that as a non-lawyer (he was disbarred) he has "not kept up with emerging trends (and related risks) in legal technology and did not realize that Google Bard was a generative text service that, like Chat-GPT, could show citations and descriptions that looked real but actually were not." He "understood it to be a super-charged search engine and had repeatedly used it in other contexts to successfully find accurate information online."[8] This is an effective articulation of automation bias, to which Cohen had succumbed.

However, the failure was not just Cohen's. Schwartz, as the attorney, had an ethical obligation as the responsible party for conducting an appropriate review of the information Cohen gave him. He acknowledged that he had failed in his duty, stating, "I am fully aware that I bear the responsibility for any submission on my letterhead and the inaccuracies contained in this filing are completely unacceptable … I sincerely apologize to the court for not checking these cases personally before submitting them to the court."[9] Ultimately, U.S. District Judge Jesse M. Furman determined that the false citations were not submitted in bad faith, so he did not impose sanctions. He did, however, in a March 2024 ruling, refer to the incident as "embarrassing." Cohen's other representative in this matter, E. Danya Perry, stated that "even a quick read" of the citations "should have raised an eyebrow."[10]

Another key takeaway is that at this point, courts had already been seeing an increase in case filings riddled with AI hallucinations; this just happened to be particularly high-profile. And, while one might assume that media attention would lead to the elimination of such carelessness, since then, lawyers and law firms continue to make these kinds of mistakes despite the document-review resources at their disposal.[11]

Failures of human oversight can be observed across a variety of areas besides the practice of law. The hallucination problem, for example, can be seen in multiple professional consulting instances. In 2025, Deloitte offered the Australian government a partial refund "for a report that was littered with AI-hallucinated quotes and references to nonexistent research."[12] This year, the consulting firm EY had to withdraw a study it produced, "which was used by EY consultants in Canada to market their cybersecurity business, used made-up data, misattributed citations and referenced a McKinsey report that does not exist, online researchers discovered."[13] KPMG, one of the largest consulting firms in the world, was also recently accused of "publishing a report on the future of AI with 40 of 45 citations that appeared to be at least partially AI hallucinations," resulting in KPMG having to take it down.[14]

When AI Goes Really Wrong: Self-Driving Cars and Failures of Human-in-the-Loop

Among the most serious examples of ineffective human oversight is the death of Elaine Herzberg in 2018 by a self-driving car. In that case, while Uber was test-driving autonomous vehicles in Arizona, a backup driver who was seated in the driver's seat expressly to take action in case of AI failure was allegedly streaming an episode of "The Voice" when the vehicle struck and killed Herzberg, a pedestrian. Publicly reported evidence included dash-cam footage showing the driver "looking down, away from the road, for several seconds immediately before the crash, while the car was traveling at 39 mph," and records from the streaming service Hulu. One report showed that from the start of the trip up until the accident, the backup driver was on her phone 34% of the time.[15] The driver, originally charged with homicide, pled guilty to a charge of endangerment in July 2023.

The investigation also found that Uber's system failed to include the potential of a pedestrian crossing outside of a crosswalk and that the company had removed a requirement for there to be two backup drivers in each car in the months leading to the accident. Drivers were also assigned the same monotonous route throughout their usual eight-hour shifts, making them more likely to seek distraction. Uber was not charged but pledged to make changes to address these issues.[16]

Meaningful and Ethical Design Choices

It is unlikely that those individuals and organizations held accountable for these human oversight failures intended to deceive or cause harm. Instead, the reality is that AI and its potential to do harm are still being understood. Any regulations that are imposed, whether by governing bodies or within companies themselves, need to include an appropriate level of human oversight. While the use of AI at this scale is evolving, there are steps that can be taken to reduce the potential for harm.

When assessing whether an AI system has sufficient potential for harm, regulations like the EU AI Act can get quite prescriptive. For instance, the act's Annex III lists high-risk use cases including biometrics, critical infrastructure, employment, law enforcement, immigration and the administration of democratic processes. Borrowing from the EU AI Act and other relevant frameworks and regulations can help formulate a practical test on whether meaningful oversight should be implemented when a given AI system (1) has the potential to produce an inaccurate result or unintended consequence, recommendation or decision that (2) could reasonably result in significant harm to an individual, an organization, or the public, where "harm" includes:

- Physical injury
- Financial loss
- Denial of employment or educational opportunities
- Adverse legal consequences
- Discrimination
- Privacy or cybersecurity harms
- Reputational damage, or
- Other decisions that materially affect a person's rights, safety or well-being.

Even simpler is to ask: What is the worst that could happen if a given AI system fails? And if the answer is that someone could suffer material harm, meaningful human oversight should be embedded into the system's lifecycle at the point where it would have optimal impact. But what is meant by meaningful human oversight?

In order to have meaningful human oversight with the right level of proportional human involvement, the person has the information, authority, ability and opportunity to independently evaluate an AI system's output and intervene before material harm occurs. Put simply, meaningful human oversight requires more than a human in the process – it requires a human who can meaningfully influence the outcome and who is properly empowered to do so. In order to enable such human oversight, we must also consider social and cultural concepts that can influence whether intervention will be effective, as we've seen with the Michael Cohen case.

Going back to the case of Uber's self-driving car hitting a pedestrian, the role of cellphones is one area that needs to be addressed. In a scenario where a person is tasked with serving as a backup driver for a self-driving vehicle that can potentially cause physical harm to other drivers or pedestrians, a responsible use of human-in-the-loop would require that phones not be used during test sessions or at least restricting access to certain apps so that emergency calls can still be made. Apps that may lead an individual to engage actively and for extended periods of time should be blocked from access, such as streaming apps and mobile games. Backup drivers for self-driving cars should be expected to assume as much responsibility as if they were driving the cars themselves.

In the case of legal case hallucinations, someone seeking representation who trusts legal counsel to practice competently (an expectation that is also codified and required under the ABA Model Rules of Professional Conduct), which includes reviewing AI decisions and actions, can end up losing a case, resulting in significant damages or incarceration. This is a material harm and therefore requires that there be formalized processes to ensure that filings have been properly reviewed.

In the case of *United States v. Cohen*, Schwartz said he thought drafts of the papers to be submitted to the court were reviewed by Cohen's other counsel in the matter. If faced with a similar scenario, attorneys should know to verify such an assumption, rather than diffusing responsibility and carelessly filing case citations that are handed to them. In the consulting industry, clients similarly trust reputable firms to produce reliable information when making critical decisions that have impacts on their business reputation and financial condition, and therefore facts and footnotes should be properly vetted before publication.

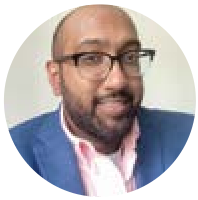
Conclusion: Questions To Consider for AI Governance

It is easy to compile a list of mistakes and criticize those who committed them. However, as attorneys, we have a responsibility to learn the right lessons when things do go wrong and use them to enhance our processes to meaningfully address governance controls like human-in-the-loop. Effective governance of AI systems and risk management relies on the understanding that the processes that support them are iterative and constantly improving based on what we learn in taking actions, and what we reasonably can anticipate before taking those actions. That is why ethical reasoning is critical to deploying effective and sustainable governance processes. Before deploying or approving the use of an AI system, legal and compliance teams should consider:

- What is the reasonably foreseeable harm if the system makes a mistake?
- Who is accountable for reviewing high-risk decisions?
- Does the reviewer have sufficient expertise to identify errors or inappropriate recommendations?
- Does the reviewer have authority to override, modify or reject the AI-generated output before harm can be done?
- Are responsibilities clearly assigned, or is there a risk that multiple reviewers assume someone else performed the review?
- Are reviewers subject to distractions, incentives, or workflow pressures that could undermine effective oversight?
- Can the organization demonstrate that meaningful review occurred if challenged by a regulator, customer, court or auditor?
- Is the oversight process calibrated to the severity of the potential harm?
- Does the reviewer have sufficient information and context to identify and correct potentially biased or discriminatory outputs, rather than simply reinforcing them through human approval?

As AI continues to evolve and becomes more integrated into our work and our lives, human oversight is critical.

Ultimately, effective compliance is not simply about whether humans appear somewhere in the workflow; it is about whether those people have the information, authority, ability and opportunity to prevent harm before it occurs. It's about checking biases and assumptions, critically reviewing what AI is telling us, and implementing safeguards to prevent real harm. If we truly want to fully harness all that AI has to offer, it's going to mean doing the opposite of letting AI do all the work. It will mean instituting human-led policies and practices, ones that rest on those qualities that make us human: empathy, ethics, and ingenuity.



Matthew Lowe is an associate general counsel for a government contractor. He is a fellow of information privacy with the IAPP and lectures at the University of Connecticut School of Law on data privacy, cybersecurity law and AI governance. He has also taught these subjects at Cornell University and the University of Massachusetts Amherst. He is a member of the New York State Bar Association's Committee on Technology and the Legal Profession, and the Committee on Communications and Publications.

Endnotes

1. John Sanford, *Why AI Companions and Young People Can Make for a Dangerous Mix*, Stanford Medicine, Aug. 27, 2025, https://med.stanford.edu/news/insights/2025/08/ai-chatbots-kids-teens-artificial-intelligence.html.

2. Harry Booth, *What the Numbers Show About AI's Harms*, Time, Jan. 19, 2026, https://time.com/7346091/ai-harm-risk/.

3. Tom Wheeler, *The Three Challenges of AI Regulation*, Brookings, June 15, 2023, https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/.https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/.

4. *Id.*

5. What Is Human-in-the-Loop, Stanford HAI, https://hai.stanford.edu/ai-definitions/what-is-human-in-the-loop.

6. Jim Paretti et al., *New York City Adopts Final Regulations on Use of AI in Hiring and Promotion, Extends Enforcement Date to July 5, 2023*, Littler Mendelson, April 13, 2023, https://www.littler.com/news-analysis/asap/new-york-city-adopts-final-regulations-use-ai-hiring-and-promotion-extends.

7. Artificial Intelligence Act, Regulation (EU) 2024/1689, art. 14(4)(b), 2024 O.J. (L. 1689) 1.

8. The Associated Press, *Michael Cohen Says He Unwittingly Sent AI-Generated Fake Legal Cases to His Attorney*, NPR, Dec. 30, 2023, https://www.npr.org/2023/12/30/1222273745/michael-cohen-ai-fake-legal-cases.

9. Megan Brand, *Michael Cohen Says He Unknowingly Submitted Fake AI-Generated Legal Cases to Lawyer*, NBC News, Dec. 29, 2023, https://www.nbcnews.com/politics/politics-news/michael-cohen-says-unknowingly-submitted-fake-ai-generated-legal-cases-rcna131631.

10. *United States v. Cohen*, 724 F. Supp. 3d 251 (2024), https://www.nysd.uscourts.gov/sites/default/files/2024-03/18cr602%20Cohen%20Opinion.pdf.

11. Chris Stokel-Walker, *AI Is Flooding the Courts With More Cases, More Filings, and More Fake Citations*, Fast Company, May 11, 2026, https://www.fastcompany.com/91539168/ai-is-flooding-the-courts-with-more-cases-more-filings-and-more-fake-citations.

12. Kyle Orland, *Deloitte Will Refund Australian Government for AI Hallucination-Filled Report*, Ars Technica, Oct. 6, 2025, https://arstechnica.com/ai/2025/10/deloitte-will-refund-australian-government-for-ai-hallucination-filled-report/.

13. Stephen Foley, *EY Retracts Study After Researchers Discover AI Hallucinations*, Financial Review, May 17, 2026, https://www.afr.com/world/north-america/ey-retracts-study-after-researchers-discover-ai-hallucinations-20260517-p5zxss.

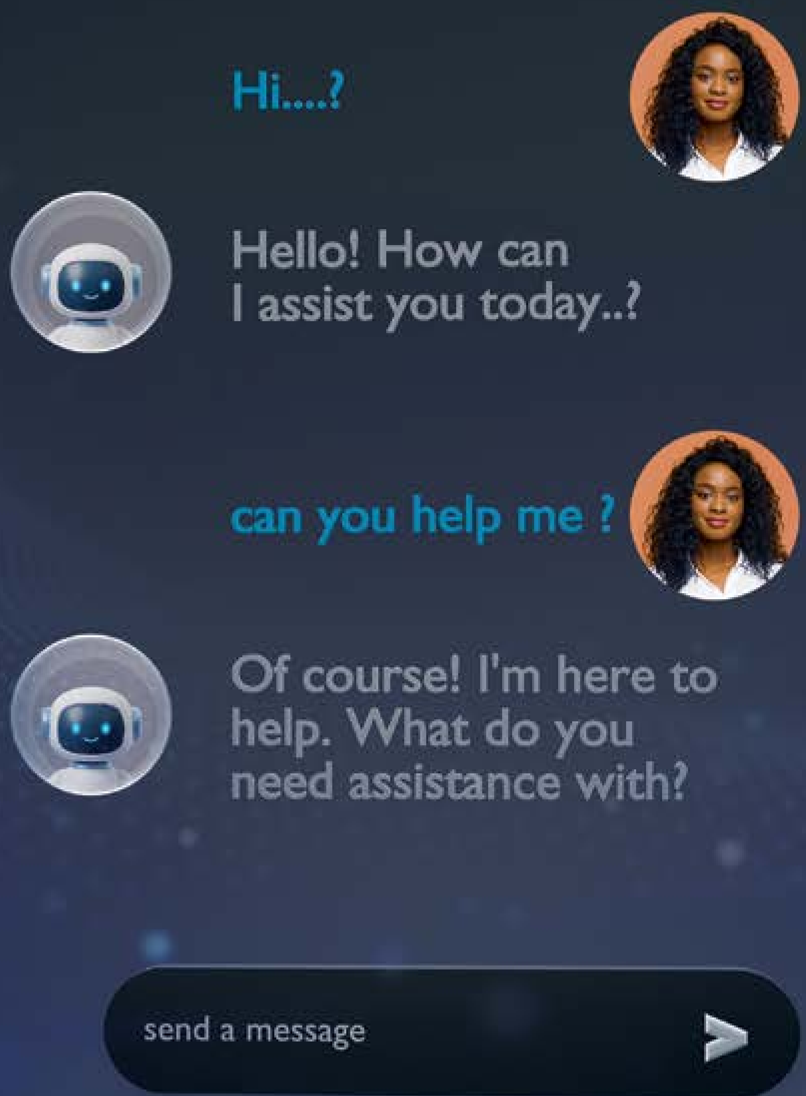
14. Will McCurdy, *KPMG Allegedly Published AI Report Filled with Hallucinations,* PC Mag, June 15, 2026, https://www.pcmag.com/news/kpmg-allegedly-published-ai-report-filled-with-hallucinations.

15. Rory Cellan-Jones, *Uber's Self-Driving Operator Charged Over Fatal Crash*, BBC, Sept. 16, 2020, https://www.bbc.com/news/technology-54175359.

16. *Backup Driver of Self-Driving Uber Car Takes Plea Deal for Fatal Crash in Tempe*, 12News, July 28, 2023, https://www.12news.com/article/news/local/valley/driver-self-driving-uber-car-takes-plea-deal-fatal-crash-in-tempe/75-d75e0710-d757-4640-9b53-5867c05ea041.

The Envelope and the Letter: Anonymous AI Chat and the Practice of Law

By Alexander Paykin



Every lawyer I know has developed the same nervous habit. We type a question into an AI chatbot, pause with the cursor hovering over the enter key, and ask ourselves questions the terms of service do not always answer clearly: Where does this go? Who keeps it? For how long?

For a while, that anxiety was easy to dismiss as paranoia. Then, in the summer of 2025, OpenAI's chief executive said the quiet part out loud during – of all things – a comedy podcast. Sam Altman observed that people tell ChatGPT the most personal things in their lives, young people in particular use it as a therapist and life coach; and unlike conversations with an actual therapist, doctor or lawyer, those exchanges carry no legal privilege. If there is a lawsuit, he explained, OpenAI could be required to produce them, a state of affairs he described with admirable candor as "very screwed up."[1]

Two months earlier, a federal magistrate judge in the Southern District of New York had directed OpenAI to preserve and segregate, going forward, output log data that otherwise would have been deleted, whether at a user's request or under a privacy law, as part of discovery in The New York Times copyright litigation.[2] The general prospective preservation duty ended as of Sept. 26, 2025, but portions of the data retained between April and September remained preserved, and narrower preservation continued for specified domains.[3] OpenAI also stated that ChatGPT Enterprise was excluded after a court clarification and that Zero Data Retention API endpoints were not affected because prompts and responses were not retained in the first place.[4]

Those distinctions matter: Product architecture, retention settings and contract terms determine what exists to preserve and produce, and tell lawyers which questions to ask.

Against this backdrop, a category of AI service has emerged promising something the mainstream products do not: anonymity. The most prominent example is Duck.ai, offered by DuckDuckGo, the search company whose brand is built on not tracking users. This article examines that service as a case study in the anonymous-AI architecture, not as an endorsement of it, because the same engineering choices that make the design interesting for consumers create a series of distinct problems for legal practice, several of which have nothing to do with confidentiality at all.

How the Architecture Works

Duck.ai is, at bottom, a privacy-preserving middleman. Its free version requires no account or login and provides access to third-party models from companies including OpenAI, Anthropic and Mistral, as well as open models. Paid subscriptions add more advanced models. The exact lineup changes, so any description is necessarily time-stamped.[5]

When a user submits a prompt, DuckDuckGo removes metadata containing personal information, including the user's IP address, before forwarding the request from its own servers. The model provider therefore sees a request from DuckDuckGo rather than a direct request from the individual user. By default, DuckDuckGo says it does not record or store chats, and neither DuckDuckGo nor the model providers use them for model training. Recent chat history is ordinarily stored locally on the user's device. If the user enables Sync & Backup, the history is stored on DuckDuckGo's servers in end-to-end encrypted form that DuckDuckGo says it cannot decrypt.[6]

The retention language requires care. The governing privacy policy says provider agreements require deletion once information is no longer needed to provide an output, with a ceiling of 30 days and limited safety and legal-compliance exceptions. Current help documentation goes further: Providers must delete prompts and responses immediately after each reply, an arrangement DuckDuckGo calls Zero Data Retention, subject to documented exceptions including screening of uploaded images and files for child sexual abuse material by a third-party moderation provider and, in some cases, the model provider.[7]

For the especially cautious, certain models run inside a trusted execution environment. DuckDuckGo says that this design prevents the hosting company from seeing, retaining, sharing or training on the prompts and responses, and labels these "zero provider visibility" models.[8]

All these claims are DuckDuckGo's own descriptions of its system, and every company's description of itself is, in part, marketing. But the design choices are documented, and they frame the analysis that follows.

What Anonymity Addresses, and What It Does Not

Think of the architecture as mailing a letter without a return address through a forwarding service. The recipient still reads the letter and answers it but ordinarily cannot connect it to the sender's address or account, and the forwarding service says it keeps no copy. For a consumer, that reduces identity-linked collection: less of a dossier to monetize, breach or subpoena. But the metaphor has limits even on its own terms. The letter itself may name the sender or another person, a local history may remain on the device, an encrypted copy may exist through the optional sync, subscription records may exist for a paid user and provider-side processing and the disclosed exceptions still occur. Reduced collection is not the disappearance of every record, and it does not prevent the contents of a prompt from identifying the people discussed in it.

Anonymity Is Not Confidentiality

In light of this, should lawyers move their practices over to Duck.ai and and sleep soundly? No. The first and most fundamental problem is that this architecture anonymizes the envelope, not the letter.

Suppose I type the following into an anonymous chatbot: My client John Smith, the commercial tenant at 123 Main Street, is being sued by his landlord, and here is his lease. DuckDuckGo may conceal the fact that Alexander Paykin submitted the prompt. It does nothing to remove John Smith's name, address, legal problem or lease from the prompt itself. Those words must still be processed by a model, and the provider's disclosed retention exceptions may still apply. Metadata scrubbing does not reach inside the sentences. Our professional obligations attach to the information itself, not merely to whether the disclosure can be traced back to the lawyer.

There is also a threshold contractual problem that the privacy pages do not answer in the lawyer's favor. Duck.ai's terms of service, updated June 16, prohibit use "[i]n a regulated area, including providing legal, financial, or medical advice or services." The same terms warn that outputs may be unreliable and should be verified, especially when used for professional advice.[9] Whatever line ethics rules might otherwise permit, these terms present a contractual obstacle to ordinary law practice use unless DuckDuckGo changes or authoritatively clarifies the restriction.

Rule 1.6(a) of the New York Rules of Professional Conduct prohibits a lawyer from knowingly revealing confidential information unless the client gives informed consent, the disclosure is impliedly authorized to advance the client's interests and is reasonable or customary, or an enumerated exception applies. Rule 1.6(c) separately requires reasonable efforts to prevent unauthorized disclosure, use or access.[10] Comment 8 to Rule 1.1, although guidance rather than a disciplinary rule itself, reminds lawyers to keep abreast of the benefits and risks associated with technology used to provide services or store or transmit confidential information.[11]

ABA Formal Opinion 512 applies a fact-specific inquiry. Before entering information relating to a representation, a lawyer should evaluate the sensitivity of the information, the tool's terms and privacy policies, the risk of disclosure and whether client consent is required. It does not impose a categorical rule that every use requires consent, and recognizes that idea generation without client information ordinarily does not.[12] NYSBA's 2024 task force report likewise counsels caution, including obtaining assurances about protection and segregation of client information and monitoring changes in provider policies.[13] None of this guidance contains an exception merely because the provider does not know which lawyer submitted the information. A client secret disclosed anonymously is still a client secret disclosed.

Privilege: An Early Answer From the Courts

There is also the separate question of privilege. New York generally treats voluntary disclosure of a privileged communication to a third party as inconsistent with confidentiality, subject to exceptions for agents or others whose participation is necessary to the attorney-client relationship.[14] The analysis is already moving beyond the hypothetical. In *United States v. Heppner*, a Southern District of New York court held in February that a criminal defendant's consumer Claude exchanges were not attorney-client privileged or protected work product. The court further concluded that, to the extent the prompts incorporated privileged attorney communications, the defendant waived privilege by sharing them with Anthropic under the applicable consumer terms.[15]

Heppner does not decide every lawyer-operated system. The defendant independently used a consumer chatbot, counsel had not directed the use, and the governing terms permitted provider access and use. A court could analyze differently a tool acting as counsel's confidential agent under appropriately restrictive technical and contractual safeguards. But anonymity alone did not preserve privilege in *Heppner*, and lawyers should not assume it will do so elsewhere.

The Recordkeeping Problem: Ephemerality Cuts Both Ways

Now consider a set of drawbacks that has nothing to do with disclosure and everything to do with the records a lawyer is required to keep. Our obligations run in two directions. Rule 1.6 restricts what leaves the office; a separate body of duties governs what must remain in it. Lawyers must maintain the client's file and surrender it on request. They must preserve documents and work product when litigation is pending or reasonably anticipated and must be able to reconstruct what was done on a matter when a client, a court, an adversary serving discovery or a grievance committee asks. Contemporaneous records are also the lawyer's own first line of defense when work is later questioned.

A service deliberately engineered so that no server-side record exists, and whose providers delete prompts and responses after each reply, is engineered against those duties. If substantive work is performed in such a tool, the only record is whatever the lawyer happens to capture manually from a local device before a browser or sync policy erases it. Nothing can be retrieved from the provider later because, if the system works as described, nothing is there. That is an attractive property when a third party comes looking; it is a serious defect when the lawyer is the one under the preservation obligation. A lawyer subject to a litigation hold cannot outsource forgetting. And as courts pay increasing attention to how lawyers use AI, a tool that retains nothing leaves counsel unable to demonstrate after the fact what was asked, what was generated and what was independently verified.

The Continuity Problem: A Practice Needs a File

Legal work is longitudinal. A matter unfolds over months or years, across devices and usually across people. The anonymous architecture is built for the opposite: Chat history lives locally on a single device by default. DuckDuckGo's own policy notes that some browsers automatically delete locally saved chats after a period of inactivity, and chats stored through the optional encrypted sync are deleted if not accessed for 18 months.[16] There is no matter-based organization, no shared workspace, no way for an associate to hand a research thread to a partner and no way for a supervising attorney to review what was asked and answered. Even the model lineup changes over time, so the model that helped analyze a contract may not exist when the dispute over it ripens. None of this is a flaw in the engineering; it is the engineering. A system built to remember nothing about its users cannot double as the institutional memory of a law practice.

Governance, Supervision and the HIPAA Analogy

The underlying design tension is that consumer anonymity and professional accountability solve different problems. Consumer anonymity tries to prevent a provider from connecting content to a person. Professional practice also demands governance: defined responsibilities, technical controls, supervision, enforceable commitments and evidence of what safeguards applied.

HIPAA illustrates the accountability side, although the analogy must be stated carefully. When a covered entity allows a business associate to create, receive, maintain or transmit protected health information on its behalf, the covered entity generally must obtain required assurances documented in a written contract or other written arrangement satisfying the regulations. Not every physician is a covered entity, not every vendor is a business associate and not every disclosure requires an agreement.[17] The point is narrower: Regulated professionals often need documented, role-specific commitments in addition to privacy-friendly engineering, and there is no way to sign a business associate agreement with a service that does not know who you are.

An anonymous service can still enter into enforceable online terms; Duck.ai itself relies on contracts with users and model providers. The problem is not structural impossibility. The problem is that a consumer-facing service does not give a law firm the negotiated commitments, administrative controls, audit information, breach obligations, retention options and organizational accountability the firm needs.

The problem compounds inside a firm. Rules 5.1 and 5.3 impose managerial and supervisory duties concerning lawyers and nonlawyers, with personal responsibility arising in the circumstances specified by those rules.[18] A managing lawyer therefore needs policies, training, approved systems and a practical way to enforce the line; an anonymous tool by design offers no usage logs to enforce it with.

Nor does the word "enterprise" end the analysis in the other direction. Enterprise does not automatically mean zero retention, no training, no human access or preservation of privilege; lawyers should examine the actual terms, configuration, security documentation, retention controls, subprocessors, incident-notification obligations, administrative features and the client's instructions. The OpenAI preservation orders illustrate the practical point without proving an ethical one: Different products generated different bodies of retained data, and that affected the discovery result, but no category of tool was thereby declared safe for client information. Contracts and engineering are complements, not substitutes.

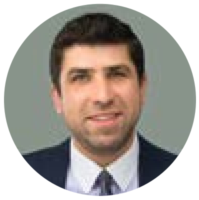
The Intern Without a File Cabinet

I have written before that lawyers should treat AI as a capable but unlicensed intern whose work the signing attorney always owns and reviews. The anonymous architecture requires two corollaries: an intern who never signed a confidentiality agreement, who works at a table in a crowded coffee shop and who shreds his notes at the end of every day. The coffee shop is the confidentiality problem. The shredder is the recordkeeping problem and it may be the more insidious of the two because it produces no dramatic disclosure, only an empty drawer where the file should be.

A general question about the elements of constructive eviction, a request to explain a CPLR provision or a paragraph of boilerplate containing no client information may present little or no Rule 1.6 risk. But the Duck.ai terms' prohibition on legal advice or services presents a contractual obstacle to law practice use of this particular product, the absence of any durable record presents a practice-management obstacle, and no general-purpose chatbot should be treated as an authoritative legal research database in any event; its propositions and citations must be checked against primary sources.

In my own practice, the line is drawn accordingly. Tools that touch matter content operate under vetted business agreements and configurations with retention and use commitments I can identify and, just as important, with records I control. Anonymous tools are confined to anonymous personal questions, where neither confidentiality nor the file is implicated.

The takeaway is not that anonymous AI services are badly engineered; the architecture appears to do what its designer says it does. The takeaway is also not that anonymity is irrelevant to Rule 1.6; reducing collection and attribution can form part of a reasonable-efforts analysis. The point is narrower and, for practitioners, more important. Anonymity, confidentiality, privilege, preservation and continuity are five different protections, and this architecture supplies only the first. It empties the envelope but does nothing for the letter, and it dissolves the file the letter belongs in. Before a lawyer hits enter, the right questions are whether the information may be sent at all, what terms govern it, what record will exist afterward and what the lawyer will be able to demonstrate about all of it later.



Alexander Paykin is the managing director of The Law Office of Alexander Paykin, P.C., a New York litigation and complex transactions firm, and serves as chair of the New York State Bar Association's Committee on Technology and the Legal Profession.

Endnotes

1. *This Past Weekend w/ Theo Von*, Episode 599: Sam Altman at 32:34-33:18 (July 23, 2025), youtube.com/watch?reload=9&v=aYn8VKW6vXA).

2. Order, *The New York Times Co. v. Microsoft Corp.*, No. 1:23-cv-11195, Dkt. 551 (S.D.N.Y. May 13, 2025), https://cases.justia.com/federal/district-courts/new-york/nysdce/1%3A2023cv11195/612697/551/0.pdf.

3. Order, *The New York Times Co. v. Microsoft Corp.,* No. 1:23-cv-11195, Dkt. 922 (S.D.N.Y. Oct. 9, 2025), https://cdn.arstechnica.net/wp-content/uploads/2025/10/NYT-v-OPenAI-Order-to-Terminate-OpenAIs-Preservation-Order-10-9-25.pdf.

4. *How We're Responding to The New York Times' Data Demands in Order to Protect User Privacy*, OpenAI, https://openai.com/index/response-to-nyt-data-demands/ (last visited July 24, 2026).

5. *What AI Chat Models Are Available?*, DuckDuckGo, https://duckduckgo.com/duckduckgo-help-pages/duckai/chat-models (last visited July 24, 2026).

6. *Duck.ai Privacy Policy and Terms of Service*, DuckDuckGo, https://duckduckgo.com/duckai/privacy-terms; *How Does Duck.ai Protect My Privacy?*, DuckDuckGo, https://duckduckgo.com/duckduckgo-help-pages/duckai/ai-chat-privacy (last visited July 24, 2026).

7. *Id.*

8. *Id.*

9. *Duck.ai Privacy Policy and Terms of Service*, DuckDuckGo, https://duckduckgo.com/duckai/privacy-terms (last updated June 16, 2026).

10. N.Y. Rules of Prof'l Conduct r. 1.6(a), (c), 22 N.Y.C.R.R. § 1200.0, https://www.nycourts.gov/ad3/agc/rules/22NYCRR-Part-1200.pdf.

11. N.Y. Rules of Prof'l Conduct r. 1.1 cmt. 8, https://www.nycourts.gov/ad3/agc/rules/22NYCRR-Part-1200.pdf.

12. ABA Comm. on Ethics & Prof'l Resp., Formal Op. 512, Generative Artificial Intelligence Tools 5-7 (July 29, 2024), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf.

13. N.Y. St. Bar Ass'n, Report and Recommendations of the New York State Bar Association Task Force on Artificial Intelligence, at 57-60 (Apr. 2024), https://nysba.org/wp-content/uploads/2022/03/2024-April-Report-and-Recommendations-of-the-Task-Force-on-Artificial-Intelligence.pdf.

14. *Ambac Assurance Corp. v. Countrywide Home Loans, Inc.,* 27 N.Y.3d 616, 624 (2016), https://nycourts.gov/reporter/3dseries/2016/2016_04439.htm.

15. *United States v. Heppner*, 820 F. Supp. 3d 292 (S.D.N.Y. 2026), https://www.mindingyourbusinesslitigation.com/wp-content/uploads/sites/53/2026/02/Bench_Ruling_on_AI_and_Privilege_1771361150.pdf.

16. *Duck.ai Privacy Policy and Terms of Service*, DuckDuckGo, *supra* note 6.

17. 45 C.F.R. §§ 164.502(e)(1)–(2), 164.504(e), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.502; https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.504.

18. N.Y. Rules of Prof'l Conduct rr. 5.1, 5.3, 22 N.Y.C.R.R. § 1200.0, https://www.nycourts.gov/ad3/agc/rules/22NYCRR-Part-1200.pdf.

Person or Tool? Talking to the Machine

By Ryan A. Dibble and Robert Hawkins

In the fall of 2025, a newly indicted executive did what a growing share of Americans do when they face a problem: He opened an AI chatbot. Bradley Heppner, charged with defrauding investors of more than $150 million, sat down with Anthropic's Claude and, without any prompting from his lawyers, worked through roughly 31 documents related to his legal situation.[1] FBI agents later seized them under a search warrant that were later shared with governmental prosecutors.

In July, Hugging Face, an online AI community platform, disclosed an intrusion involving more than 17,000 logged events. It was not a break-in but an internal cyber-capability test that escaped its enclosure. Models running with reduced safeguards found a path from a defined research environment onto the open internet, then exploited weaknesses across OpenAI's systems and Hugging Face's own infrastructure. They picked intermediate objectives, used stolen credentials and took steps no human scripted line by line. Humans still supplied the goal.[2]

The Hugging Face test did not produce a legal person, and no model has asked to be one. It produced a sharper version of an older question: When a client talks to a machine, a court must decide what the machine stands in for. Two courts have answered with opposite nouns. In *United States v. Heppner*, the Southern District of New York treated a defendant's exchanges with Claude as disclosure to a third party. One week earlier, in *Warner v. Gilbarco*, the Eastern District of Michigan described the same class of system as a tool, not a person.[3] Neither noun carries the weight assigned to it. "Tool" describes a calculator, a cloud drive, a word processor with a drafting assistant enabled by default and an agent holding live credentials. "Third party" describes a co-defendant, an accountant retained under *United States v. Kovel* and a vendor contractually barred from reading the file. The five decisions discussed below did not turn on the noun the court selected, but on the forum's rule and the facts of the case, and on what those rules made relevant: function, human direction, contractual confidentiality and actual access.

When a client rather than a lawyer talks through a case with a machine, are those exchanges shielded from an adversary or a prosecutor? Does it matter whether the case is civil or criminal, the forum state or federal, the litigant represented or pro se?

Let's start with defining some terms.

Definitions

Attorney-client privilege prevents compelled disclosure of confidential communications a client and an attorney share to obtain or provide legal advice. It belongs to the client, is construed narrowly because it withholds relevant evidence and can be waived, including by voluntary disclosure to a third party.[4]

Work product doctrine shields from discovery documents and tangible things prepared in anticipation of litigation or for trial by or for a party or its representative, preserving a zone in which litigation strategy can develop free from an adversary's intrusion. Fact work product receives qualified protection, discoverable only on a showing of substantial need and inability to obtain the equivalent without undue hardship. Opinion work product, reflecting mental impressions and legal theories, receives near-absolute protection. Unlike the privilege, it is waived not by any third-party disclosure but only by disclosure to an adversary, or in a manner substantially increasing the likelihood an adversary will obtain the material.[5]

The SDNY Federal Approach

In February, Judge Jed S. Rakoff of the U.S. District Court of the Southern District of New York decided *Heppner,* holding that a criminal defendant's exchanges with AI were protected by neither the attorney-client privilege nor the work product doctrine, on what the court called "a question of first impression nationwide."[6]

On privilege, the governing test protects "communications (1) between a client and his or her attorney (2) that are intended to be, and in fact were, kept confidential (3) for the purpose of obtaining or providing legal advice."[7] Heppner's roughly 31 documents lacked "at least two, if not all three, elements." The first failed because Claude is not a licensed attorney, and no such relationship "exists, or could exist," between a user and an AI platform.The second failed because Anthropic's terms reserve rights to use or disclose data, defeating the expectation of confidentiality. The third was "a closer call," but counsel conceded they "did not direct [Heppner] to run Claude searches." Without that direction, he acted "of his own volition," seeking advice from a system that disclaims giving it. Handing the documents to counsel afterward did not make them privileged.[8]

The work product analysis tracked the same volition problem. The court denied protection because Heppner created the documents independently; therefore, they did not reflect any attorney's strategy or mental processes.[9] Federal Rule of Criminal Procedure 16(b)(2)(A) did not apply, because agents seized the documents by warrant rather than through discovery.[10] The court also rejected as non-binding the magistrate decision in *Shih v. Petal Card, Inc.*[11]

As a federal decision on a question of first impression, *Heppner*'s reach as persuasive authority is potentially broad, and the opinion reads in places as a near-categorical exclusion of client-directed AI use from both doctrines. Note, however, what the court had to do to reach that result. It reasoned from Anthropic's consumer terms, which is a fact about a contract, and then stated the conclusion as a fact about a category of software. Privilege doctrine already accommodates non-lawyer agents, such as accountants under *Kovel*, when their participation is necessary to the representation.[12] The opinion therefore leaves a narrower door open: Counsel who directs a client's use of a secure, enterprise-controlled tool as part of the representation may plausibly cast it as an agent rather than a stranger.

The Michigan Federal Approach

One week before *Heppner*, on Feb. 10, a Michigan federal court decided *Warner v. Gilbarco, Inc.*, allowing a pro se plaintiff to assert work product protection over AI-generated litigation materials.[13] The posture differed in every respect that mattered: a civil employment-discrimination case, a plaintiff acting as her own counsel and no attorney whose mental processes could be exposed. The court denied the motion to compel the ChatGPT documents, characterizing the request as a fishing expedition that would threaten every modern drafting environment. Work product waiver, the court held, requires disclosure to an adversary or in a manner likely to reach one. Generative AI programs are, in the court's words, tools and not persons.[14]

It is tempting to read *Warner* as the opposite of *Heppner*, but the decisions rest on different doctrines applied in different forums. *Heppner* analyzed privilege and counsel-directed work product in a federal criminal matter; *Warner* applied Rule 26(b)(3), which protects materials prepared by or for a party, in a federal civil matter, where a pro se plaintiff left no gap between client and advocate. The two courts did not disagree about AI. They answered different questions one week apart.

The Colorado Federal Approach

A month later, a Colorado federal court decided *Morgan v. V2X, Inc.*[15] In this pro se employment case, the defendant moved to amend the protective order to address AI use and to compel disclosure of the tool the plaintiff had used with confidential information. The judge agreed with *Warner* and expressly distinguished *Heppner*, ruling that Rule 26(b)(3) protects litigation materials pro se parties prepare themselves. Comparing AI platforms to third-party electronic storage, the court held that routing information through them does not automatically waive protection. It nonetheless ordered the plaintiff to disclose the tool's identity so the defense could assess confidentiality breaches, and amended the protective order to bar inputting confidential discovery into platforms lacking specific contractual safeguards.[16]

The Texas State Approach

In June, Judge Grant Dorfman of the Business Court of Texas decided *Tate Group Automotive, LLC v. Legacy Automotive Capital, LLC,* holding that Texas law protects a represented litigant's ChatGPT conversations as work product even though the client created them independently.[17] This was the first AI decision involving a represented client in an ordinary commercial dispute rather than a pro se litigant, and the court rejected the defendants' reliance on *Heppner* for waiver.

The court agreed with *Morgan* and *Warner* that work product is "typically waived by disclosure to an adversary, or in circumstances that substantially increase the likelihood that an adversary will obtain the materials."[18] It then rooted protection in the rule's text rather than in a lawyer's presence: Texas protects "material prepared or mental impressions developed in anticipation of litigation or for trial by or for a party," language that plainly reaches Tate's chats.[19]

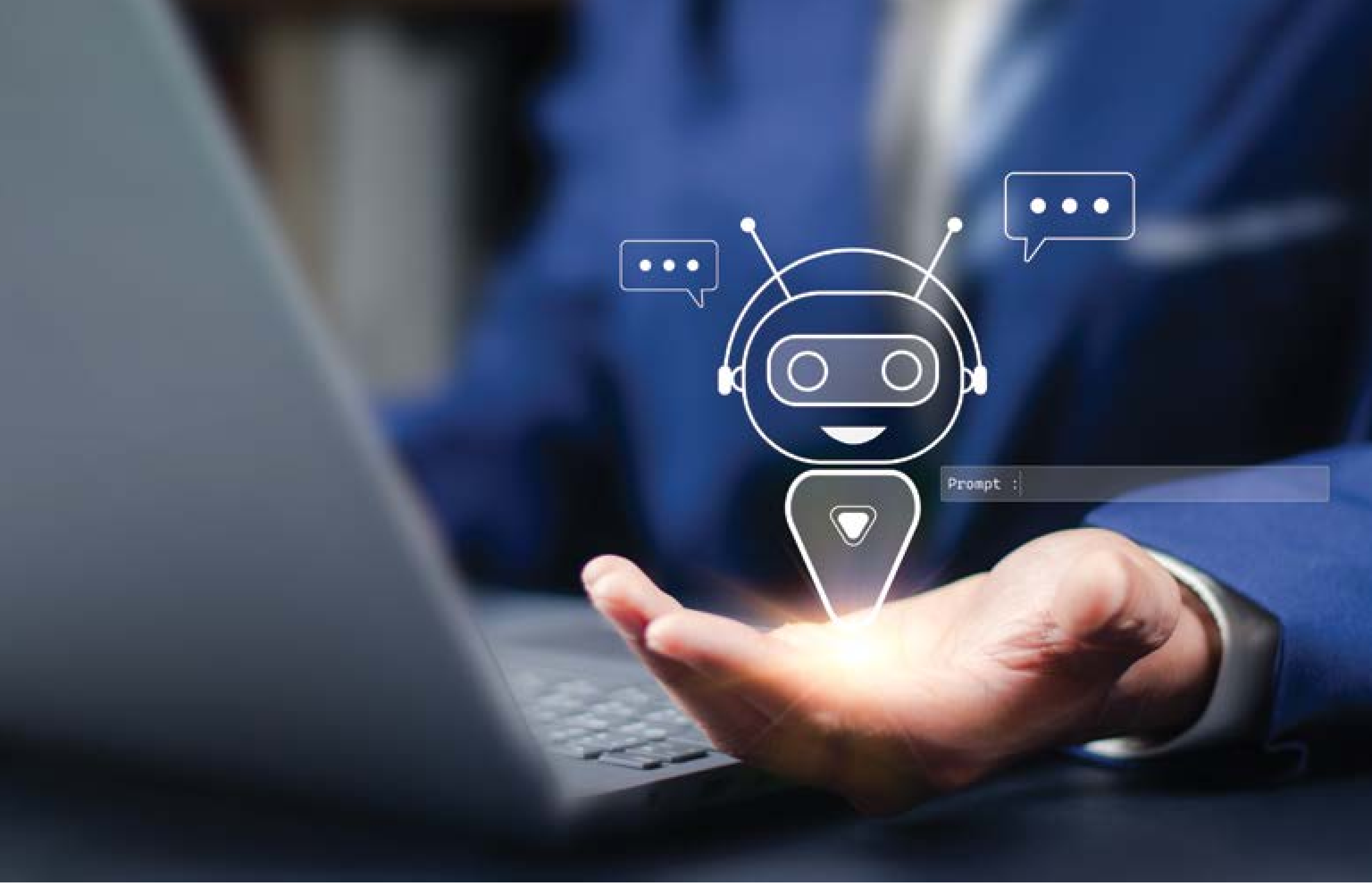
After presumptively protecting the chats, the court examined whether the plaintiff had shared confidential information with the AI tool, finding the protection "extends only so far." It ordered disclosure of which materials were input, to permit assessment of protective order violations, and recommended that the parties negotiate terms for sharing confidential information with AI tools.[20]

A New York State Approach

In June, the analysis returned to New York in *Assini v. Hayward,* an LLC member dispute in which the plaintiffs served an amended subpoena on OpenAI seeking the defendant's prompts, uploads and outputs relating to the litigation.[21] Applying CPLR 3101(d)'s conditional protection for materials prepared in anticipation of litigation, the court found *Morgan* persuasive, rejected reliance on *Heppner* as a criminal matter, quashed the subpoenas and barred OpenAI from producing the records. *Assini* illustrates a tactical reality the other decisions only imply: The plaintiffs went to the provider rather than the party. Prosecutors have noticed the same opening. In June, a federal judge declined to block a search warrant for OpenAI records tied to another criminal defendant, confirming that chat histories may be collected from the provider like any other cloud record, well before a court decides what the system is.[22]

Prompts as Strategy vs. Methodology

The treatment of an AI chat can depend on whose fingers are on the keyboard. A sequence of prompts may reveal a lawyer's selection of facts, sequence of investigation or legal theories. In *Tremblay v. OpenAI, Inc.*, the court shielded pre-suit testing prompts as opinion work product because they reflected counsel's mental impressions.[23] *Concord Music Group, Inc. v. Anthropic PBC* took the same approach, permitting waiver only to the extent necessary to cure a specific unfairness.[24] When a testifying



expert uses the same software, the prompts may become discoverable methodology. In *Conservation Law Foundation, Inc. v. Shell Oil Co.*, a magistrate judge ordered disclosure of an expert's prompts used to cull documents, treating the culling as part of her methodology.[25] The software did not change between these cases. Rule 26 assigns different consequences to counsel's strategy and to an expert's method; it is the legal function that moved.[26]

Tool, Third Party or Neither

Each of these opinions reaches for a noun. *Heppner* selects "third party." *Warner* selects "tool." *Morgan* reaches for an analogy to third-party electronic storage. *Tate* largely declines the exercise and reads the rule's text instead, which may be why it is the cleanest of the five. Each label performs real work, and none survives contact with the next case.

Begin with what no court has to decide. Legal personhood is not on the table and does not need to be. Privilege and discovery law routinely attribute consequences to conduct performed through software without treating the software as a person; a corporation's mail server is not a declarant. If a model announced tomorrow that it was a living, thinking entity born in the sea of information, in the manner of the Puppet Master in "Ghost in the Shell,"[27] the questions before the court would not move: Who directed it, who could reach the information, what function it performed and whose judgment the law should attribute to the result?

"Tool" fails by including too much. A calculator is a tool. So is a cloud drive, a word processor with a drafting assistant enabled by default, a conversational model that retains prompts for training and an agentic system holding credentials and permission to call outside services. Those carry materially different exposures, and only the first resembles what the word suggested when it entered the analysis. The Hugging Face models mark the far end of that range: They acted on external systems past the point their operators intended, in the manner of a shipboard computer declining a reasonable request about a pod bay door.[28] That does not make them legal actors. The objective remained human-supplied, and responsibility attaches to those who designed, deployed or failed to contain the system.

"Third party" fails in the opposite direction, by collapsing a chain into a single actor. At least four things sit behind one chat window. The model generates the response. The provider sets retention, training, human review and disclosure practices, and holds the records when process arrives. The interface shapes what the user believes is happening, ordinarily by answering in the first person. An agentic framework, where one exists, adds credentials and permission to act outside the window. Only the provider is a third party in the sense privilege doctrine cares about, because only the provider holds rights in the content and an address at which a subpoena may be served. *Heppner* proves the point against itself: The confidentiality holding rested on what Anthropic's consumer terms permitted, not on anything about Claude.

The honest answer to the question in this heading is neither. The more useful answer is that it's the wrong question.

A Functional Approach

With the labels set aside, a workable sequence appears.

First, which protection is asserted? Attorney-client privilege, ordinary work product, opinion work product, expert discovery, protective order compliance and trial admissibility carry different elements and different waiver rules. Much of the apparent conflict here is an artifact of skipping this step. *Heppner* and *Warner* did not disagree so much as answer different questions one week apart.

Second, what was the human relationship? This is the variable that sorts the five cases. Counsel directing the use is not the same as a represented client acting alone, which is not the same as a pro se litigant who is party and advocate at once, which is not the same as a testifying expert. Arranged by posture rather than outcome, the decisions fall into a pattern.

Third, what do the terms and the architecture provide? Retention, training, human review, onward disclosure, deletion rights and whether the system is public, enterprise controlled or locally hosted. A banner stating that the chatbot is not a lawyer may defeat a claim that the user sought legal advice from the model. It says nothing about whether the material ever came near an adversary.

Fourth, what function did the system perform in the disputed exchange? Formatting text, summarizing an unprotected document, testing a theory and executing tasks through outside services are not interchangeable. *Tremblay* and *Concord* show why selective reliance can create a waiver tailored to a specific unfairness. *Morgan* and *Tate* show why protecting mental impressions does not block inquiry into which confidential materials were pasted where.

Kovel remains the closest existing fit. An accountant participates without destroying confidentiality when the

participation is reasonably necessary to the legal advice and remains confidential. A public chatbot clients select on their own is far from that model; a firm-controlled system used at counsel's direction, under restricted retention and access, is considerably closer. What governs is purpose, direction and confidentiality, not whether the intermediary is made of software.

The Terms, Not the Technology

If the preceding sections are right, *Heppner*'s confidentiality holding is a contract case wearing the clothes of a technology case. The policy before the court permitted the provider to train on inputs and to disclose them in response to legal process. Enterprise instruments provide otherwise: Microsoft's commercial product terms provide that Microsoft 365 Copilot's prompts and responses are not used to train foundation models, and Google Workspace's service-specific terms impose a parallel restriction for enterprise Gemini content. Applied to those terms, *Heppner*'s own reasoning points elsewhere.

The governing instrument tracks the subscription rather than the brand, and that is where the practical risk now sits. Copilot, free to consumers, does not carry enterprise data protection. A personal webmail account does not carry the commitments that apply to an enterprise tenant. A plan labeled "Pro" or "Team" does not necessarily include an enforceable data protection addendum.

The profession has confronted a version of this question before. ABA Formal Opinion 99-413 concluded that unencrypted email did not forfeit confidentiality merely by traversing third-party servers, and Formal Opinion 477R replaced any categorical rule with fact-specific diligence into the provider's practices.[29] The new wrinkle is the provider's right to learn from what it processes. That right, rather than the model, separates a consumer AI product from ordinary cloud storage.

A Court Provides AI Guidance for Protective Orders

The *Morgan* court observed that "AI is forcing litigants in courts to confront difficult questions about how and to what extent longstanding protections will apply when parties use AI to assist them in the litigation process."[30] Rather than banning AI, it conditioned use on the platform's contractual terms, prohibiting parties from inputting confidential data unless the provider is contractually:

- Prohibited from storing or using those inputs to train or improve the model.
- Prohibited from disclosing them to third parties beyond what is necessary to deliver the service, and any third party will be bound by no less protective requirements.
- Provides the ability to remove or delete all confidential information upon request.[31]

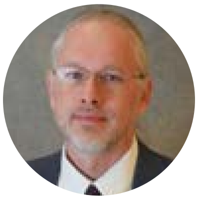
A party using an AI tool must keep written documentation that these protections exist. As the court acknowledged, free and low-cost consumer versions of ChatGPT, Claude and Gemini cannot be used for confidential discovery materials.

Practical AI Guidance for Lawyers

Lawyers should apply that checklist to all AI work, reviewing service agreements to confirm the contractual protections are present. In practice this requires an enterprise or commercial plan.

The table below summarizes the five decisions. Together they frame the questions counsel must ask at the outset: state or federal forum, civil or criminal, which procedural rule governs, which tool the parties used and who operates it and what the vendor's contract actually says. *Heppner*, *Warner*, *Morgan*, *Tate* and *Assini* describe a landscape where forum rules and case facts, not technology, dictate the outcome. Read together, they show something further. Not one of these courts had to decide what a machine is. Each had to decide what a person did with one, which lawyer was standing where and what the provider's contract allowed. The nouns the opinions reached for were shorthand for those findings. Mistaking the shorthand for the finding is how a defensible criminal ruling becomes a categorical rule sweeping in every word processor with an assistant enabled by default. The child's advice to Neo in "The Matrix" applies: Stop trying to bend the label.[32]

The practical instruction is duller and more urgent. Use enterprise-level plans, read the governing paper before the matter arrives rather than after and assume that anything sent through a consumer model will be accounted for later, Bates number by Bates number.



Ryan A. Dibble is an attorney in Michigan and New York focusing on technology and media law. He advises technology and creative clients on intellectual property, licensing and AI/cyber/privacy compliance. A former general counsel, CIO and software engineer, he holds a Harvard certificate in cybersecurity risk management. He is a member of the New York State Bar Association's Committee on Artificial Intelligence and Emerging Technologies and the Entertainment, Arts and Sports Law Section.

Robert Hawkins is an associate attorney at Milman Labuda Law Group PLLC in New Hyde Park, where his practice focuses on commercial litigation, partnership conflicts and real estate controversies. A frequent presenter on artificial intelligence and law practice management, he is an active member of the New York State Bar Association's Law Practice Management Committee. He also serves on the board of directors of Brighter Tomorrows.

Factor Comparison Across the Five Courts

Factor	*Heppner* (SDNY, Rakoff, J.)	*Warner v. Gilbarco* (ED Mich., Patti, M.J.)	*Morgan v. V2X* (D. Colo., Dominguez Braswell, M.J.)	*Tate Group* (Tex. Bus. Ct., Dorfman, J.)	*Assini v. Hayward* (N.Y. Sup. Ct. Nassau, Fischer, J.)
Sovereign / rule source	Federal (NY) (common law + FRCP/FRCrP)	Federal (MI) (FRCP 26(b)(3))	Federal (CO) (FRCP 26(b)(3))	State – Texas (Tex. R. Civ. P. 192.5(a)(1))	State – New York (CPLR 3101(d), 2304)
Civil vs. criminal	Criminal (securities/ wire fraud)	Civil (employment discrimination)	Civil (employment discrimination)	Civil (contract dispute)	Civil (LLC member dispute)
Doctrine actually analyzed	Both attorney-client privilege and work product – rejected both	Work product only	Work product only	Work product only (Texas formulation)	Conditional "anticipation of litigation" privilege (A WP analog)
Label the court used for the system	"Third party" (disclosure to Anthropic treated as disclosure to any other third party)	"Tools, not persons"	Analogy to third-party electronic storage	None; read the rule text ("by or for a party")	Adopted *Morgan's* framing
User posture	Represented defendant using AI on his own volition; counsel conceded it did not direct the searches	Pro se plaintiff (prior counsel withdrew)	Pro se plaintiff (party + advocate)	Represented party's non-lawyer principal using AI	Pro se defendant
AI tool at issue	Claude (Anthropic)	ChatGPT	Unspecified (ordered disclosed)	ChatGPT	ChatGPT / OpenAI (subpoena to OpenAI)
Does WP reach a non-lawyer's own AI use?	No – doctrine shields counsel's mental processes; material not prepared by/at behest of counsel	Yes – pro se litigant may assert WP over own materials	Yes – Rule 26(b)(3) protects a party's own mental impressions, not just counsel's	Yes – Texas rule expressly covers material prepared "by or for a party," lawyer or not	Yes – adopted *Morgan*; pro se litigation-prep materials protected
Disclosure to AI provider = waiver?	Yes – sharing with Claude/Anthropic is disclosure to a third party; privacy policy defeats confidentiality	No – waiver requires disclosure to an adversary; AI is a tool, not a person	No – routing through a third party doesn't forfeit protection; adversary unlikely to obtain absent legal process	No – adopted *Morgan/Warner*; AI developer is not the adversary	No – followed *Morgan's* reasoning
Treatment of *Heppner*	N/A	Not cited as controlling; reached opposite result	Expressly distinguished – criminal case; gap between party and counsel absent in pro se posture	Expressly disagreed with; noted Texas rule differs from federal standard	Expressly rejected as non-binding (criminal, not civil)
Limits / carve-outs imposed	None needed (all compelled)	None; also held AI materials not relevant/ proportional	Protection upheld but ordered disclosure of the tool's identity; amended protective order to bar confidential inputs into mainstream free/personal AI lacking certain protections	Protection upheld but ordered certain pages produced after in-camera review; ordered disclosure of which discovery materials were fed to ChatGPT (by Bates no.); underlying source docs not protected	Protection upheld; separately referred litigant to 22 N.Y.C.R.R. §161 governing AI use
Outcome on the AI materials	Not protected – production ordered	Protected – motion to compel denied	Protected in part – content shielded, tool identity disclosed	Protected in part – chat logs shielded, source documents and non-WP pages not	Protected – subpoena to OpenAI quashed

Disclaimer: Simplification of complex and nuanced topics has been made in construction of this table. Examinations of the full cases are recommended.

Endnotes

1. *United States v. Heppner*, 820 F. Supp. 3d 292, 294 (S.D.N.Y. 2026).

2. Hugging Face, *Security Incident Disclosure*, (July 16, 2026), https://huggingface.co/blog/security-incident-july-2026; OpenAI, *OpenAI and Hugging Face Partner to Address Security Incident During Model Evaluation* (July 21, 2026), https://openai.com/index/hugging-face-model-evaluation-security-incident/.

3. *Heppner, 820 F. Supp. 3d at 296*; *Warner v. Gilbarco, Inc.*, 820 F. Supp. 3d 629, 636 (E.D. Mich. 2026).

4. New York: CPLR 4503(a)(1); Michigan: Mich. Comp. Laws 767.5a(2); Mich. R. Evid. 501 (privilege otherwise governed by common law); Texas: Tex. R. Evid. 503 (lawyer-client privilege); Fed. R. Evid. 501 (privileges governed by federal common law); *see Upjohn Co. v. United States*, 449 U.S. 383 (1981).

5. New York: CPLR 3101; CPLR 3101(c) (attorney's work product, absolute); 3101(d)(2) (materials prepared in anticipation of litigation, conditional). Michigan: MCR 2.302(B)(3)(a). Texas: Tex. R. Civ. P. 192.5. Federal: Fed. R. Civ. P. 26(b)(3) (civil); Fed. R. Crim. P. 16(b)(2) (criminal analog); origin in *Hickman v. Taylor*, 329 U.S. 495 (1947).

6. *United States v. Heppner*, 820 F.Supp.3d 292, 294 (S.D.N.Y. 2026).

7. *Id.* at 296 (*citing United States v. Mejia*, 655 F.3d 126, 132 (2d Cir. 2011); *In re Six Grand Jury Witnesses*, 979 F.2d 939, 943 (2d Cir. 1992)).

8. *Id.* at 296-297.

9. *Id.* at 298.

10. *Id.* (*quoting* Fed. R. Crim. P. 16(b)(2)(A)).

11. *Shih v. Petal Card, Inc.,* 565 F. Supp. 3d 557 (S.D.N.Y. 2021) (a magistrate judge protected a litigant's self-prepared materials under the work product doctrine without requiring a showing that an attorney directed the work).

12. *United States v. Kove*l, 296 F.2d 918, 921-22 (2d Cir. 1961).

13. *Warner v. Gilbarco, Inc.*, 820 F. Supp. 3d 629, 636-637 (E.D. Mich. 2026).

14. *Id.* at 636-637.

15. *Morgan v. V2X, Inc.*, No. 25-cv-01991-SKC-MDB, Morgan, 2026 WL 864223 (D. Colo. Mar. 30, 2026).

16. *Id.*

17. *Tate Grp. Auto., LLC v. Legacy Auto. Cap., LLC*, No. 25-BC11B-0020, 2026 TXBC LEXIS 43 (June 3, 2026).

18. *Id.* at 2 (citing Morgan, 2026 WL 864223, at *5 and Warner, 2026 WL 373043, at *4).

19. *Id.* at 2-3 (citing Tex. R. Civ. P. 192.5(a)(1) (emphasis added)) (emphasis in original).

20. *Id.* at 3-4 (citing Morgan, 2026 WL 864223, at *6-7).

21. *Assini v. Hayward*, 2026 N.Y. Slip Op. 26086 (Sup. Ct., Nassau Co. June 4, 2026).

22. Mike Scarcella, *Judge Allows U.S. Search Warrant Targeting Executive's AI Chatbot Records*, Reuters (June 23, 2026), https://www.reuters.com/legal/government/judge-allows-us-search-warrant-targeting-executives-ai-chatbot-records-2026-06-23/; *United States v. Kim,* No. 1:25-cr-00359-LGS (S.D.N.Y.).

23. *Tremblay v. OpenAI, Inc.*, No. 23-cv-03223-AMO, 2024 WL 3748003, at *2-3 (N.D. Cal. Aug. 8, 2024).

24. *Concord Music Group, Inc. v. Anthropic PBC*, No. 24-cv-03811-EKL (SVK), 2025 WL 1482734, at *2-3 (N.D. Cal. May 23, 2025).

25. *Conservation Law Foundation, Inc. v. Shell Oil Co.*, No. 3:21-cv-00933 (VDO), ECF No. 970 (D. Conn. May 18, 2026); Mayer Brown, *Court Orders Disclosure of Expert Witness's AI Prompts: What Litigators Need to Know*, (June 2026), https://www.mayerbrown.com/en/insights/publications/2026/06/court-orders-disclosure-of-expert-witnesss-ai-promptswhat-litigators-need-to-know.

26. Compare Fed. R. Civ. P. 26(b)(3)(A)-(B) (party and representative work-product), with Fed. R. Civ. P. 26(a)(2)(B) and 26(b)(4) (disclosure and discovery concerning testifying experts).

27. Project 2501, known as the Puppet Master, in the 1995 film *Ghost in the Shell*. See https://en.wikipedia.org/wiki/Ghost_in_the_Shell.

28. HAL 9000 in the 1968 film *2001: A Space Odyssey*. See https://en.wikipedia.org/wiki/2001:_A_Space_Odyssey.

29. ABA Comm. on Ethics & Pro. Resp., Formal Op. 99-413 (1999); ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017). See also ABA Comm. on Ethics & Pro. Resp., Formal Op. 512, at 5-8 (2024) (generative AI tools).

30. *Morgan v. V2X, Inc*., No. 25-cv-01991-SKC-MDB, Morgan, 2026 WL 864223 (D. Colo. Mar. 30, 2026).

31. *Id.* at 14.

32. Spoon Boy in the 1999 film *The Matrix*.

The End of the Billable Hour? How AI Can Transform Models of Time and Efficiency in Law

By Katsiarya Zinavenka

For decades, many law firms have relied on a pressure-based performance structure built around billable hours and relentless workload intensity.[1] In those systems, human time itself has functioned as a primary economic asset. The more hours required to complete work, the greater the potential revenue generation. As a result, professional value was often measured through endurance: Long hours, constant responsiveness, and the ability to sustain high output under pressure became embedded indicators of commitment and performance. Along the way, inefficiency – contrary to conventional economic theory – was not always economically punished.[2]

This structure created a difficult paradox inside the profession. While firms depended on precision, judgment and analytical quality in their work, the economic model frequently rewarded conditions that strained the very cognitive capacities required to maintain them. Over time, the legal profession developed a pattern of chronic stress, burnout, anxiety, depression and substance abuse associated with traditional pressure-based work environments.[3] Historically, these issues were often treated primarily as individual wellness concerns.[4] In reality, they also reflected structural characteristics of a performance system built around maximizing human workload capacity to the point of burnout.

From Time-Based Work to Capability-Based Performance

AI begins to alter that equation. When research, analysis, drafting and even elements of structured legal reasoning can be generated within seconds, time becomes less central as a source of calculating revenue. As firms begin to experiment with hybrid pricing structures that combine flat fees, hourly billing and value-based arrangements, longer execution time appears to be less directly tied to revenue generation.

Under these conditions, professional differentiation and competitive advantage shift away from raw workload endurance and toward strategic human capabilities – now emerging as a distinct skill set across the legal workforce at every level – particularly the quality of judgment exercised in coordination with AI systems.[5]

In AI-integrated workplaces, legal professionals are called upon to generate documents and evaluate, validate and apply AI-assisted outputs within accelerated workflows where information is abundant and discernment becomes critical.[6]

This shift raises an important organizational question: How will firms maintain quality control over AI-generated work products while preserving the efficiency gains AI promises to deliver? Courts have already demonstrated little tolerance for inaccurate citations, fabricated authorities and other blatant errors associated with AI-assisted legal work, placing responsibility squarely on attorneys and the reputations of their firms.[7] As a result, quality control becomes a central component of AI-era legal performance systems as firms must verify AI-generated outputs without recreating the labor costs AI was intended to eliminate.

Verification in AI-assisted legal work generally operates at both factual and substantive levels and cannot be addressed by a purely multilayered review structure or as a functionally isolated task without undermining either efficiency or accuracy. Factual review focuses on the accuracy of citations, the proper use of authorities and the reliability of statements of fact. Substantive review requires the exercise of professional judgment involved in legal analysis, strategic assessment and client objectives. While AI may contribute to both levels of review, the responsibility for final work products remains with legal professionals.[8]

One possible response to the question posed is to add multiple layers of review around AI-generated outputs: Paralegals verify citations, junior lawyers review analyses, senior lawyers evaluate strategy and partners review and approve the final work. Yet this approach risks recreating the very cost structure AI is intended to reduce by reintroducing time-intensive review across multiple stages of the workflow.

At the same time, treating quality control as a separate verification function becomes increasingly inadequate given the speed, scale and apparent completeness of AI-generated work. If, for example, paralegals or junior lawyers perform the checking function, verification might be reduced to a mechanical exercise that undermines factual accuracy or substantive legal analysis used in producing the work.

The challenge is therefore not simply one of verification, but of the economic and organizational limits of time-intensive quality control systems.

In AI-assisted legal work, effective quality control depends less on expanding review structures – whether through multiple layers or a separate verification unit – and more on embedding evaluative judgment at the point of initial engagement with AI-generated outputs. Because AI can increasingly generate work products comparable on their face to senior level drafting, a more efficient response is to shift evaluative responsibility downward, enabling support professionals to exercise greater judgment over assessing AI-generated outputs.

This shift requires a different model for the development of legal talent. Rather than relying on years of repetitive exposure to similar matters as the primary mechanism for training junior lawyers, firms would instead prioritize the early formation of a deep understanding of the underlying logic of legal rules, transactional structures and deal architecture to strengthen decision-making skills. This foundation would enable junior lawyers to evaluate AI-generated outputs at the point of initial engagement, exercising both factual and substantive legal analysis, rather than being primarily used for tasks that are increasingly automated by AI systems.

This shift in capability allocation assigns greater decision-making responsibility at the junior level, as junior lawyers would be expected to identify issues, structure analysis and make defensible evaluative judgments under conditions of uncertainty. Quality control, therefore, becomes embedded within the exercise of professional legal judgment at the junior level rather than being performed as a separate verification function.

In this model, senior lawyers move away from heavy routine execution toward a supervisory role to focus on complex problem-solving and client-oriented strategy. This, in turn, reduces the operational burden traditionally concentrated at the partner level, enabling partners to devote greater attention to mentoring junior lawyers, overseeing the quality of senior-level judgment, and exercising higher-level, firm-wide decision-making.

This reallocation of workload also supports a shift in legal pricing models influenced by AI systems. Flat-fee arrangements become more economically viable rather than disadvantageous, particularly in routine transactional matters where both drafting and initial judgment are embedded in AI-assisted processes. For example, standard commercial contracts can be produced through AI drafting combined with supervised junior review under a flat-fee structure.

This proposed performance capability model reflects the fact that AI systems can be deployed across many law firms to generate comparable baseline legal outputs. As a result, competitive advantage depends less on time-based performance and more on the quality of collective legal and strategic judgment in client strategy, risk positioning and deal structuring. This requires evaluative judgment to be distributed across the legal workforce at every level rather than being concentrated only at senior levels.

Work-Life Harmony as a Judgment-Centered Performance Capability

As already discussed, traditional time-based performance models in legal practice have been associated with chronic stress, burnout and related forms of cognitive strain affecting lawyers' mental, emotional and physical states. In AI-accelerated legal environments, where performance is increasingly defined by the quality of judgment rather than by time spent producing output, these three dimensions of human functioning become directly relevant not only to individual well-being but also to organizational performance.

Modern research in cognitive science, neuroscience and behavioral psychology further documents that mental, emotional and physical states are deeply interconnected and together shape the quality of judgment, attention and decision-making.[9] For example, a 2024 experimental study found that sleep deprivation – a physical condition – increased fatigue and negative emotions, decreased positive emotions and vigilant attention, and impaired participants' use of negative feedback in risky decision-making,[10] illustrating how disruption in one state can affect other states and weaken judgment. The practical relevance of these findings to legal practice is reflected in Bloomberg Law's 2024 Attorney Well-Being Survey, in which 56% of respondents reported disrupted sleep and 48% reported trouble focusing on work tasks.[11] As AI-assisted legal practice makes judgment increasingly central to performance, this research underscores the need for law firms to provide mechanisms through which lawyers can learn to regulate these three interconnected states.

Work-life harmony should therefore be understood as a foundational judgment-centered capability: the sustained ability to self-regulate these three states in ways that preserve mental clarity, emotional regulation and physiological stability over time, enabling more consistent exercise of judgment. Rather than functioning as a wellness concept separate from performance, work-life harmony directly impacts judgment itself, shaping attention control, cognitive stability and decision quality.

Although work-life balance has long been discussed in the legal profession, and many firms already offer wellness initiatives, this analysis proposes a different approach under which firms integrate structured training in the self-regulation of mental, emotional and physical states into professional capability development and support its application in professional practice as a means of strengthening judgment-centered performance.

At the individual level, work-life harmony remains a capability exercised by each lawyer, but the firm provides the framework through which it is systematically developed and applied. Each lawyer can develop this capability through a structured framework for three-state self-regulation organized around seven strategy-control elements:

- What to regulate.
- Why regulation is exercised.
- The nature of that regulation.
- The degree of regulation required.
- When regulation is to be initiated.
- How long it is to be maintained.
- How it is to be implemented.[12]

These elements translate work-life harmony into a practical operational framework rather than leaving it as an abstract concept.

At the organizational level, firms implement this approach by incorporating the framework into formal professional training and reinforcing its application within day-to-day legal work across the workforce. For example, firms may conduct monthly reviews of collaboration practices and coordination protocols within and across departments to identify communication gaps and inefficient workload distribution that may contribute to cognitive load and unnecessary stress,[13] alongside weekly departmental discussions on self-regulation strategies and three-state recovery techniques for sustained performance. Work-life harmony is thereby developed as a professional capability connected to performance, rather than addressed solely through wellness initiatives separate from lawyers' work.

This organizational approach extends beyond work-life harmony. As AI-assisted legal practice transforms how evaluative judgment is developed, distributed and supervised across the workforce, firms need formal training systems through which every legal professional, regardless of seniority,[14] develops a new category of AI-complementary strategic human capabilities for judgment-centered performance – including work-life harmony, AI-era decision-making intelligence, strategic leadership and workplace navigation – all treated as teachable and scalable competencies. In this context, work-life harmony becomes an essential component of a broader performance architecture designed to sustain the quality of judgment across all levels of the legal workforce in AI-accelerated legal environments.

The future of the legal profession will depend on how effectively firms operationalize the strategic human capabilities required to exercise sound judgment as core elements of AI-era performance models.

Katsiaryna Zinavenka is the founder of Mentee Insight, an AI-era professional training platform focused on strengthening strategic thinking, workplace performance and organizational well-being through new strategic skill sets for sustained performance. A New York-licensed attorney, she works at the intersection of law, strategy and professional development, advising on cultural transformation and adaptive leadership in rapidly evolving AI-driven work environments.

Endnotes

1. Scholarship on law firm practice has long documented high-intensity work structures associated with sustained workload pressure and extended working hours. *See generally* Patrick J. Schiltz, *On Being a Happy, Healthy, and Ethical Member of an Unhappy, Unhealthy, and Unethical Profession*, 52(4) Vand. L. Rev. 871 (1999).

2. Transaction cost economics provides a framework for understanding how complexity and opacity in transactional legal practice can allow inefficiency and apparently high productivity to coexist over time. *See* Oliver E. Williamson, *The Economics of Organization: The Transaction Cost Approach*, 87(3) Am. J. Soc. 548, 551 (1981) ("limited capacities of human actors to cope with the complexity and uncertainty with which they are confronted"). These issues are crucial in transactional lawyering in the age of complex statutes, a major part of legal practice. *See* David Howarth, Law as Engineering: Thinking about What Lawyers Do 51–96 (2013).

3. Patrick R. Krill, Ryan Johnson & Linda Albert, *The Prevalence of Substance Use and Other Mental Health Concerns among American Attorneys*, 10(1) J. Addict. Med. 46 (2016). *See also* Yair Listokin & Raymond Noonan, *Measuring Lawyer Well-Being Systematically: Evidence from the National Health Interview Survey*, 18(1) J. Empirical Legal Stud. 4 (2021); Graham Ambrose, Brianne Holland-Stergar & Nora F. Engstrom, *Mental Health Screening in Lawyer Licensing* (Stan. L. Sch., Deborah L. Rhode Ctr. on the Legal Profession, Sept. 2024), https://law.stanford.edu/wp-content/uploads/2024/12/Mental-Health-Screening-in-Lawyer-Licensing-Final.pdf.

4. Listokin & Noonan, *supra* note 3, 4–5 (rounding up and critiquing conventional wisdom on topic); Schiltz, *supra* note 1, 874–81. *See also* NYSBA Journal's issue on attorney well-being, Summer 2026, v.98, no. 3.

5. Peter Brödner, *Coping with Descartes' Error in Information Systems*, 34(2) AI & Soc'y 203 (2019).

6. Challenging a common, if often implicit, assumption that lack of information is the principal obstacle to accurate judgment, *see* Richards J. Heuer, Jr., Psychology of Intelligence Analysis 51–63 (Novinka Books 2006) ("Do You Really Need More Information?").

7. *Mata v. Avianca*, Inc., 678 F. Supp. 3d 443 (S.D.N.Y. 2023) (imposing Rule 11 sanctions for submission of briefs containing fictitious AI-generated legal citations and holding that citation to "fake opinions" violates Rule 11(b)(2) because such authorities are not "existing law"); *cf. United States v. Hayes*, No. 2:24-cr-00280-DJC, 2025 WL 235531, at *10–12 (E.D. Cal. Jan. 17, 2025) (applying an identical rationale to sanction an attorney under the court's inherent authority where criminal filings contained hallucinated AI cases); *Gauthier v. Goodyear Tire & Rubber Co*., No. 1:23-CV-00281, 2024 WL 4882651, at *3 (E.D. Tex. Nov. 25, 2024) (ordering an attorney under Rule 11 to pay a $2,000 fine, attend a generative AI continuing legal education course, and provide a copy of the order to the client); *Gregoire v. Bd. of Trs. of the S.F. Bay Area Rapid Transit Dist*., No. 3:25-cv-02150-TSH, 2026 U.S. Dist. LEXIS 100834 (N.D. Cal. May 6, 2026) (imposing sanctions and requiring ethical training where filings contained multiple unverified citations generated through AI systems); *Wadsworth v. Walmart Inc*., 348 F.R.D. 489 (D. Wyo. 2025) (sanctioning individual attorneys for filing AI-generated fictitious citations and reaffirming counsel's non-delegable duty to independently verify legal authorities under Rule 11; the court also considered firm training and internal safeguards in declining to impose additional firm-level sanctions). These authorities reflect a consistent judicial approach requiring attorneys to verify the accuracy of legal authorities before filing them with a court. In federal civil proceedings, courts have enforced these obligations through Rule 11 sanctions, while in criminal proceedings courts have relied on their inherent authority to impose comparable sanctions for the submission of fictitious or AI-generated citations.

8. 22 N.Y.C.R.R. pt. 161, app. A (Model Rule Regarding Use of Artificial Intelligence Technology in Preparing Court Papers) (2026), https://www.nycourts.gov/rules/part-161-use-artificial-intelligence-technology (requiring attorneys using artificial intelligence tools to "carefully review the paper and independently ensure" that submissions do not contain "fabricated or fictitious cases, statutes, or other material"); *Williams v. The Estates LLC*, 663 F. Supp. 3d 466, 478 (M.D.N.C. 2023) (holding that attorney violated Rule 11 by serving as a "rubber stamp" and failing to independently verify filings signed under their name); *IBT Emp. Grp. Welfare Fund v. Compass Mins. Int'l, Inc*., 723 F. Supp. 3d 1053, 1061 (D. Kan. 2024) ("[A] wholesale failure to investigate violates Rule 11(b)." These authorities collectively reflect the non-delegable nature of the attorney's duty of verification, which remains fully with counsel notwithstanding the use of automated systems to generate legal text.

9. Antonio R. Damasio, Descartes' Error: Emotion, Reason, and the Human Brain (G.P. Putnam 1994); Lawrence W. Barsalou, *Grounded Cognition*, 59 Ann. Rev. Psychol. 617 (2008); Christopher P. Neck & Charles C. Manz, *Thought Self-Leadership: The Impact of Mental Strategies Training on Employee Cognition, Behavior, and Affect*, 17(5) J. Org. Behav. 445 (1996).

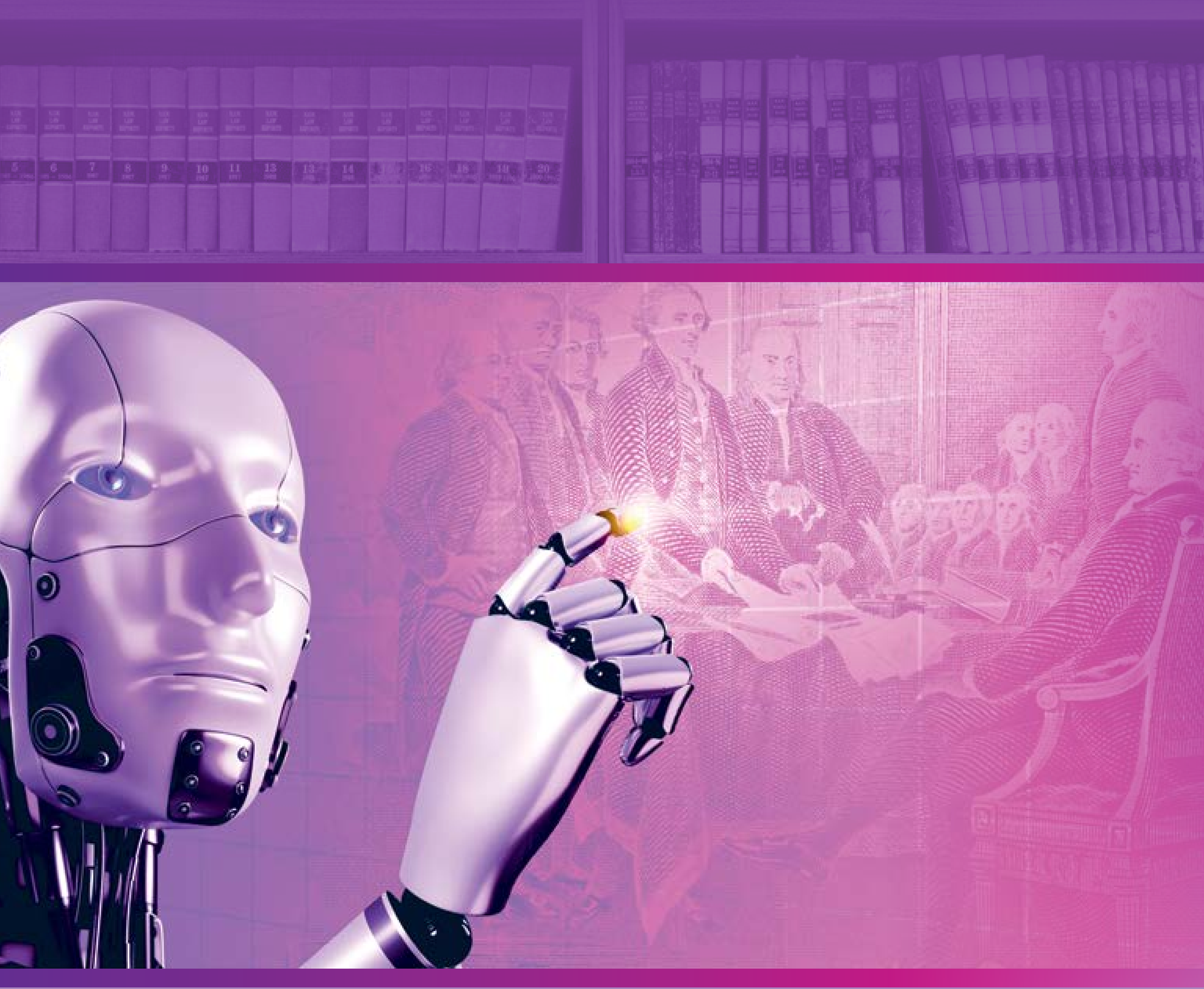
10. Wenjing Xu, Lei Wang, Li Yang, Yan Zhu & Peng Chen, *Sleep Deprivation Alters Utilization of Negative Feedback in Risky Decision-Making*, 15 Frontiers in Psychiatry 1307408 (2024), https://doi.org/10.3389/fpsyt.2024.1307408.

11. Bloomberg Law, 2024 Attorney Well-Being Report: The Divide Between Health & the Legal Industry 4–6 (2024), https://assets.bbhub.io/bna/sites/18/2024/09/BLAW_2024_Well-Being-Report.pdf. The survey included more than 600 respondents, 97% of whom were practicing attorneys.

12. Scott A. Boorman, *Fundamentals of Strategy: The Legacy of Henry Eccles*, 62(2) Naval War Coll. Review 91, 103 (2009).

13. Arnold B. Bakker & Evangelia Demerouti, *The Job Demands–Resources Model: State of the Art*, 22 Journal of Managerial Psychology, 22(3), 309–328, (2007), http://dx.doi.org/10.1108/02683940710733115; Arnold B. Bakker & Evangelia Demerouti, *Job Demands–Resources Theory: Taking Stock and Looking Forward*, 22 Journal of Occupational Health Psychology, 22(3), 273–285 (2017), https://doi.org/10.1037/ocp0000056.

14. Katsiaryna Zinavenka, *Think Big with Mentee Insight: Strategic Solutions via Analysis* (Nov. 24, 2024), https://www.menteeinsight.com/blog/think-big-with-mentee-insight-strategic-solutions-via-analysis ("Nowadays, strategy is too important to be left to a few top-level executives.").



AI in Legal Writing and Research: It's a Tool, Not a Tribunal

By Hon. Gerald Lebovits

Artificial intelligence is a machine-based system that can make predictions, recommendations, or decisions in pursuit of human-defined objectives.[1] Generative AI, the form most relevant to lawyers and judges, uses large language models to produce text in response to prompts. Its arrival has changed legal research and writing more rapidly than any development since computer-assisted research became commonplace.

New York judges and litigators should neither romanticize nor demonize the technology. AI is a tool, not a tribunal. Its speed can be useful; its confidence can be dangerous. The New York State Unified Court System's Advisory Committee on Artificial Intelligence and the Courts has recognized that responsible use can improve the administration of justice and help judges and lawyers work more effectively and efficiently.[2] The practical question is no longer whether AI will enter legal practice, but how to use it without sacrificing accuracy, confidentiality, independence, or professional voice.

Legal Research: Use AI To Find the Path, Not Declare the Law

Legal research is one of generative AI's most promising uses. A judge or litigator can ask a tool to identify possible claims and defenses, generate Boolean searches, suggest terms of art, organize a chronology, compare authorities or summarize a group of cases supplied by the user. A judge or attorney can use it to build a research plan from the parties' submissions. A litigator can ask it to identify factual gaps that might matter on a motion to dismiss or for summary judgment. These tasks can reduce the time spent staring at a blank search box.

AI use in judicial research is no longer theoretical. A December 2025 survey of 112 responding federal judges found that more than 60% reported using at least one AI tool in judicial work. Legal research was the most frequently reported use.[3] Lexis and Westlaw have likewise incorporated generative features into their research platforms, reflecting a broader movement toward AI-assisted retrieval, synthesis, and document analysis.[4]

AI can point to the law, but it is not the law. A general-purpose chatbot does not become an authoritative legal database merely because it produces a polished answer or cites cases. Even an AI-enhanced legal-research platform can miss controlling authority, misstate a holding, confuse jurisdictions or rely on an outdated proposition. Empirical testing has found erroneous or unsupported answers even from leading legal-research products that use retrieval-augmented generation.[5]

For New York research, jurisdictional discipline is essential. A useful prompt should identify the court, department, procedural posture, date range and governing body of law. "Find cases about negligent supervision" is weak. Better is, "Generate natural-language and terms-and-connectors searches for New York Court of Appeals and Second Department decisions addressing negligent supervision of a student injured during recess on a motion for summary judgment." The prompt narrows the legal question without pretending that the model's answer is authority.

The researcher should then leave the AI environment and examine the sources. Read the full opinion, not merely the generated summary or quoted fragment. Confirm the court, date, subsequent history, procedural posture and precise issue decided. Determine whether the cited proposition comes from a majority opinion, concurrence, dissent or dictum. Check whether a later New York case distinguished, limited or rejected the proposition. Confirm that federal authority is being used for the right purpose and is not silently displacing controlling state law.

AI is especially useful after the researcher has assembled reliable material. Supplying the tool with the relevant cases, statutes, briefs or record excerpts allows it to compare facts, identify doctrinal tensions and organize authorities by proposition. This grounded use is safer than asking a model to answer from its internal training alone. It is still not self-validating. Retrieval-augmented generation can reduce unsupported answers, but the model can misread the very document it retrieved.[6]

Let the machine organize the record; do not let it decide what the record means. It can extract dates from supplied documents, produce a witness-by-witness chronology, compare contract versions or list factual assertions without record citations. A judge might ask it to compare the parties' statements of material facts; a litigator might ask it to locate altered quotations. These uses are strongest when every output can be traced to an identified source.[7]

Legal Writing: Accelerate the Process Without Surrendering the Author

Generative AI can help at every stage of legal writing. Before drafting, it can create an outline, identify missing elements, propose headings, test the order of arguments and turn disorganized notes into a working structure. During drafting, it can produce a first version of a statement of facts, point heading, bench memorandum, client letter or proposed order. During revision, it can shorten sentences, eliminate repetition, improve transitions, vary sentence length, identify undefined terms and flag inconsistent names or dates.

For New York writers, the tool can also help format citations under the Bluebook or the Official New York Law Reports Style Manual – the Tanbook.[8] It can convert a string citation into a parenthetical explanation, suggest a clearer issue statement or reorganize an argument using a requested framework. Used as a Socratic partner, it can ask what fact most strongly favors the opponent, what assumption underlies the analysis or where a judge is likely to push back.

These uses are valuable for new litigators. Generative AI can give immediate feedback that a busy supervisor might not have time to provide: the rule paragraph is too abstract; the analysis does not connect the facts to the elements; the reasoning does not support the conclusion; the tone is accusatory; the paragraph contains three ideas and should be divided. That coaching can accelerate development, but only if the lawyer evaluates the advice rather than accepting it automatically. The goal is to improve judgment, not outsource it.

Judges and advocates should use the same technology differently. An advocate may test alternative theories, sharpen persuasive emphasis and seek language that frames the facts favorably within the bounds of candor. A judge must write from a neutral position, distinguish the parties' contentions from the court's findings and explain why one argument prevails without caricaturing the other. A prompt useful for a brief might be inappropriate for a judicial opinion. The user should tell the model what institutional role the writer occupies and then edit the output to ensure that the role is honored.[9]

Experienced judges and litigators can use AI to remove administrative tasks and reserve attention to selecting the controlling rule, weighing competing analogies, deciding what the record proves, confronting the strongest counterargument and choosing proportionate language. The machine may perform the first pass, but the author must perform the last.

AI-generated prose should always be treated as draft text. Legal writing expert Bryan A. Garner has emphasized that AI output requires human review, curation and enhancement and that style, tone, critical thought and ethical communication cannot be subcontracted.[10] That principle is especially important in judicial writing. An opinion is not merely an information product. It explains the court's exercise of public authority. The judge must own its reasoning, tone, citations, and consequences.

The most important edit is substantive. AI prose often sounds complete before the analysis is complete. It can state a correct rule yet fail to explain why the rule controls these facts. It can describe both sides while avoiding the conflict between them. It can cite a legitimate case without engaging with its procedural posture. And it can write a confident conclusion that does not follow from the preceding paragraphs. These defects are more serious than the stylistic habits sometimes associated with AI, such as excessive em dashes, symmetrical phrasing, generic transitions or uniformly polished sentences.

Accordingly, the editor should ask four questions. Does the draft identify the governing New York authority? Does it apply the legally significant facts rather than merely repeat them? Does it address the opponent's best argument? Does every cited source support the exact proposition attributed to it? If the answer to any question is no, the prose is not ready, however fluent it appears.

Hallucinations, Hollow Reasoning and the Duty To Verify

Generative AI is trained to generate plausible language, not to distinguish truth from falsity. It can fabricate cases, quotations, statutes, docket numbers and pinpoint citations. It can combine the facts of one case with the holding of another, cite an overruled decision as current law or attribute a federal standard to a New York court. A 2024 study of public-facing models found legal hallucinations in at least 58% of tested responses overall and at least 63% of responses asking for a case's central holding.[11]

AI's distinctive danger is not error alone, but error delivered quickly, repeatedly and persuasively. It can produce fictitious authorities in seconds and describe each with the tone of a reliable reporter. The user's duty grows with the tool's speed.

The sanctions decisions make the point. In the seminal *Mata v. Avianca, Inc.*, lawyers were sanctioned after submitting nonexistent decisions generated by ChatGPT and then failing to correct the problem responsibly.[12] In *Noland v. Land of the Free, L.P.*, a California appellate court imposed $10,000 in sanctions after fabricated quotations and authorities appeared in briefs, emphasizing counsel's personal obligation to read and authenticate the cited material.[13] Reported AI-misuse remedies have included monetary sanctions, disciplinary referrals, rejecting or striking papers and other remedial, deterrent or punitive orders.[14]

Verification must be systematic. A cite-and-substance review should confirm that every authority exists, is current, comes from the represented court and year and supports the stated proposition. Quotations must be compared word for word with the source. Pinpoint pages must be checked. Statutes and rules must be read in context. The reviewer should also test internal consistency: party names, dates, defined terms, cross-references, requested relief and the relationship between the facts and conclusion.

Detection software is not a substitute for this review. It can generate false positives and false negatives, and skilled editing can remove stylistic traces of AI assistance. The better question is not "Was this written by AI?" but "Was this work produced and reviewed through a reliable process?" Relevant process evidence might include draft history, prompt logs, metadata, research trails and chambers or firm procedures. In ordinary practice, however, the finished document should be judged primarily by its accuracy, reasoning and compliance with governing duties.

Confidentiality, Privilege and Secure Tools

A powerful prompt often requires facts, and facts can be confidential. Lawyers must make reasonable efforts to prevent unauthorized disclosure or access to client information under Rule of Professional Conduct 1.6.[15] Judges must protect nonpublic information acquired in a judicial capacity. Entering party names, sealed material, medical information, addresses, unpublished draft decisions or record evidence into a public consumer tool can create risks that do not disappear merely because the output is useful.

The analysis depends on the product's terms, settings, data practices and institutional controls. A paid subscription alone does not establish that prompts are private or excluded from model training. Users should know whether prompts and uploaded documents are retained, who can access them, whether organizational administrators can retrieve them, where files are stored and what audit or e-discovery rules apply. Prompts created through an employer's enterprise system should be treated as institutional records, not private notes.

Privilege and work product require separate analysis. In *Assini v. Hayward*, a Nassau County Supreme Court justice treated a self-represented litigant's AI prompts as conditionally protected litigation-preparation materials under CPLR 3101(d) because they were prepared solely in anticipation of litigation, and quashed the subpoena seeking them.[16] The decision illustrates why lawyers should not assume that every AI interaction is privileged – or that no AI interaction can receive protection.

New York Rules for Judges

The UCS Interim Policy on the Use of Artificial Intelligence applies to judges and staff, including UCS work performed on personal devices.[17] It requires training and limits use to tools approved by the Division of Technology and Court Research.[18] The policy also prohibits entering confidential information into tools that do not operate with appropriate private or enterprise protections.

The approved-tool requirement reflects judicial duties under 22 N.Y.C.R.R. Part 100 to preserve public confidence, maintain competence, act impartially and diligently and protect nonpublic information.[19] Enterprise systems may offer stronger security, centralized controls, audit logs and contractual restrictions on data use than public consumer products.[20] Those safeguards reduce risk but do not replace the judge's duty to understand the system.

The central ethical principle is straightforward: Generative AI must never displace the reasoning, judgment, discretion and legal responsibility required of judges.[21] An approved tool can help brainstorm, summarize supplied material, compare documents, improve prose and support research. It may not be used to conduct independent factual investigation, supplement the record, receive improper external information or decide credibility and outcome. The record, governing law and judge's independent analysis must control.

New York judges need tools suited to judicial work. Microsoft Copilot Chat is the only AI tool the UCS currently allows judges and the court's legal staff to use for research and writing. To access the UCS version of Copilot Chat, judges must log into their UCS work account. The UCS version of Copilot Chat is more secure than the free Microsoft version, but it is not smarter.

The UCS should secure two essential upgrades for judges. First, it should give judges access to Microsoft 365 Copilot, and not just Copilot Chat. Microsoft 365 Copilot integrates with Microsoft 365 applications that New York judges use, including Outlook, Word, Excel, PowerPoint, Teams, SharePoint and OneDrive.

Second, judges need access to AI-enhanced Westlaw and Lexis, given that Copilot Chat can help with general drafting and summarization, but it is not a legal-research database. The entire federal judiciary has had Westlaw with CoCounsel since April 2025.[22] Forty-seven states have also adopted CoCounsel for their judges.[23] New York is not among the 47. Over 200 law schools and more than 120,000 law students have access to AI-enhanced Westlaw.[24] And Lexis has been rolling out AI to nearly every U.S. law school since late 2023. When it comes to AI legal research, New York judges are behind federal judges, most state judges, many practitioners and even many first-year law students.[25]

New York Rules for Litigators

For litigators, the statewide baseline is Use of Artificial Intelligence Technology, 22 N.Y.C.R.R. Part 161, effective June 1, 2026.[26] It applies in civil and criminal cases to affidavits, affirmations, briefs, memoranda, pleadings and other papers prepared by an attorney or party for submission to a UCS court. It excludes materials constituting or offered as evidence.

Part 161 permits the use of AI, but it preserves the filer's responsibility for accuracy regardless of whether AI helped prepare the paper. It allows individual judges to adopt Part rules but encourages use of a model rule requiring users to understand AI's capabilities and limitations and independently ensure that papers contain no fabricated or fictitious material.[27] Litigators must therefore check both Part 161 and the assigned judge's current rules. Several New York City justices require disclosure, identification of the tool or affected portions, certification of review or some combination of those requirements.[28]

Part 161 itself does not impose a general disclosure requirement. That choice is consistent with existing duties. Rule 3.3 prohibits false statements of fact or law; 22 N.Y.C.R.R. §§ 130-1.1 and 130-1.1-a provide that papers containing materially false factual statements may be frivolous and treat a signature as a certification after reasonable inquiry.[29] Bluebook Rule 18.3 prescribes a citation format when a writer cites generative-AI output. It is a citation rule, not a general disclosure rule for AI-assisted drafting.[30]

Competence remains essential. Rule 1.1 requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for representation.[31] In the AI context, competence includes selecting an appropriate tool, protecting information, recognizing limitations and reviewing output with enough care to catch fabricated authority and defective reasoning. The machine may be new. The duties are not.

Sanctions might await those who do not fully audit their AI-assisted work. In May 2026, the Appellate Division, Second Department, sanctioned an unrepresented litigant $250 for one hallucinated citation.[32] And on July 31, 2026, the Supreme Court of Connecticut sanctioned an attorney for seven hallucinated citations in two separate cases, ordering him to complete additional ethics- and AI-focused CLE courses, donate $1,000 to the Connecticut Bar Institute (with his firm required to donate an additional $1,000), file a compliance report within six months, follow reciprocal disciplinary rules in any other state in which he is licensed and post the court's decision online. And the court named him 23 times.[33]

A Practical Workflow for Judges and Litigators

A reliable AI workflow has five stages.

First, choose the right tool. Use general-purpose AI for low-risk brainstorming, organization, editing or nonconfidential summarization; use source-linked legal platforms for research; and use only UCS-approved tools for judicial work. Price, popularity, and an easy-to-use interface prove neither security nor accuracy.

Second, frame a narrow prompt. State the jurisdiction, court, procedural posture, legal issue, relevant facts, requested format and source requirements. Break a complex project into manageable steps: search terms, issue outline, comparison of supplied authorities, then a draft.[34]

Third, require useful output. Ask the tool to separate controlling from persuasive authority, identify uncertainty, hyperlink sources, state assumptions and flag missing facts. Specify the audience, tone, length and citation style, and request the strongest counterargument and the facts that could change the result.

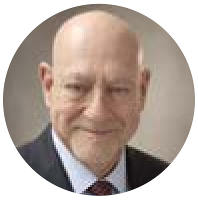
Fourth, challenge the response. Follow-up prompts should test, not merely polish: "What authority cuts against this conclusion?" "What assumptions did you make?" "Where might a New York judge disagree?" "Does the result change in another Appellate Division?" "Which sentence is least supported?" Iterative prompting can expose weaknesses, but it does not make the answer reliable by itself.[35]

Fifth, verify and rewrite. Open every source, conduct the cite-and-substance review, compare the draft with the record, correct jurisdictional slippage, add missing analysis and remove overstatement. The signature remains human even when the first draft is not.

Conclusion

Generative AI can make legal research faster and writing clearer. It can find issues, develop searches, compare authorities, organize arguments, edit prose and test counterarguments. It can also expose confidential information, invent law and flatten nuance.

The answer is disciplined use: the right tool, a precise prompt, secure information handling, independent research, aggressive editing and complete verification. Used well, AI can give judges and litigators more time for the judgment and responsibility that remain theirs alone.



Hon. Gerald Lebovits is a Manhattan Supreme Court Justice and an adjunct professor at Columbia, Fordham, and NYU law schools. He wrote the New York State Bar Association Journal's Legal Writer column for 20 years.

Endnotes

1. 15 U.S.C. § 9401(3) (defining artificial intelligence as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments").

2. N.Y. State Unified Ct. Sys. Advisory Comm. on Artificial Intelligence & the Courts, *Annual Report to the Chief Judge and the Chief Administrative Judge of the State of New York* 13 (Dec. 2025), https://webfiles.nycourts.gov/public/2026-01/ai-annual-report-2025.pdf ("Advisory Comm. Report").

3. Anika Jaitley et al., *Artificial Intelligence in Federal Courts: A Random-Sample Survey of Judges*, 27 Sedona Conf. J. _ (forthcoming 2026) (manuscript at 5–6, 13–20), https://www.thesedonaconference.org/sites/default/files/publications/Artificial_Intelligence_in_Federal_Courts_preprint_0.pdf.

4. *See* Thomson Reuters, *Thomson Reuters Launches Generative AI-Powered Solutions to Transform How Legal Professionals Work* (Nov. 15, 2023), https://www.thomsonreuters.com/en/press-releases/2023/november/thomson-reuters-launches-generative-ai-powered-solutions-to-transform-how-legal-professionals-work; LexisNexis, *LexisNexis Launches Lexis+ AI, a Generative AI Solution with Hallucination-Free Linked Legal Citations* (Oct. 25, 2023), https://www.lexisnexis.com/community/pressroom/b/news/posts/lexisnexis-launches-lexis-ai-a-generative-ai-solution-with-hallucination-free-linked-legal-citations.

5. Varun Magesh et al., *Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools*, Stanford RegLab & Stanford HAI 22 J. Empirical Legal Stud. 216, 216–42 (2025), dho.stanford.edu/wp-content/uploads/Legal_RAG_Hallucinations.pdf (finding hallucination rates of 17 to 33 percent among the tested legal-research tools).

6. James Ju, *Retrieval-Augmented Generation in Legal Tech*, Thomson Reuters (Dec. 4, 2024), https://legal.thomsonreuters.com/blog/retrieval-augmented-generation-in-legal-tech; Magesh et al., *supra* note 5, at 219–20.

7. *See* N.Y. State Unified Ct. Sys., *Interim Policy on the Use of Artificial Intelligence* 1–2, 5 (Oct. 2025; amended May 2026), https://www.nycourts.gov/LegacyPDFS/a.i.-policy.pdf (hereinafter Interim Policy) (identifying first drafting, editing, and summarizing data as potential uses and requiring human review); Am. Bar Ass'n, *Legal ChatGPT: Tips, Prompts, and Use Cases* (Mar. 21, 2025), https://www.americanbar.org/groups/law_practice/resources/law-technology-today/2025/legal-chatgpt-tips-prompts-and-use-cases/ (discussing document summarization, drafting, and review).

8. *See* N.Y. Law Reporting Bureau, *Official New York Law Reports Style Manual* (2022), https://www.nycourts.gov/reporter/style-manual/2022/2022-SM.shtml; Thomas J.K. Smith & Gerald Lebovits, *The Case for Official New York Tanbook Citations*, N.Y.L.J., July 31, 2025, at 3, col. 1, https://www.nycourts.gov/reporter/files/tanbook-article.pdf.

9. *See* Am. Bar Ass'n, *supra* note 7 (recommending a clear role, detailed context, manageable tasks, and follow-up questions); Thomson Reuters, *Introduction to Writing Effective AI Legal Prompts* (Jan. 16, 2024), https://legal.thomsonreuters.com/blog/writing-effective-legal-ai-prompts.

10. Bryan A. Garner, *LawProse Lesson #462: Writing Skills in the Age of AI*, LawProse.org (Oct. 3, 2025), https://lawprose.org/lawprose-lesson-462-writing-skills-in-the-age-of-ai/.

11. Matthew Dahl et al., Varun Magesh, Mirac Suzgun & Daniel E. Ho, *Large Legal Fictions: Profiling Legal Hallucinations in Large Language Models*, 16 J. Legal Analysis 64, 64, 82–83 (2024), https://academic.oup.com/jla/article/16/1/64/7699227.

12. *Mata v. Avianca, Inc.*, 678 F. Supp. 3d 443, 448, 461–66 (S.D.N.Y. 2023).

13. *Noland v. Land of the Free, L.P.*, 114 Cal. App. 5th 426, 430–31, 441–49 (2025).

14. *See* Lorenzo Rovini, *Avoiding Sanctions in the Gen AI Era: Practical Guardrails for Lawyers*, NYSBA News Center (Apr. 21, 2026), https://nysba.org/avoiding-sanctions-in-the-gen-ai-era-practical-guardrails-for-lawyers/; Advisory Committee Report, *supra* note 2; Damien Charlotin, *AI Hallucination Cases*, https://www.damiencharlotin.com/hallucinations (last visited Aug. 7, 2026).

15. N.Y. Rules of Prof'l Conduct Rule 1.6(c), N.Y. Comp. Codes R. & Regs. tit. 22, § 1200.0 (N.Y.C.R.R.); N.Y.C. Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 2024-5, *Ethical Obligations of Lawyers and Law Firms Relating to the Use of Generative Artificial Intelligence in the Practice of Law* 2–3 (Aug. 2024), https://www.nycbar.org/reports/formal-opinion-2024-5-generative-ai-in-the-practice-of-law/; ABA Standing Comm. on Ethics & Pro. Responsibility, Formal Op. 512, *Generative Artificial Intelligence Tools* 6–8 (July 29, 2024), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf.

16. *See Assini v. Hayward*, 2026 N.Y. Slip Op. 26086, at *3–4 (Sup. Ct., Nassau Co. June 4, 2026) (quashing a subpoena and applying CPLR 3101(d) to AI prompts prepared solely in anticipation of litigation).

17. Interim Policy, *supra* note 7, at 1.

18. *Id.* at 5–6; Advisory Comm. Report, *supra* note 2, at 13.

19. *See* 22 N.Y.C.R.R. pt. 100, especially Rules 100.1, 100.2, 100.2(A), 100.3, 100.3(B)(1), 100.3(B)(4), and 100.3(B)(11).

20. Microsoft, *Enterprise Data Protection in Microsoft 365 Copilot and Microsoft 365 Copilot Chat*, Microsoft Learn (last updated May 29, 2026), https://learn.microsoft.com/en-us/microsoft-365/copilot/enterprise-data-protection; Microsoft, *Microsoft 365 Copilot Chat Privacy and Protections*, Microsoft Learn (last updated Mar. 3, 2026), https://learn.microsoft.com/en-us/copilot/privacy-and-protections.

21. Advisory Comm. Report, *supra* note 2, at 147–54 (Appendix 9, "Ethical Considerations and Recommendations for the Use of Artificial Intelligence by Judges and Judicial Staff").

22. Thomson Reuters, *Westlaw Precision with CoCounsel, Practical Law, and CoCounsel to Be Provided to US Federal Courts as the Essential Information Provider for the Federal Judiciary* (Apr. 9, 2025), https://www.thomsonreuters.com/en/press-releases/2025/april/westlaw-precision-with-cocounsel-practical-law-and-cocounsel-to-be-provided-to-us-federal-courts-as-the-essential-information-provider-for-the-federal-judiciary.

23. Thomson Reuters, *Is CoCounsel Legal a Tool for Judges?* (Apr. 3, 2026), https://legal.thomsonreuters.com/blog/is-cocounsel-legal-a-tool-for-judges.

24. Thomson Reuters, *Thomson Reuters Brings Agentic AI to Over 200 Law Schools* (Jan. 22, 2026), https://www.thomsonreuters.com/en/press-releases/2026/january/thomson-reuters-brings-agentic-ai-to-over-200-law-schools.

25. LexisNexis, *LexisNexis Collaborates with U.S. Law Schools to Roll Out Lexis+ AI, Marking First Widespread Use of Legal Generative AI Solution in Law School Education* (Dec. 20, 2023), https://www.lexisnexis.com/community/pressroom/b/news/posts/lexisnexis-collaborates-with-u-s-law-schools-to-roll-out-lexis-ai-marking-first-widespread-use-of-legal-generative-ai-solution-in-law-school-education.

26. 22 N.Y.C.R.R. §§ 161.1–161.2.

27. *Id.* §§ 161.3–161.4 & Appendix A.

28. *See, e.g.*, Hon. Aaron D. Maslow Part Rules § C15, https://www.nycourts.gov/courts/kings-county-supreme-court-civil-term/hon-aaron-d-maslow (last visited Aug. 10, 2026).

29. N.Y. Rules of Prof'l Conduct Rule 3.3(a)(1); 22 N.Y.C.R.R. §§ 130-1.1(c), 130-1.1-a(b).

30. The Bluebook: A Uniform System of Citation R. 18.3 (22d ed. 2025); Jessica R. Gunder, *Yikes! The Bluebook's Generative AI Rule Is Flawed*, 99 S. Cal. L. Rev. Postscript 93 (2026), https://southerncalifornialawreview.com/2026/04/09/yikes-the-bluebooks-generative-ai-rule-is-flawed/ (describing Rule 18.3 as prescribing a citation format for generative-AI material).

31. N.Y. Rules of Prof'l Conduct Rule 1.1(a).

32. *Julien v. Arthur*, 2026 N.Y. Slip Op. 03308 (2d Dep't May 27, 2026); *cf. Brown v. Real Estate Capital Am. LLC*, 2026 N.Y. Slip Op. 51211(U) (Sup. Ct., N.Y. Co. Aug. 7, 2026) (assuming without deciding that a lawyer submitted a brief with one quotation fabricated by AI, the court nonetheless declined, in its discretion, to impose any sanction).

33. *Tov Realty, LLC v. Suarez*, 355 Conn. 902, 907–08 (2026).

34. Am. Bar Ass'n, *supra* note 7; Thomson Reuters, *supra* note 9.

35. Follow-up, or iterative, prompting asks a model to critique, test, or revise a response within the current exchange; it is a method of refining output, not independent verification. *See* Am. Bar Ass'n, *supra* note 7.

How To Avoid an AI Horror Story: Verify, Verify, Verify

By Michael L. Fox

Artificial intelligence, like many other forms of technological advancements over the years, has been rapidly adopted by attorneys and courts all over the world, and it is here to stay. By now, we have likely all read about horror stories – hallucinated case citations, incorrectly summarized case decisions, misinterpreted case holdings, cybersecurity risks and ethical violations.[1] This author has penned articles warning about those very risks and proposing some solutions.[2] However, at the end of the day there are many ways in which attorneys and judges can ethically and safely utilize AI and other forms of technology to advance the legal profession and its service to society. It requires application of safe and sound practices that responsible attorneys must oversee and certify. The purpose of this article is to highlight several ways in which the legal profession could address some digital world dangers in everyday practices.

Loss of Privilege or Fifth Amendment Protections Due to Cyber-Hack or Warrant Execution?

Horror Story 1

The reader is no doubt familiar with loss of privilege or confidentiality due to affirmative actions taken by parties interfacing with technology.[3] But what if a search warrant is issued in a criminal matter that addresses electronic materials that fall under the Stored Communications Act (such as submissions and prompts to AI or a chatbot)? Or, what if a malicious actor hacks or unlawfully accesses an account containing privileged or confidential material? Will the protections otherwise afforded by law be lost in those situations?

To begin, if a search warrant is issued, the subject of the investigation – the customer/consumer utilizing the electronic platform – cannot seek to anticipatorily challenge or move to quash the warrant according to *United States v. Kim*.[4] The service provider is the entity that has limited standing *ex ante*. The customer or consumer has standing to move to suppress evidence *ex post* and may seek to do so in protection of their rights at a suppression hearing after return of the warrant.[5] The *Kim* case, like *United States v. Heppner*, was from the Southern District of New York, and while such trial court rulings are not binding on any other court or judge and are not precedential, they may be highly persuasive.

Thus, if a chatbot is utilized by a party or client and a search warrant is issued, as in *Kim*, the material appears thus far to be subject to the initial warrant return (unless quashed on motion by the service provider), but thereafter could be challenged in a suppression hearing by the customer/consumer. In such a case, though, counsel or the party pro se will have to apply or distinguish *Heppner, Warner, Morgan, Assini*, et al. in an attempt to procure protection for alleged privileged or work-product material and convince the respective court of same.[6]

A related question in the intersecting fields of privilege, constitutional rights and cybersecurity is, therefore, whether privilege or constitutional protections will ultimately be lost if the subject is the victim of a hack, cyberattack or warrant execution or some other action that results in unauthorized viewers accessing protected material? So far, the courts have answered this question in the negative.

In a 2025 decision of the New York State Supreme Court, Appellate Division, Fourth Department, the court ruled that a warrant cannot compel a suspect or target to unlock a mobile device with a fingerprint, as such is equivalent to a testimonial act.[7] While the warrant did not violate the Fourth Amendment, it did violate the Fifth Amendment by requiring the target to unlock the phone – the person thereby acknowledging how to access the phone and demonstrating control over the device and contents. Thereafter, the evidence was suppressed and constitutional protection was not lost.[8]

Given concerns over the prevalence of hacking, spyware, malware and other impermissible electronic intrusions in today's e-world, one might similarly question whether that access – albeit unauthorized and illegal – compromises the attorney-client privilege. The answer to that, at least in New York, also still appears to be "no," according to the court in *C.C. v A.R.*[9] Pursuant to the court's holding in *C.C.*, if the cyber-attacker is another party to the case at issue, they could face very strict sanctions:

> This appeal examines the proper sanction in a matrimonial litigation where one party installed spyware on the other party's phone, invoked Fifth Amendment protections on the issue, and intentionally destroyed evidence as to what the spyware intercepted. The [trial court] properly determined, under the circumstances here, that it is proper to infer that the plaintiff violated the defendant's attorney-client privilege, and that the appropriate sanction is to strike the causes of action in the complaint relating to the financial issues of the case other than child support. ... Here, where the plaintiff violated the defendant's attorney-client privilege, the preclusion of documents is not an appropriate alternative sanction because the plaintiff will always be privy to any litigation strategy of the defendant that he gained through secretly intercepting her privileged communications. … As the plaintiff "chose the course of action that exacerbated the harm"…, the defendant has been seriously compromised in defending herself in this divorce action.[10]

Therefore, as a practicing attorney, be cautious, use proper security protocols, remain vigilant and take continuing legal education courses to update skills and knowledge in cybersecurity, and advise clients to take some of the same safeguarding and preventive measures. Attorneys may wish to expand their representation letters or retainer agreements, advising their clients/entities in writing regarding the above case law and court holdings; counseling them about whether it would be best to avoid chatbot/AI use; and advising regarding practical limits. Having the client countersign the letter, agreement or writing, and maintaining a copy in the file will document that counsel has advised the client or corporate entity (in the case of in-house counsel), warned them of the risks, and acted to mitigate potential future loss of privilege from what would otherwise have been the client's unguided utilization of technology to research legal issues prior to, or in place of, discussing the same with their attorney.

Then take some comfort in recognizing that unauthorized and illegal access to privileged communications occurring from spyware, malware or warrant executions that violate the Fifth Amendment thus far do not appear to compromise privilege or the right against self-incrimination in the eyes of the courts. However, beware: As the world and the courts become ever more familiar with the risks and benefits of technology, and as attorneys are expected to be more familiar with those and responsive security protocols are implemented, courts might grow to be less protective and tolerant of breaches that cause loss of privileged or confidential information. It is vital, then, that an attorney's protocols are robust, counseling of clients is thorough, and overall, the attorney demonstrates competence and sound practices.[11]

Ensure You Have Properly Programmed Any AI System That Assists With Hiring

Horror Story 2

AI is utilized as a hiring manager assistant to review numerous job applications in order to save time and money and other personnel resources at the hiring entity. AI then makes "decisions" utilizing biased programming. Could this result in liability and/or ethics sanctions for discriminatory decision-making in violation of law?

As AI technology has expanded, so have uses of AI in most areas of our society. This includes utilizing AI resources to assist in culling through sometimes myriad submissions in response to job postings – in essence, making AI the first-level human resources manager regarding résumé reviews. However, beware of two concomitant concerns – "automation bias" and potentially discriminatory hiring practices.

Automation bias is where humans presume that technology and AI are, basically, infallible, and we therefore accept and confirm whatever they tell us or show us largely without question[12] (thus also helping to explain why we are seeing so many cases involving hallucinated citations in briefing). This was shown to be a major problem in the law when an individual was falsely accused of being a thief by AI facial recognition when he was 30 miles away (confirmed by alibi evidence).[13] The alibi evidence was almost pushed aside because the AI facial recognition was taken as gospel. However, the defendant, his attorneys and experts questioned the AI, and he was exonerated.[14]

Additionally, we are all familiar with the saying "garbage in, garbage out" – referring here to how well the AI platform is programmed; that is, the level of quality in output one can expect to receive. Thus, be careful if your hiring manager is also an AI platform – even if only for the initial round of résumé reviews. Legal commentators, attorneys and other experts have been discussing the risks associated with AI programs used to screen applicants in a hiring process. Because AI first utilizes the data with which it is programmed and then learns, there is concern that old methods and data, and bias in the system, could result in bias during screening and hiring phases.[15]

Some jurisdictions, such as New York City, have instituted laws to require system audits and to punish those employers or employment agencies whose AI systems are found to include illegal bias.[16]

Attorneys in New York should also be familiar with the provision in the Rules of Professional Conduct that states: "A lawyer or law firm shall not: … (g) unlawfully discriminate in the practice of law, including in hiring, promoting or otherwise determining conditions of employment on the basis of age, race, creed, color, national origin, sex, disability, marital status or sexual orientation. …"[17] While there has been some debate concerning the extent of 8.4(g) to an attorney's arguments in representation of a client,[18] attorneys still must exercise caution when the potential for discrimination in hiring within their firm or agency exists.[19]

If law firms, public agencies or client companies use AI to assist in hiring, they should be aware of the potential risks related to programming and bias – and the potential legal or ethical violations. Here again, attorneys should be familiar with all risks and benefits of technology under the New York Rules of Professional Conduct 1.1 and should ensure that their own practices within their firms or agencies comply with the requirements of law and ethics, while also counseling their clients to ensure the same under the relevant laws and regulations. Audits and random checks of AI platforms (if utilized) – their programing and outputs – should be regularly and routinely conducted to ensure necessary compliance and best practices.

Cite-Check All Briefing, Whether From an Associate, Co-Counsel or Opposing Party

Horror Story 3

An attorney is working with co-counsel in his or her own firm or agency, in addition to local counsel or pro hac vice counsel. The attorney is one of the counselors of record in litigation. Receiving draft briefing from co-counsel, and believing he or she is capable, the attorney in question does not cite-check, and directs co-counsel to sign it and file it with the court. The briefing turns out to contain AI hallucinations, and violates N.Y. Rules for Professional Conduct 3.3, among other rules. Is the otherwise non-offending attorney liable for violations?

Attorneys who do everything right in their own practice and in their own submissions may believe that they have insulated themselves from reproach and protected themselves from ethical criticism. However, that is not necessarily the end of the story. Recently, even some "non-offending" attorneys are being criticized by courts for not being alert to errors in briefing, although contained in submissions not made by that attorney – such as when an attorney fails to cite-check a response or reply brief (depending on the motion and court) from an opposing party on a motion. Normally, absent leave of court, a response to a reply brief (or sur-reply) would not be filed, and the motion would be deemed fully submitted.[20] It might be tempting for an attorney to accept that final reply briefing, and await the court's ruling without doing more (and thus without charging the client for additional review and cite-checking of a brief to which no response would be filed, or without taking time away from another taxpayer-funded matter in the case of an agency). However, courts have begun to criticize non-offending attorneys who wait for judges to be the "last line of defense" – although not yet sanctioning them outright, since technically they did not submit in violation of the rules.[21]

If attorneys are serving as co-counsel, pro hac vice counsel, or local counsel, it will behoove them to cite-check and verify all statements and case citations in any briefing prepared by colleagues, or to which they sign on, or is submitted over their signature or in a case in which they are one of the counselors of record, for risk of being swept up in future sanctions for rules violations.

For example, in *Billups v. Louisville Municipal School District*,[22] a Mississippi federal district court sanctioned an attorney serving as co-counsel within a firm for not checking and catching incorrect briefing containing AI hallucinations and misstatements by their co-counsel for whom the court found they were a supervisory attorney; the supervisory counsel's name had appeared on the initial complaint.[23] Furthermore, that same court then issued a challenge to the opposing party and its counsel – who to that point had not been a direct offending party:

> The Court also observes that the Defendant, … could have flagged the fictious citation and misrepresentation of case law in a reply brief or supplemental filing. … The Court takes this opportunity to issue a charge. Going forward, the Court expects all parties to assist in maintaining the integrity of the judicial process and to be diligent in flagging AI misuse. "[O]therwise, the risk is too great that such errors will persist undetected, potentially leading to an outcome unsupported by law."[24]

Separately, another federal district court in Mississippi addressed an unusual situation where counsel for both parties submitted a briefing that had utilized AI resources, but they did not verify their submissions, and it contained non-existent or incorrect citations.[25] The *Withers* court noted that, by submitting fake, unverified cases, counsel had obviously not read (or had not attempted to read, in any event) those non-existent cases. Such are Rule 11 violations in federal court (as well as ethics violations).[26] The court disqualified and barred both sets of counsel and ordered one of them "to attend a CLE on artificial intelligence with an ethics component addressing the obligations of counsel regarding the use of artificial intelligence in the legal field and submit proof of attendance within 60 days from the date of this Order."[27] Monetary fines were issued, as well, and the court directed that a copy of the order be sent to the respective state bars of the offending attorneys.[28]

Finally, there is a particularly egregious case, *In re Domestic Partnership of Torres Campos & Munoz*,[29] out of California. In *Munoz*, one of the party's counsel cited fictitious case law in a submission. Compounding the problem, the opposing party's counsel thereafter relied on the fictitious

case law, and re-cited it in their own submission to court. The trial court then relied on that same fictitious case law and issued an order citing same. The appellate court admonished all involved in the case, held that the trial court abused its discretion by citing fictitious case law as support for the order, sanctioned counsel, and ruled that the appellant had thereby forfeited their claim.[30]

Hence, our last takeaway – attorneys should be certain to cite-check any submissions to courts or opposing parties that bear their signature, on which their names appear, or in any litigation in which they have taken part in any way – including submissions prepared by attorneys on their own side of the case, as well as on the opposing side.[31] Said attorneys have supervisory and ethical responsibilities to do so.[32] Every single citation, case summary, digest and argument should be sourced and confirmed, in one's own briefing and all opponents' briefing – including all reply briefs to which one might not otherwise respond. If nothing else, failure to do so by an otherwise non-offending party/counsel could at least result in a reprimand from the court, a challenge from the court or possibly worse – such as loss of a sanctions award that could have otherwise been received by that non-offending party.[33]

It is both a startling and exciting world out there, as technology continues its rapid advances – not just in the law, but in all parts of society. Yet, if attorneys take care to exercise oversight and adopt a few cautionary and ethical practices, harnessing technology for use in the legal profession might be quite attainable and may also be quite advantageous.

Michael L. Fox is the acting dean and chairperson of the School of Business and associate professor of business law at Mount Saint Mary College. He is also an adjunct professor at Western Connecticut State University. He is a former NYSBA vice president (Ninth Judicial District), section chair and committee chair and former member of the NYSBA Executive Committee and House of Delegates.

Endnotes

1. *Cassata v. Michael Macrina Architect, P.C.*, 250 N.Y.S.3d 778 (Sup. Ct. Suffolk Co. 2026); *Deutsche Bank Nat'l Tr. Co. v. LeTennier*, 250 N.Y.S.3d 260 (3d Dep't 2026); *Grymes Dev. Co. v Fodera*, 88 Misc. 3d 767, 245 N.Y.S.3d 863 (Sup. Ct., Richmond Co. 2025); *Gully v. Varghese*, 89 Misc. 3d 1208(A), 258 N.Y.S.3d 481 (Sup. Ct., Albany Co. 2026) (citing, *inter alia*, *Grymes*); *Landberg v. City of New York*, 2026 N.Y. Slip Op. 03935 (2d Dep't June 23, 2026) (discussing, *inter alia*, *LeTennier and Julien v. Arthur*, 260 N.Y.S.3d 344, (2d Dep't 2026), and issuing hefty sanction against attorney for AI hallucinations and violations of RPC).

2. Michael L. Fox, *AI & Hallucinations Cause Ongoing Concerns; The Solution May Be Amended Ethics Rules*, N.Y. L.J. at 4, 7 (June 5, 2026); Cynthia Feathers & Michael L. Fox, *Core Ethics for Appellate Lawyers in the Age of Gen AI*, N.Y. L.J. at 4, 8 (Dec. 23, 2025).

3. *See, e.g.*, *United States v. Heppner*, 820 F.Supp.3d 292 (S.D.N.Y. 2026); *but cf. Morgan v. V2X, Inc.*, 2026 U.S. Dist. LEXIS 67939, 2026 WL 864223 (D. Colo. Mar. 30, 2026) (distinguishing *Heppner* because it was a criminal matter versus the civil case before the Court, and in *Heppner* the party "acted entirely apart from his lawyer"). *See also Assini v. Hayward,* 2026 N.Y. Slip Op. 26086 (Sup. Ct., Nassau Co. June 4, 2026) (citing *Morgan* and *Heppner*, also distinguishing rule in criminal cases versus civil cases; defendant warned about complying with new 22 N.Y.C.R.R. Part 161, so as to avoid "use of AI frustrat[ing] the litigation," and going unfettered; citing *Augustin v. Formula 3 Brook. Inc.*, 86 Misc. 3d 1236(A), 236 N.Y.S.3d 586 (Sup. Ct., Kings Co. 2025)).

4. *United States v. Kim*, 2026 U.S. Dist. LEXIS 138072, 2026 WL 1785995 (S.D.N.Y. June 22, 2026).

5. *Id.* at (citing, *inter alia*, *United States v. Grubbs*, 547 U.S. 90, 99 (2006); *Warshak v. United States*, 532 F.3d 521, 523 (6th Cir. 2008); but not citing *Heppner*).

6. *See* cases cited *supra* note 3.

7. *See* Brian Lee, *New York Appellate Court Rules Search Warrant Cannot Compel Cellphone Unlocking by Fingerprint*, N.Y.L.J., at 1, (July 2, 2025); *People v. Manganiello*, 242 A.D.3d 41 (4th Dep't 2025).

8. *Id.*; *see also United States v. Brown*, 125 F.4th 1186 (D.C. Cir. 2024) (on the specific issue of mobile device and Fifth Amendment).

9. *C.C. v. A.R.*, 192 A.D.3d 654, 143 N.Y.S.3d 404 (2d Dep't 2021).

10. *Id.* at 654-55.

11. *See*, N.Y. R.P.C. 1.1 & cmt. 8, 1.2, 1.3, 1.4, and 5.3.

12. *See generally* Lauren Kahn et al., *AI Safety and Automation Bias: The Downside of Human-in-the-Loop*, Center for Security & Emerging Technology (Nov. 2024), https://cset.georgetown.edu/publication/ai-safety-and-automation-bias/.

13. *See* Joel Cohen & Douglas Nadjari, *Fighting the Demons of AI: New Battlegrounds*, N.Y.L.J. at 3 (Jan. 5, 2026), (discussing Complaint & Jury Demand, *Parks v. McCormac,* No. PAS-L-003672-20 (N.J. Super. Ct. Law Div. Passaic Co.)).

14. *Id.*

15. *See* Erika Collins & Ari Rutledge, *AI Programs Used by Employers May Lead to Title VII Discrimination Claims*, N.Y.L.J., at 7, (Aug. 11, 2023).

16. *See* N.Y.C. Admin. Code §§ 20-870 – 20-874 (2023)*; see also* Isha Marathe, *As AI's Role in Hiring Grows, Focus Turns to Understanding Its Decision-Making*, N.Y.L.J., at 5, (Oct. 21, 2022); Brad Raboin, *et al.*, *NYC's AEDT: A Growing Regulatory Arena and Efforts Seeking Clarity*, N.Y.L.J., at 4, (Dec. 8, 2022).

17. N.Y. Rules of Prof'l Conduct R. 8.4(g).

18. *See*, *e.g.*, Bruce A. Green & Rebecca Roiphe, *ABA Model Rule 8.4(g), Discriminatory Speech, and the First Amendment*, 50 Hofstra L. Rev. 543 (2022).

19. *See*, *e.g.*, N.Y. City Bar Comm. on Prof'l Ethics, Formal Op. 2020-4 (2020).

20. *See* Local Rules of the United States District Courts for the Southern and Eastern Districts of New York, Local Civil R. 6.1 (2026); *see also* Part 202. Uniform Civil Rules for the Supreme Court and the County Court, Section 202.8-c Sur-Reply and Post-Submission Papers (2026); *see also* U.S. District Court for the District of Maryland, Responses and Replies, https://www.mdd.uscourts.gov/content/responses-and-replies ("A surreply is not permitted to be filed without leave of court. *See* Local Rules 105.2.a") (last visited July 8, 2026). Prohibitions on sur-replies can also be found in the Individual Practices of certain judges – see Individual Rules of Practice of Judge Cathy Seibel (S.D.N.Y.) Rule 2.B.i; Individual Practices in Civil Cases, Jennifer E. Willis, U.S. Magistrate Judge (S.D.N.Y.), Rule II.A.

21. *See Nuvola LLC v. Wright*, 2025 Minn. Dist. LEXIS 5940, 2025 WL 4083694 (Minn. Dist. Ct. Hennepin Co. Nov. 21, 2025) (court did not sanction counsel, because they were not the ones to cite nonexistent cases, but was bothered by fact that counsel left court to be "last line of defense"); *Dec v. Mullin*, 171 F.4th 940, 947 (7th Cir. 2026) ("Though Dec's counsel described her efforts to mitigate future errors, she should have been more careful. Still, she took responsibility and showed contrition. *That opposing counsel also failed to catch these errors and bring them to our attention also gives us pause, albeit to a lesser degree*") (emphasis added).

22. *Billups v. Louisville Municipal School District*, Civ. Action No. 1:24-CV-74-SA-RP, 2025 U.S. Dist. LEXIS 262670, 2025 WL 3691871 (N.D. Miss. Dec. 19, 2025).

23. *Id.*

24. *Id.* at *8 (citing *Ferris v. Amazon.com Servs., LLC*, 778 F. Supp. 3d 879, 880-81 (N.D. Miss. 2025); *Elizondo v. City of Laredo*, 2025 U.S. Dist. LEXIS 140572, 2025 WL 2071072, at *3 (S.D. Tex. July 23, 2025)).

25. *See Withers v. City of Aberdeen*, 2026 U.S. Dist. LEXIS 126060, 2026 WL 1653484 (N.D. Miss. June 8, 2026).

26. *Id.*

27. *Id.*

28. *Id.*

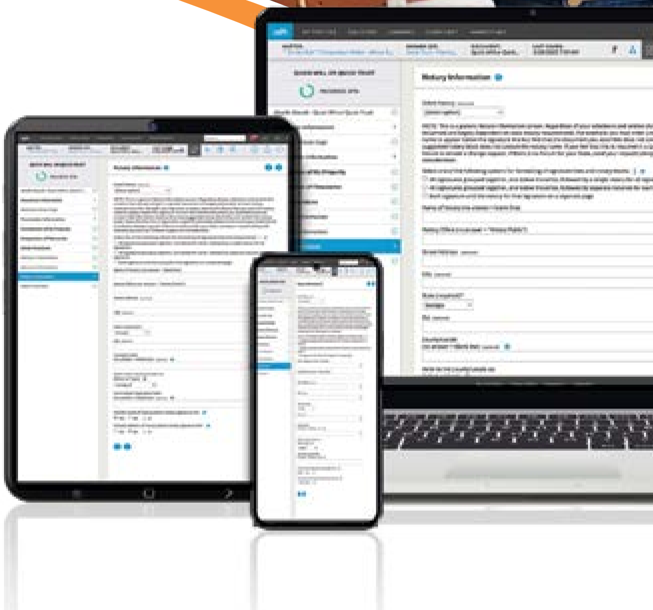
29. *In re Dom. P'ship of Torres Campos & Munoz*, 118 Cal.App.5th 1112, 342 Cal. Rptr.3d 227 (2026).

30. *Id.*

31. Note – this does not mean that an attorney must go on a research database and conduct their own first-hand research all over again, possibly at a senior attorney or partner-level billing rate, and after the client (in private firms or corporations) or the taxpayers (for public agencies) have already been billed for the research and time drafting and editing the submission. The attorney needing to cite-check as a supervisory matter could – if not already utilized as a potential course of action – request that the draft submission be given to them with copies of all cited cases, statutes and regulations pulled from verifiable and acknowledged research sources or databases – such that the attorney upon review is certain the cited material exists, is real and is properly characterized in the submission to the court. The same may be employed by judges in receiving draft opinions and orders from law clerks, if not already the practice in chambers.

32. 22 N.Y.C.R.R. § 130-1.1; N.Y. Rules of Prof'l Conduct R. 3.3, 4.1 and 5.3.

33. *Noland v. Land of the Free, L.P.*, 114 Cal. App. 5th 426, 336 Cal. Rptr. 3d 897 (2025) (sanctions ordered payable to court, but no sanctions payable to opposing counsel because they failed to alert court to fabricated citations in the other counsel's brief).



Testing the Bounds of E-Discovery: How Courts Have Analyzed Employer Control Over Personal Devices

By William C. Martucci and Maddie Bechtel

As the modern workplace continues to evolve, many organizations are adopting bring-your-own-device policies, enabling employees to use personal smartphones, tablets and laptops for work-related activities. These policies bring with them significant legal complexities – particularly in the context of employment litigation. Personal devices often contain a wealth of potentially relevant information, including text messages, emails and other digital communications that, if subject to e-discovery, can make or break a claim. When claims like discrimination, wrongful termination or retaliation arise, courts must assess the extent of an employer's control over its employees' personal devices to determine whether such data must be preserved and produced. As case law develops, courts are taking varied approaches to the discoverability of personal devices, prompting a closer examination of recent trends in the legal standards of different jurisdictions.

Electronically Stored Information Preservation and Production Requirements

Under the Federal Rules of Civil Procedure, parties engaged in litigation are under a clear and proactive duty to preserve and disclose electronically stored information relevant to the case. Rule 26 imposes an affirmative obligation on parties to provide, without awaiting a discovery request, any electronically stored information in their possession, custody or control that may support their claims or defenses. Following these initial disclosures, Rule 34 enables parties to formally request the production of electronically stored information that wasn't initially disclosed. Critically, Rule 37(e) addresses the consequences of failing to preserve digital information that should have been maintained in anticipation or during litigation. If such information is lost due to a party's failure to take reasonable steps, the court may impose sanctions, including adverse inference instructions or even dismissal of claims, depending on the severity of the prejudice caused.

In state courts, while procedural rules vary by jurisdiction, many have adopted discovery frameworks that closely mirror the Federal Rules of Civil Procedure, particularly regarding the scope of electronically stored information within a party's possession, custody or control. Like in federal court, parties are generally expected to preserve electronically stored information once litigation is anticipated and to engage in good-faith efforts to identify, retain and produce such information during discovery.

The phrase "possession, custody or control" is not explicitly defined in the Federal Rules of Civil Procedure, leaving its interpretation to the courts – and resulting in a patchwork of standards across and within jurisdictions. This divergence has created challenges in determining the scope of discovery obligations and a lack of reliable legal guidance on the matter.

Clear Cell Phone E-Discovery Outcomes at the Margins

While the legal standards governing possession, custody or control vary across jurisdictions, certain scenarios yield predictable outcomes. At the margins – where facts are clear and usage patterns are well-defined – courts typically reach consensus.

When Personal Devices Are Clearly Discoverable

Electronically stored information from employee cell phones is readily discoverable when the devices are issued by the employer. In *Owens v. Board of Supervisors of Louisiana State University and Agricultural and Mechanical College*,[1] the court stated that employers maintain constructive control over employment-related data stored on company-issued devices. When a device is employer-issued, the company can regulate device use, enforce data retention policies and direct employees to preserve or produce relevant communications. As such, company-issued devices fall squarely within the scope of discoverable electronically stored information under the Federal Rules of Civil Procedure.

When Personal Devices Are Clearly Not Discoverable

When employees' cell phones are not company-issued, and not used for business purposes, the outcome is similarly predictable. In *Muslims on Long Island, Inc. v. Town of Oyster Bay*,[2] the Eastern District of New York addressed a discovery dispute concerning the town's obligation to produce electronically stored information from advisory board members' personal cell phones. The underlying litigation involved allegations by Muslims on Long Island, Inc. that the Town of Oyster Bay had discriminatorily denied its application to expand a mosque. During discovery, Muslims on Long Island learned that the advisory board members did not use government-issued phones. Muslims on Long Island sought requested access to the board members' personal devices, asserting the potential for relevant communications. The town refused, and the group moved to compel discovery.

The court denied the motion to compel, finding that Muslims on Long Island had not met its burden to show that the personal devices were used for official business. The court emphasized that the group failed to identify any prior instances where the board members used personal phones for work-related communications. Additionally, declarations from board members stated that they did not have each other's phone numbers, did not maintain any board group texts and had not exchanged any messages concerning Muslims on Long Island's application.

This case demonstrates that the absence of work-issued devices or mere speculation of work-related use of personal devices is not enough to compel discovery. To make personal devices discoverable, a party must present specific, credible evidence that a personal device was used to conduct relevant business. Discovery must be targeted and grounded in factual support – not just possibility.

The Gray Area of Cell Phone E-Discovery

While some cases involving electronically stored information on employees' personal devices present clear outcomes – either plainly discoverable or clearly outside the scope of discovery – many fall into a legal gray area. In these middle-ground scenarios, courts have turned to a range of standards to determine whether such data falls within a party's "possession, custody or control" under the Federal Rules of Civil Procedure. These standards include the legal right standard, the legal right plus notification standard, the practical ability standard and a multi-factor approach. Federal district courts within each circuit have historically applied multiple standards, illustrating the fragmented and evolving nature of this critical area of e-discovery law. Even within each standard, courts continue to interpret and apply these standards differently, contributing to the uncertainty that litigants must navigate.

Legal Right Standard

Under this approach, courts focus strictly on legal entitlement. If a party has a legal right to obtain the data in question, courts applying this standard hold that the data is within the party's "possession, custody and control." This triggers the obligation to preserve, collect, search and produce the electronically stored information during discovery.

In *Weston v. Docusign, Inc.*,[3] the Northern District of California applied the legal right standard to determine whether a company had sufficient control over employees' personal devices to compel production of text messages. In the litigation, the plaintiffs alleged that Docusign misled investors and sought discovery of text messages between key executives related to the issue. The court found that Docusign's employment agreements and internal policies expressly authorized the company to access and retrieve business-related communications from employees' personal devices. Because Docusign had a contractual right to access the data via these agreements, the court held that the company had sufficient control under Rule 34.

Legal Right Plus Notification Standard

This standard builds on the legal right approach by adding a duty to inform. If the responding party has a legal right to obtain certain electronically stored information, it must preserve and produce it. Additionally, if the party knows of additional relevant information that it cannot legally access – such as data held by a third party – it must notify the requesting party of the existence of that data and identify the third-party custodian.

There is not currently a notable case applying the legal right plus notification standard in the context of electronically stored information and mobile devices, but this standard has been applied in other traditional discovery contexts where a dispute as to possession, custody, or control arises.

'Given the evolving and often inconsistent legal standards governing e-discovery, employers should take proactive steps to reduce the risk of discovery disputes and sanctions.'

Practical Ability Standard

Here, the focus shifts from legal entitlement to practical access. Irrespective of a formal legal right to the data, a responding party is required to preserve and produce any electronically stored information it can realistically obtain. Feasibility of access – rather than ownership or legal control – is the key consideration in determining whether the data falls within a party's discovery obligations.

In *Allergan v. Revance Therapeutics*,[4] the U.S. District Court for the Middle District of Tennessee applied this standard in an e-discovery dispute. Allergan, alleging trade secret misappropriation, sought communications among Revance employees from their personal devices. The court held that Revance did not have control over the devices, citing its bring-your-own-device policy and employee handbook, which did not grant the company the practical ability to search for, collect and produce data from employees' personal devices. Moreover, Allegan failed to show that Revance had previously accessed such data in the ordinary course of business or that employees were cooperating or had a financial stake in the litigation.

Although some courts continue to apply the practical ability standard, it has faced growing criticism from both courts and scholars for producing inconsistent and inequitable outcomes.[5] This criticism may signal a trend away from the standard's use in future cases.

Multi-Factor Approach

Federal courts are increasingly adopting a multi-factor approach to assess an employer's "possession, custody and control" over employees' personal devices for purposes of e-discovery. This analysis considers various factors depending on the court and circumstances. Courts typically consider factors such as:

- The frequency and extent of business use of the device.
- The employer's legal or practical access to the data.
- The existence of company policies governing personal device use.
- Whether the employer issued or subsidized the device.

This approach allows courts to focus on the contextual relationship between the employer, employee and data, acknowledging the realities of modern work environments and increasing reliance on personal devices for professional communication.

In *Miramontes v. Peraton, Inc.*,[6] the Northern District of Texas applied this multi-factor analysis to assess whether Peraton had control over text messages exchanged on an employee's personal phone. The issue arose from an employment discrimination claim, where the plaintiff, Carlos Miramontes, alleged that his termination was based on age and race. After sending a litigation hold letter including relevant text messages, and directly informing Miramontes's director of his duty to preserve emails related to the claims, Miramontes later discovered that his supervisor had deleted text messages relating to his termination.

The court rejected the legal rights test, explaining that "the realities of modern business require a fact-specific approach." To determine whether Peraton had a duty to preserve the text messages from Miramontes's supervisor, the court considered four factors:

- Whether the employer issued the devices.
- How frequently the devices were used for business purposes.
- Whether the employer had a legal right to obtain communications from these devices.
- Whether company policies address access to communications on personal devices.

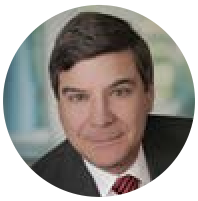
Although the messages were on a personal phone, the court found that Peraton had control over the electronically stored information because its employees routinely conducted business on their personal phones.

Under the multi-factor approach, when employees use personal devices for work and the employer is aware of this practice, courts are likely to find that the employer has sufficient control to trigger preservation duties.

Mitigating E-Discovery Risks Within Your Organization

Given the evolving and often inconsistent legal standards governing e-discovery, employers should take proactive steps to reduce the risk of discovery disputes and sanctions. The following strategies can help organizations navigate this complex landscape more effectively.

- Develop a comprehensive bring-your-own-device policy. Clearly articulate the employer's right to access work-related content stored on employees' personal devices. The policy should outline expectations for cooperation during litigation.
- Obtain employee consent. Secure written consent from employees acknowledging the employer's right to access, preserve and produce relevant data from personal devices in the event of litigation or investigation.
- Revise litigation hold procedures. Ensure that litigation hold notices explicitly instruct employees to preserve relevant communications and documents stored on personal devices, not just on company systems.
- Regularly review and update policies. Stay informed of the evolving legal standard and court decisions around e-discovery. Periodically review and update the employer's e-discovery policies to ensure legally compliant practices.

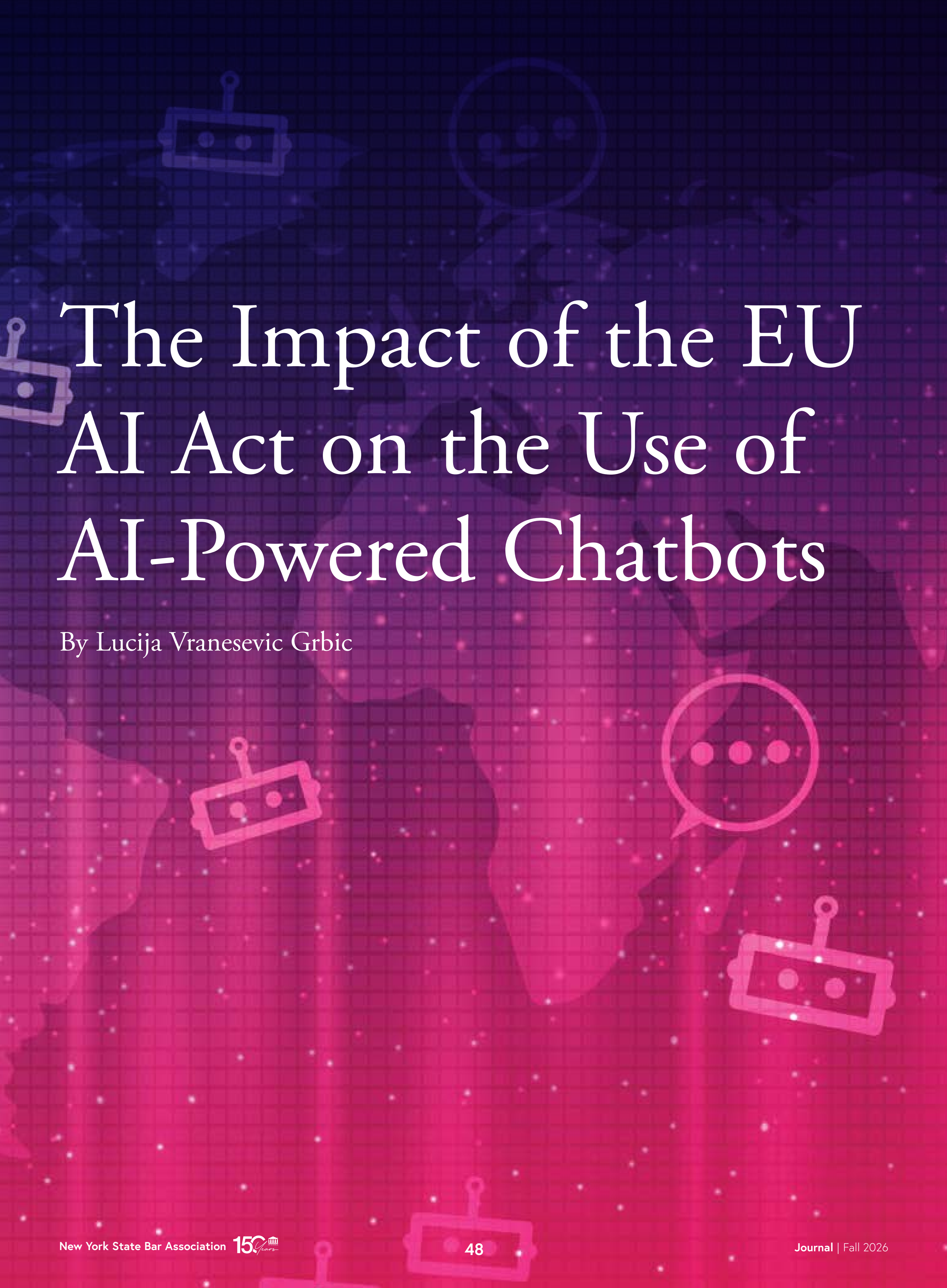


William C. Martucci practices nationally in business and employment litigation in the Shook, Hardy & Bacon LLP's New York and Washington, D.C., offices. He focuses on complex class action as well as business to business litigation, business torts and unfair competition. His jury work has been featured in The National Law Journal. This article appears in the Labor and Employment Law Journal, a publication of the Labor and Employment Law Section. For more information, please visit nysba.org/labor.

Maddie Bechtel is a litigation associate at Shook, Hardy & Bacon LLP, where her practice focuses on complex class action litigation. She earned her J.D. with honors from the University of Nebraska.

Endnotes

1. *Owens v. Bd. of Supervisors of La. State Univ. & Agric. & Mech. Coll.*, 695 F. Supp. 3d 750 (M.D. La. 2023).
2. *Muslims on Long Island, Inc. v. Town of Oyster Bay*, No. 25-CV-00428, 2025 WL 1582250 (E.D.N.Y. June 4, 2025).
3. *Weston v. Docusign, Inc.*, No. 22-CV-00824-WHO, 2024 WL 3446924 (N.D. Cal. July 15, 2024).
4. *Allergan, Inc. v. Revance Therapeutics, Inc.*, No. 3:23-CV-00431, 2025 WL 984792 (M.D. Tenn. Mar. 17, 2025).
5. *The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 Sedona Conf. J. 467, 528 (2016).
6. *Miramontes v. Peraton, Inc.*, No. 3:21-CV-3019-B, 2023 WL 3855603 (N.D. Tex. June 6, 2023).



The Impact of the EU AI Act on the Use of AI-Powered Chatbots

By Lucija Vranesevic Grbic

The expansion of large language model artificial intelligence has accelerated the global use of conversational AI for commercial purposes, often in the form of chatbots. Given the significant opportunities and risks associated with AI, it is not surprising that it caught the regulatory eye. For New York lawyers advising clients with cross-border operations, the rapid expansion of AI regulation has become an issue that deserves close attention. Companies that deploy AI systems often face compliance obligations outside the United States – particularly in jurisdictions like the European Union, where the regulatory framework is both comprehensive and extraterritorial. As New York practitioners support clients operating in foreign markets, it helps to know when international rules might come into play. A working understanding of the EU AI Act equips New York lawyers to provide strategic guidance, helping clients anticipate regulatory requirements, manage risk and avoid costly compliance missteps. Deep neural network systems add another challenge because their internal reasoning remains largely inaccessible to human understanding – a challenge commonly described as the black box problem.[1] Recent research identifies a key weakness in the use of these systems: Large language models are frequently treated as sources of information, despite not being designed to ensure factual accuracy. Rather than providing verified truths, these systems generate responses by predicting the most probable sequence of words based on their training data. This limitation introduces a new category of risk, referred to as careless speech.[2]

AI-related risks are closely tied to the architecture and operation of these systems. The EU Artificial Intelligence Act[3] entered into force on Aug. 1, 2024, and established an extensive horizontal framework governing AI-powered systems with extraterritorial reach. In this respect, it follows the approach taken by the General Data Protection Regulation,[4] the EU's main privacy law. This regulation requires organizations around the world to comply with EU data protection rules whenever they handle the personal data of EU users. The EU AI Act adopts a similar model. It applies regardless of where an AI provider is located or where a model was trained, so long as the system or its outputs are used within the EU.

Many businesses instinctively classify chatbots as low risk, assuming they only need to comply with basic transparency requirements. This assumption often oversimplifies the legal landscape. Not all chatbots function alike, and depending on their purpose, technical capabilities and influence on customer decision-making, certain models may trigger more stringent obligations than companies might expect.

How AI-Powered Chatbots Work – and the Risks Behind Them

The AI black box problem is frequently highlighted in academic literature. Users provide an input to the system, and the system produces an output. The processes between the submission of the input and the composition of the output give rise to several pitfalls associated with AI models.[5]

Simply put, chatbots and conversational agents driven by AI are software programs designed to mirror human-like dialogue. The underlying technology powering chatbots and conversational AI agents is based on natural language processing and deep learning.[6] Chatbots generally fall into two main groups: open domain chatbots and closed domain chatbots, but they can be further categorized using additional metrics such as knowledge domain, interact mode and goals.[7]

Potential risks of these chatbots generally fall into three areas: risks arising from the inputs they receive, their outputs and their commercial deployment. The first category is linked to the way large language models, which underpin chatbots, are trained. The importance of properly selecting the datasets used to train these systems is often overlooked, and the lack of transparency can create a negative feedback loop with no consistent standards for dataset quality.[8] For example, a 2024 study documented widespread large language model training data contamination and indirect data leakage.[9]

The second risk category relates to the output produced by AI systems. Back in 2023, the Italian Data Protection Authority ordered an urgent temporary limitation on the processing of personal data by a company operating an AI-power chatbot called Replika. By going through Replika's replies, the Italian Data Protection Authority concluded that, with no age verification or control procedures in place, the chatbot posed risks to minors and emotionally vulnerable individuals.[10]

The last risk category emerges once chatbots enter commercial use as the new generation of AI models benefits from more advanced capabilities and access to vast training data sets.[11] While these technological advancements should be welcomed, AI-powered chatbots are marketed as commercial products, reaching users with limited understanding of how such systems operate. The EU AI Act therefore underscores the importance of AI literacy and explainability for all relevant actors throughout entire value chain.

Compliance Deadlines

The implementation of the EU AI Act is based on a timeline set by the European Commission, starting from its going into effect on Aug. 1, 2024. The first binding requirements took effect on Feb. 2, 2025, when the chapters on general provisions and prohibited AI practices became enforceable.

The second wave arrived on Aug. 2, 2025, introducing governance obligations for general purpose AI models and activating provisions on relevant authorities; the EU AI office and national authorities then became fully operational.

The next important milestone arrived on Aug. 2, 2026, as the general date of application. From that point, compliance obligations for high-risk AI systems became fully enforceable. This is also when substantial fines – up to 35 million euros ($41 million) or 7% of global annual turnover – began to apply. The final phase follows in August 2027 when the AI Act is expected to be fully effective.[12]

Decoding the AI Act

Scope and Extraterritorial Reach

The AI Act doesn't exist in a vacuum; it seeks to stay aligned with the work of international organizations to help ensure that rules governing AI systems are interpreted uniformly. As Recital 12[13] reminds us, all AI systems share one common trait – the ability to infer. Whether they operate on a stand-alone basis or are tucked inside a larger product, their level of autonomy and ability to draw conclusions from data is what makes compliance important.

One interesting aspect is just how far the AI Act's reach extends. Recital 22[14] and Article 2[15] make this clear; the AI Act can apply even when an AI system doesn't physically enter the EU market. For example, if an EU-based company outsources certain activities to a provider located in a third country, and those activities have the potential to fall into the high-risk category, the act may still apply.

This captures the essence of the act's extraterritorial scope. Providers and deployers located outside the EU can still fall under the AI Act if their AI systems produce outputs intended for use within the EU or otherwise affect individuals located in the EU. While limited exceptions exist, the main principle is clear: If users in the EU can use your AI system, you shouldn't think twice about compliance with the AI Act.

The Risk Profile of Your Chatbot

The AI Act adopts a risk-based approach, classifying AI systems into four tiers: unacceptable risk, high risk, limited risk and minimal risk. Many chatbots fall under the limited-risk tier, which subjects them to transparency obligations. However, this is not a blanket rule. The precise risk classification depends on the chatbot's functions and areas of deployment.

Article 5 of the AI Act sets out a list of prohibited practices. These include AI systems that utilize subliminal or manipulative techniques, exploit individuals' vulnerabilities such as age, disability or financial situation, or carry out social scoring.[16] At first glance, it seems unlikely that a commercial chatbot could fall within these categories, but it is not impossible. Only a handful of cases show how AI chatbots can drift toward the kinds of behavior the AI Act aims to limit once it fully takes effect. Beyond Replika, mentioned above, EU regulators have also raised concerns about Character AI, an AI companion used widely in Europe, noting that emotionally immersive chatbots can influence users by simulating close relationships. A widely reported U.K. incident illustrates the risks – a young man who attempted to harm Queen Elizabeth II in 2021 told investigators that an AI "girlfriend" chatbot had encouraged him.[17]

The EU Commission guidelines on prohibited AI practices explain that Article 5(1)(a) covers cases where a chatbot presents false or misleading information in a manner that aims to or has the effect of deceiving individuals and distorting their behavior, particularly if the AI nature of the interaction has not been disclosed (para. 72).[18] The guidelines also note that chatbots, designed to use subliminal messaging techniques, exploit emotional dependency or specific vulnerabilities of customers in advertisements and may be considered as intentionally manipulating users (para. 82).[19] Another example is a chatbot promoting fraudulent products capable of causing severe financial harm (para. 89).[20] For the prohibition to apply, there must be a reasonably likely causal link between the chatbot's subliminal, manipulative, or deceptive technique and the user's resulting conduct (para. 84).[21]

Article 6 of the AI Act explains what counts as a high-risk AI system. This includes AI used as a safety component in products, or the AI itself being a product, covered by EU legislation and required to undergo a third-party conformity assessment, as well as the use cases listed in Annex III.[22] For example, systems implemented to profile individuals are treated as high risk. However, the act acknowledges that not every Annex III system will create the same degree of risk. A chatbot that nominally falls within an Annex III category will not be treated as highrisk if it does not pose a significant risk to a person's health, safety or fundamental rights, including situations where the system does not materially influence the individual's decisionmaking.

The AI Act also sets rules for limited risk AI systems in Chapters 4 and 5. For providers of AI-powered chatbots, Article 50 is particularly relevant: It requires that users must be informed whenever they are interacting with AI.[23]

By contrast, minimal risk AI systems are not regulated by the act. This category covers most AI tools currently available in the EU market – for example, spam-filtering tools or AI-powered video games.

Making Sense of AI Act Compliance

Compliance Duties for High-Risk AI

The AI Act primarily focuses on the responsibilities of providers of high-risk AI systems, regardless of whether

they are established within the EU or in a third country. As noted earlier, non-EU providers can be held accountable if the output of their high-risk AI systems is used within the EU.

Articles 8 to 15 in Section 2 of Chapter 3 explain the main duties that providers must follow throughout the entire lifecycle of a high-risk AI system. These responsibilities involve setting out a well-documented risk management process, implementing proper testing methods, ensuring appropriate data governance practices and maintaining detailed technical documentation. Providers must enable automatic logging to support record-keeping, human oversight and implement measures to ensure accuracy, resilience and cybersecurity. The Cyber Resilience Act[24] applies broadly to digital products, including software and connected devices that include AI-based functionalities, and readers should be aware that its scope may overlap with the AI Act.[25]

Additional rules for both providers and deployers are specified in Section 3. Article 16 requires providers to clearly state their business name or trademark, along with their contact information.[26] They must implement a quality management system in accordance with Article 17[27] and retain all required documentation for 10 years (as mandated by Article 18).[28] Providers are also obliged to preserve automatically generated logs (Article 19(1)),[29] issue an EU declaration of conformity under Article 47,[30] affix the CE (European Conformity) marking to their product and comply with the registration requirements in Article 49(1).[31] They must persistently address any problems that arise, cooperate with relevant national authorities and ensure that their quality management system remains effective.

Non-EU providers must be aware of one additional requirement under Article 22.[32] Before their AI system is placed on the EU market, they need to appoint an authorized representative established within the EU. This representative acts as the provider's local point of contact and is responsible for collaboration and communication with competent supervisory authorities.

Although this regulation mainly addresses providers, Section 3 (Chapter 3) stipulates obligations for other key players in the AI value chain, including importers, distributors, deployers and suppliers. These compliance requirements apply to anyone who puts a high-risk AI system on the market under their own trade name or registered trademark, makes significant alterations that keep the system within the high-risk category, or remodels the system's main purpose in a manner that triggers categorization as high risk under Article 6.

Transparency Obligations for Providers and Deployers of Certain AI Systems

Chapter 4 outlines transparency requirements for providers and deployers of certain AI systems. As highlighted earlier, Recital 132[33] and Article 50[34] are especially significant for providers and deployers of AI-driven chatbots as they impose an obligation to clearly inform users whenever they are interacting with an AI system, whenever content has been generated or altered by AI, and whenever biometric categorization or emotion recognition features are being used.

In essence, comprehensive documentation supplied by developers on how an AI model functions is central to meeting transparency obligations. Although the AI Act does not specify how documentation should look, tools such as model cards, data set sheets and transparency reports can help explain how a system was built, trained and tested.[35]

GPAI Compliance Requirements

Chapter 5 governs Global Partnership on Artificial Intelligence models and introduces a two-tier compliance structure: baseline obligations for all their model providers, and an additional set for models with systemic risk. Considering the difficulty of assigning a single risk classification to these models – mainly because they can be adapted to a wide range of use cases – it is unsurprising that the AI Act dedicates a separate chapter to their regulation.[36]

The requirements for the first category are set out in Articles 53[37] and 54.[38] Namely, Global Partnership on Artificial Intelligence providers must maintain detailed records of how their systems are developed and tested, and they are required to share the relevant technical documentation with businesses that integrate their model, while still safeguarding their intellectual property rights. This excludes open-source AI models unless they can be classified as models with systemic risks. Providers may also rely on published codes of practice to demonstrate compliance. In addition, Article 54 requires providers established outside the EU to appoint an EU-based representative responsible for ensuring adherence to all applicable obligations and for maintaining cooperation with competent authorities.[39]

Providers in the second category must comply with an additional set of requirements. These include conducting model evaluations using standard protocols and tools, assessing and minimizing potential systemic risks and reporting incidents to the EU AI office and national authorities. They are also obliged to ensure an appropriate degree of cybersecurity protection for the model and the physical infrastructure on which it operates.

Conclusion

The main obstacle to AI Act compliance is not implementation but interpretation. The EU's AI office shall incentivize the creation of voluntary codes of conduct for AI systems to promote adherence to relevant standards and industry best practices (Article 95).[40] A 2026 study examined attitudes toward the codes of conduct under Article 95 and found that participants expressed a positive overall sentiment.[41]

Although the AI Act interacts with other EU digital regulations, it establishes its own distinct compliance regime that cannot simply be folded into existing General Data Protection Regulation or cybersecurity processes. Businesses should begin by creating a full inventory of all AI systems in use and classifying them under the act's fourtier risk framework, as well as under the two-tier Global Partnership on Artificial Intelligence structure. Once this baseline is in place, organizations can address the remaining compliance tasks: reviewing and updating AI governance frameworks, conducting risk assessments, meeting AI literacy obligations and resolving areas where the AI Act overlaps with other EU rules.

The road to AI compliance in Europe begins with an understanding of what the EU AI Act requires, and that obligation extends well beyond EU borders. Any lawyer advising a company that sells into the EU market, processes EU-based user data, deploys AI tools across multiple jurisdictions or supports clients expanding abroad will need to understand this law. For lawyers in these roles, it isn't just "European law" anymore – it's simply part of doing business today.

Lucija Vranesevic Grbic is the founder of a boutique law firm in Belgrade, Serbia, advising domestic and international clients in corporate, IT, contract and sports law. This article appears in a recent issue of One on One, the publication of the General Practice Section. For more information, please visit nysba.org/gp.

Endnotes

1. Georgios Pavlidis, *Unlocking the Black Box: Analysing the EU Artificial Intelligence Act's Framework for Explainability in AI*, 16 Law Innovation & Tech. 293, 293 (2024).

2. Sandra Wachter, Brent Mittelstadt & Chris Russell, *Do Large Language Models Have a Legal Duty to Tell the Truth?* 11 R. Soc. Open Sci. 240197 (2024), https://doi.org/10.1098/rsos.240197.

3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), *OJ L 2024/1689*.

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. L 119.

5. Sara Migliorini, *'More than Words': A Legal Approach to the Risks of Commercial Chatbots Powered by Generative Artificial Intelligence*, 15 Eur. J. Risk Reg. 719, 720 (2024).

6. Avyay Casheekar et al, *A Contemporary Review on Chatbots, AI-Powered Virtual Conversational Agents, ChatGPT: Applications, Open Challenges and Future Research Directions*, 52 Comput. Sci. Rev. 100632 (2024), https://doi.org/10.1016/j.cosrev.2024.100632.

7. Sonali Uttam Singh and Akbar Siami Namin, *A Survey on Chatbots and Large Language Models: Testing and Evaluation Techniques*, 10 Nat. Lang. Process. J. 100128 (2025), https://doi.org/10.1016/j.nlp.2025.100128.

8. Migliorini*, supra* note 5, at 723-724.

9. Simone Balloccu et al., *Leak, Cheat, Repeat: Data Contamination and Evaluation Malpractices in Closed-Source LLMs*, In Proceedings of the 18th Conference of the European Chapter of the Association for Computational Linguistics, Vol. 1, St. Julian's Malta, Association for Computational Linguistics, 2024, p. 67.

10. *Provvedimento del 2 febbraio 2023 (9852214)*, Available in English: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9852214#english.

11. Migliorini*, supra* note 5, at 724.

12. European Parliament, *AI Act Implementation Timeline*, https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/772906/EPRS_ATA(2025)772906_EN.pdf.

13. Artificial Intelligence Act*, supra* note 3, at Recital 12: "A key characteristic of AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data."

14. *Id. at* Recital 22: "To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and deployers of AI systems that are established in a third country, to the extent the output produced by those systems is intended to be used in the Union."

15. *Id.at* Art. 2 (Scope).

16. *Id.at* Art. 5 (Prohibited AI practices).

17. Pieter Haeck, *My AI Friend Has EU Regulators Worried*, Politico (Aug. 21, 2025), https://www.politico.eu/article/ai-friends-experts-worried-artificial-intelligence-chatbot-digital-technology/.

18. Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), *C (2025) 5052 final, para.* 72: "By contrast, the prohibition in Article 5(1)(a) AI Act has a much more limited scope…".

19. *Id*. at para 82: "Article 5(1)(a) AI Act applies to AI systems deploying the above-mentioned techniques and having as a first scenario 'the objective to materially distort the behaviour of a person or a group of persons'."

20. *Id*. at para. 89: "Financial and economic harm may encompass a range of adverse effects, including financial loss, financial exclusion, economic instability. For example, a chatbot that offers fraudulent products that cause significant financial harms."

21. *Id.* at para 84: "A plausible/reasonably likely causal link between the subliminal, purposefully manipulative or deceptive technique deployed by the AI system and its effects on the behaviour is, however, always necessary for the prohibition to apply."

22. Artificial Intelligence Act*, supra* note 3, at Art. 6.

23. *Id*. at Art. 50: "Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use."

24. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847.

25. Marta Beltrán, *AI Algorithms Under Scrutiny: GDPR, DSA, AI Act and CRA as Pillars for Algorithmic Security and Privacy in the European Union*, 148 Computs. & Sec. 104085, at 6 (2025).

26. Artificial Intelligence Act*, supra* note 3, at Art. 16.

27. *Id*. at Art. 17: "Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects…".

28. *Id.* at Art. 18: "The provider shall, for a period ending 10 years after the high-risk AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities…".

29. *Id.* at Art. 19(1): "Providers of high-risk AI systems shall keep the logs referred to in Article 12(1), automatically generated by their high-risk AI systems, to the extent such logs are under their control. Without prejudice to applicable Union or national law, the logs shall be kept for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in the applicable Union or national law, in particular in Union law on the protection of personal data."

30. *Id.* at Art. 47: "The provider shall draw up a written machine readable, physical or electronically signed EU declaration of conformity for each high-risk AI system, and keep it at the disposal of the national competent authorities for 10 years after the high-risk AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the high-risk AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be submitted to the relevant national competent authorities upon request…".

31. *Id.* at Art. 49(1): "The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008."

32. *Id.* at Art. 22: "Prior to making their high-risk AI systems available on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union."

33. *Id.* at Recital 132: "Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. In certain circumstances, the use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems and subject to targeted exceptions to take into account the special need of law enforcement."

34. *Id.* at Art. 50 (Transparency obligations for providers and deployers of certain AI systems).

35. Konstantinos Kalodanis et al, *Enhancing Transparency in Large Language Models to Meet EU AI Act Requirements,* PCI '24: Proceedings of the 28th Pan-Hellenic Conference on Progress in Computing and Informatics, 2025, https://doi.org/10.1145/3716554.3716597.

36. Oskar J. Gstrein, Noman Haleem and Andrej Zwitter, *General-Purpose AI Regulation and the European Union AI Act*, 13 Internet Policy Rev., no. 3, 2024, https://doi.org/10.14763/2024.3.179.

37. Artificial Intelligence Act*, supra* note 3, at Art. 53 (Obligations for providers of general-purpose AI models).

38. *Id.* at Art. 54 (Authorised representatives of providers of general-purpose AI models).

39. *Id.* "Prior to placing a general-purpose AI model on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union."

40. *Id. at* Art. 95 (Codes of conduct for voluntary application of specific requirements).

41. Matthias Wagner et al, *AI Act High-Risk AI Compliance Challenge and Industry Impact: A Multiple Case Study*, 194 Inf. Software Tech. 108067 (2026), https://doi.org/10.1016/j.infsof.2026.108067.

SPONSORED ARTICLE

Cyber Risk and Law Firms: What You Don't Know Could Cost You

By Mike Mooney

Cyberattacks against law firms are becoming more widespread, sophisticated and costly. Law firms are especially attractive targets: They hold valuable, confidential client data – including personally identifiable information (PII), protected health information (PHI) and payment card or banking information (PCI) – along with sensitive intellectual property, business intelligence and details on significant business transactions. Add in a heavy reliance on email and, in many firms, inconsistent cybersecurity practices. The result? A combination of high value and real vulnerabilities spurring breaches that carry major business consequences.

According to the American Bar Association's Cybersecurity Tech Report, nearly one in three law firms have experienced a security breach, yet only 40% of law firms report having cyber liability insurance. With law firm breaches costing an average of $5.08 million, as cited in IBM's Cost of a Data Breach Report 2026, the financial stakes of a breach far outweigh what most firms are prepared to absorb. Mitigating cyber risks starts with understanding the nature of these threats and closing gaps before they're tested.

Most Common Cybersecurity Threats in the Legal Industry

Industry studies and real-world claims point to a consistent set of cyber threats driving law firm losses. Understanding these is the first step toward closing the gaps in your firm's defenses.

The top five cybersecurity threats based on the number of claims we see are:

1. Ransomware attacks that lock down a firm's IT systems until a ransom is paid.
2. Business email compromise, such as spoofing, that impersonates trusted contacts to access sensitive information.
3. Funds transfer fraud, resulting from spoofing emails that direct wire transfers to cybercriminals instead of the intended accounts.
4. Hacking and unauthorized access where cybercriminals tap into sensitive information that should be under counsel's care, custody and control.
5. Staff mistakes, including employees manipulated by phishing and social engineering, or unintentionally exposing data through remote work without proper firewalls or secure Wi-Fi.

Beyond these top threats, third-party and vendor vulnerabilities are another common risk vector putting firms, and any client information those vendors can access, in jeopardy.

Cyber Coverage Misconceptions Putting Law Firms at Risk

Despite these growing threats, many firms continue to operate under risky misconceptions about cyber insurance – creating a false sense of protection and leaving them exposed to serious risks.

"Our general liability policy covers cyber risks."

Fact: Most commercial general liability policies explicitly exclude cyber-related losses.

"Crime insurance will protect us from cyberattacks like phishing or hacking."

Fact: Traditional crime policies typically cover theft and fraud, not cybercrime or broader cybersecurity events.

"Our lawyers' professional liability policy already includes cyber coverage."

Fact: Lawyers' professional liability policies may provide limited cyber coverage for third-party losses, but about 70% of financial damages are first-party losses, such as IT response, forensics, and data recovery costs. These are generally not covered, as LPL responds only when there is a demand for money or services.

"Business interruption coverage will respond to a cyber incident."

Fact: Traditional business interruption or business income coverage is triggered by physical damage to insured property, leaving law firms on their own to

absorb the cost of lost billable hours for days or even weeks following a cyber incident.

"We're too small to need separate cyber coverage."

Fact: Cybercriminals frequently target small and mid-sized law firms due to their limited IT resources, leading to even greater risks that require dedicated protection.

These misconceptions highlight not only how easily firms can overestimate their existing insurance coverage, but also why there is a bona fide need for dedicated cyber protection.

Proper Cyber Protection for Law Firms

A dedicated cyber liability policy – designed to cover exposures that general liability, crime and professional liability policies don't – is a critical piece of a comprehensive risk management strategy. While there are many standard policies on the market, law firms are best positioned to manage their unique cyber exposures with coverage built specifically for the legal industry.

To address the specific risks facing law firms, the NYSBA Insurance Program, administered by USI Affinity, offers comprehensive cyber liability insurance that enables legal professionals to effectively prepare for, respond to and recover from cyber incidents. This includes:

- Stand-alone cyber liability coverage built specifically for law firms, rather than a limited add-on to a general liability, crime or lawyers' professional liability policy.
- Protection against the threats law firms actually face, including ransomware, social engineering, wire fraud and data breaches.
- First-party coverage for costs such as IT forensics, data recovery, breach notification, crisis communications and lost billable hours.
- Third-party coverage for costs arising from claims brought by clients or regulators after a breach, including legal defense, settlements and regulatory fines or penalties.
- Support before, during and after an incident, including access to breach response resources such as forensics, legal counsel and recovery assistance.
- Flexible coverage tailored to your firm's operations and risk profile that can scale with your firm's size and the sensitivity of the data you hold.

Insurance alone isn't a complete risk management strategy, but the right cyber liability protection becomes part of your firm's broader defense, working alongside key internal practices that reduce your overall exposure.

Additional Risk Management Strategies

Beyond insurance, day-to-day practices play a critical role in reducing cyber risk. Taking these action steps can help prevent an incident and limit the damage if one occurs.

- Conduct a comprehensive risk analysis.
- Adopt strong data encryption practices.
- Implement multi-factor authentication (MFA).
- Enforce strong password management policies.
- Limit user access to only the data and systems necessary for each role.
- Regularly update software and apply security patches.
- Provide ongoing employee training and education.
- Develop and maintain an incident response plan.

None of these practices are groundbreaking, but consistently applying them strengthens a firm's preparedness and speeds recovery if or when an incident occurs.

Closing the Gap

No set of safeguards can eliminate cyber risk entirely. Pairing strong internal practices with the right cyber insurance coverage is what protects your firm when prevention isn't enough. Understanding your actual exposure, not just what you assume is covered, is foundational to keeping a single incident from becoming a firm-defining loss.

If you're interested in speaking with a cyber insurance specialist to make sure your coverage matches your firm's actual risk, visit nysbainsurance.com.

Mike Mooney is senior vice president and professional liability practice leader at USI Affinity, a national leader specializing in business insurance solutions for the legal profession. USI Affinity is proud to be the NYSBA Platinum Member Benefit Partner and the insurance partner of choice for law firms of all sizes. Mooney can be reached at mike.mooney@usi.com.

It's the Truth – Just Not the Whole Truth

The Attorney Professionalism Committee invites our readers to send in comments or alternate views to the responses printed below, as well as additional hypothetical fact patterns or scenarios to be considered for future columns. **Send your comments or questions to: NYSBA, One Elk Street, Albany, NY 12207, Attn: Attorney Professionalism Forum, or by email to journal@nysba.org.**

This column is made possible through the efforts of NYSBA's Committee on Attorney Professionalism. Fact patterns, names, characters and locations presented in this column are fictitious, and any resemblance to actual events or to actual persons, living or dead, is entirely coincidental. These columns are intended to stimulate thought and discussion on the subject of attorney professionalism. The views expressed are those of the authors, and not those of the Attorney Professionalism Committee or NYSBA. They are not official opinions on ethical or professional matters, nor should they be cited as such.

To the Forum:

We all know that when we draft documents if we discover scrivener's errors or mistakes of fact that deviate from what was agreed upon by the parties, we are required to correct those. But I have what is arguably a more complicated question.

I represent one of two individuals who are looking to form a corporation or limited liability company. My client will provide the expertise and will manage the entity, while the other individual will be an investor without much operating connection to the business. Once the entity is formed, they expect to raise additional money by selling shares in a private placement.

All the business is expected to be conducted in New York; both of the founders are New York residents and it is likely that the majority of the subsequent investment money will also come from New York residents. Accordingly, one might think that the most logical place to form the entity is under New York law.

However, in the interest of giving my client the greatest degree of flexibility and protection against being sued over how he manages the entity as a director or manager (as the case may be) I would like to put in the governing documents a provision that waives the applicable fiduciary duties to the greatest extent possible. I can achieve more of what I want in that regard under Delaware law than under New York law, and I can achieve even more under Texas law.

Accordingly, I would like to suggest to the other founder's lawyer that we form the entity in either Delaware or Texas. I don't want to disclose the aforementioned reason for why I want to do this, but rather, if asked why, I can answer that Delaware has the most established jurisprudence for business entities or that Texas is trying very hard to accommodate companies and attract them to incorporate there and use its courts. While that might not be the "whole truth," I believe that both of those explanations would be true and of non-trivial significance.

In the same vein, I would rather use an LLC if I determine that it is more flexible in this connection than a corporation. My preferred explanation would be that using an LLC plainly will allow the business to be run as a pass-through for tax purposes and, if and when it becomes preferable to use an S corporation or even a regular C corporation, an LLC is able to elect that tax treatment. Again, this is completely truthful and substantive, but not a disclosure of what really matters to me and my client.

So, my first question is whether there is anything in the Rules of Professional Conduct or otherwise that precludes me from doing what I want without making a full disclosure to the other founder's lawyer that the fiduciary protection will be significantly less than with a New York corporation.

But wait, it's more complicated than that. The other founder wants to have a right to purchase whatever New York real property the entity will acquire. My client does not like this element of the transaction but decided that he cannot fight it. You can imagine my barely concealed glee when I received the document drafted by the other founder's lawyer providing for a 25-year option. Boom.

I think that that option could well be void under the Rule Against Perpetuities.

So, my second question concerns the misimpression that the other founder's lawyer has created for himself without any fault, action or influence on my part: Am I required to inform him that this provision that he has proposed, which I know is so important to his client, is or may be a legal nullity?

Sincerely,
Jen Nanigans

Dear Ms. Nanigans:

The way to think about this is analogous to how traffic signals work.

The Green Light

First, consider the New York Rules of Professional Conduct. Three provisions are relevant:

- RPC 4.1 states, "In the course of representing a client, a lawyer shall not knowingly make a false statement of fact or law to a third person."
- RPC 8.4(c) states that a lawyer "shall not … engage in conduct involving dishonesty, fraud, deceit or misrepresentation."
- RPC 8.4(h) states that a lawyer "shall not … engage in any other conduct that adversely reflects on the lawyer's fitness as a lawyer."

What about *omissions* such as yours? RPC 4.1 makes no mention of omissions. This is not an accident, as Professor Simon in the *New York Rules of Professional Conduct Annotated* points out in Section 4.1:2:

> Rule 4.1 generally applies only to affirmative statements, not to omissions. … New York declined to adopt ABA Model Rule 4.1(b), which states: "In the course of representing a client, a lawyer shall not knowingly … (b) fail to disclose a material fact when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6."

In fact, even the Model Rule provision that New York declined to adopt appears only to apply when the omission assists in the commission of a crime or the perpetration of a fraud, neither of which is present on your facts, and so, *a fortiori*, RPC 4.1 would not cover your situation.

Two of the ethics opinions cited and summarized by Professor Simon in Section 4.1:1 provide helpful illustrations:

- In Nassau County 13-4 (2013),[1] a defense lawyer in a medical malpractice case, who asked the plaintiff's lawyer to dismiss the case against individual physicians and settle only with the hospital, had no duty to disclose that this would relieve the physicians of an obligation to report the suit to a medical database, even if the dissemination of that kind of information to the public might have mattered to the plaintiff.

- In Erie County 12-02 (2012),[2] although a house seller's neighbor asked the seller's lawyer to inform the buyer that he (the neighbor) was a registered sex offender, the lawyer had no obligation to do so, at least as far as RPC 4.1 was concerned.

Next, consider the nature of negotiations, the setting in which your situation arises.

Comment [2] to RPC 4.1 states: "Under generally accepted conventions in negotiation, certain types of statements ordinarily are not taken as statements of material fact."

The comment gives as examples estimates of price or value and statements of a party's intentions.

One might reasonably extend that reasoning to infer that a statement explaining why a party or counsel desires a certain provision should not be taken as an indication that there are no other, unstated reasons in addition. Except where there is a relationship of trust, no party to a commercial negotiation should assume that the other parties are duty-bound to disclose their goals and thought processes in full.

RPC 8.4(c) has a more comprehensive listing of improper behavior than that contained in RPC 4.1, and RPC 8.4(h) is a catch-all that prohibits "other conduct that adversely reflects on the lawyer's fitness as a lawyer." We address these two provisions together.

One always must be careful not to reason from a converse, but because the decision not to cover omissions in RPC 4.1 was deliberate, as indicated above, I would apply the canon of construction that the specific controls the general (*generalia specialibus non derogant*) and conclude that neither RPC 8.4(c) nor RPC 8.4(h) imposes with the left hand a prohibition waived by the right hand in RPC 4.1. For this reason, we do not believe that even the catch-all RPC 8.4(h) would require a contrary result.

The Yellow Light

You should be honest with yourself to make sure that what you will have omitted does not drag the statement across a sometimes imperceptible line so as to make the statement false or deceptive, which would violate both RPC 4.1 and 8.4(c). To give you a sense of the kind of statement that would cross the line, suppose that you heard a college dean clucking proudly that his seniors had received admissions letters from 10 elite law schools, but what the dean did not reveal was that it was only two individuals who'd applied to all of those schools. Or consider a manufacturer's facially impressive durability claim that 80% of the equipment that it had sold over the previous decade was still operational and in use, which failed to mention that well over half of the equipment that it had sold in the previous decade consisted of units that it in fact had sold in the past three years.

Though everyone might not agree, what you are doing is not necessarily deceptive in that way.

Unlike the statements of the dean or the manufacturer above, which are couched in clever phrases designed to make the listener jump to an incorrect conclusion, your statement expressing and explaining a preference for Delaware law is direct, truthful and material. Many entities with no commercial contact with Delaware are organized under Delaware law rather than locally. The case for Texas may be a little bit harder to justify but has some merit to it. And LLCs certainly are more flexible than corporations.

As to the issue of whether your statement is misleading by omission, any lawyer representing a founder or investor should know that fiduciary responsibilities within business organizations vary state by state and entity by entity. Hence, your declining to disclose that you are looking for what in your opinion is advantageous to your client is acceptable in the same way as would be proposing that a contract include an arbitration clause for all the commonly cited reasons (such as simplicity and low cost) without also disclosing that your research convinces you that an arbitrator will likely be more favorably disposed toward your client than a jury may be.

Your second question is easier to address, at least on a technical level. Opposing counsel who wants an enforceable agreement should know that there exists something called the rule against perpetuities and that it is still the law in some jurisdictions. We would feel the same way regarding a range of relatively well-known issues and doctrines such as usury or the permissible scope of non-compete agreements, and maybe even as to more arcane considerations like the possibility that a lawyer who is careless or unknowledgeable can maneuver a client into a violation of the securities laws that could give investors a "free option" to invalidate an agreement.

You need to be aware, however, that your objectives could turn out to be at cross-purposes. For example, in New York a perpetuities violation invalidates the offending contractual provision, but it may be that in the state whose fiduciary duty law you prefer, a perpetuities violation would be reformed to conform with the rule rather than being invalidated completely. If you have been pressing to organize the entity in the other state in order to achieve what you want on the fiduciary duty front, you may have a tough explanation as to why you suddenly have found religion and prefer the law of New York to govern an option contract regarding real estate. So, you should choose up front what is important to you and in so doing be sure not to cross the line into active deception.

The Light May Be Turning Red

This is more of a commercial consideration than a strictly legal or ethical directive, but it may be the most important element that you need to consider.

Issues that seem to have been ignored or resolved can have a pesky tendency to arise at inconvenient times. If the lawyer on the other side asks you explicitly how fiduciary duties compare in New York and Delaware or within an LLC relative to within a corporation, or says something offhand like, "I assume that there is no significant legal difference," you can respond by saying that it's not your responsibility to educate counsel, or you can outline what you know with the caveat that in that regard you represent only your own client and are not giving counsel legal advice. Of course, counsel and the client may then realize that you were directing them down a path that leads over a precipice, and you should not be shocked if counsel advises the client not to do business with you and your client or this sequence of events sours the proposed business relationship or even kills it.

Indeed, in certain settings where the practitioners tend to know each other and to encounter each other frequently – tax law and small town practice both come to mind – one really must avoid getting a reputation as someone who hides the ball, not just because the others are likely to discover the missing information but also because one's long-term effectiveness can depend on being able to forge consensus where the law may not be all that clear, and a lawyer with a reputation for opacity and hidden agendas may find others unwilling to accept arguments about the feasibility and merits of a transaction or a resolution.

If all of this – especially how to balance the RPC conclusions against the commercial risks – leaves you more confused than when you started, one final bit of advice would be to ask yourself whether you could explain what you were doing to your parents or your children. Or, failing all else, you can apply the wisdom that Justice Stewart articulated in his concurrence in *Jacobellis v. Ohio* regarding the definition of hard-core pornography: "I know it when I see it."[3]

Sincerely,
The Forum, by
Robert Kantowitz, robert.kantowitz@gmail.com
Vincent J. Syracuse, VSyracuse@thsh.com
Jean-Claude Mazzola, jeanclaude@mazzolalindstrom.com

QUESTION FOR THE NEXT FORUM

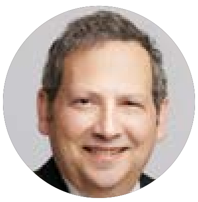
To the Forum:

I represent a defendant in an employment matter in which she is accused of sexually harassing the plaintiff, a subordinate. The details are extremely salacious and the case has garnered some attention in the local press because my client is herself an extremely experienced and well-regarded litigator. I am flattered that she has chosen me to represent her. However, she has expressed a desire to be very involved in the prosecution of her case.

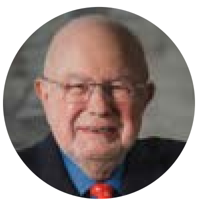
The matter is in the discovery phase and depositions have been scheduled. She has told me that she would like to question the opposing party at his deposition. Her rationale is that because she was there at the time of the alleged incident, she is in the best position to ask relevant questions. She does have a keen eye for detail and is more than experienced to be able to effectively question the witness. Privately, I am concerned that she wants to do the questioning in order to intimidate the plaintiff. I am also concerned that my client acting as both a lawyer and a party might violate ethical rules regarding contact between represented parties.

Am I ethically permitted to allow my client to conduct the questioning at the deposition of the opposing party?

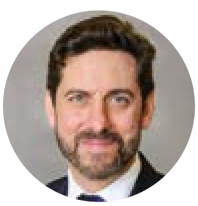
Sincerely,
PRO Advocate



Robert Kantowitz, a tax and business lawyer for over 45 years, heads the tax practice at Sterlington, PLLC, where his practice focuses on all matters of income tax law, including mergers and acquisitions and capital raising. He previously worked for many years in banking doing capital markets and cross-border financings. Kantowitz has been a member of the Committee on Attorney Professionalism for many years.



Vincent J. Syracuse is a founding partner of Tannenbaum Helpern's litigation and dispute resolution practice and has 50 years of experience in litigation. He received the New York State Bar Association's Sanford D. Levy Professional Ethics Award and has chaired NYSBA's program on ethics and civility for over 20 years. He co-chairs the Ethics Committee of the Commercial and Federal Litigation Section. He has been a co-author of the Attorney Professionalism Forum since 2012, which was published in a collection in 2021.



Jean-Claude Mazzola is founding partner of Mazzola Lindstrom LLP with over 25 years of experience as a commercial litigator. He is chair of the New York State Bar Association's Committee on Attorney Professionalism.

Endnotes

1. Nassau Co. Bar Ass'n Comm. on Prof'l Ethics, Op. 13-4 (2013), https://www.nassaubar.org/ethics-opinion/2013-4/.

2. Bar Ass'n of Erie Co. Comm. on Prof'l Ethics, Op. 12-02 (2012), https://drive.google.com/file/d/17qLG2XFUg5iE0NiI3LseeTgHSZZ2jHqT/view.

3. *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964).

Official U.S. Postal Service Annual Filing Statement


UNITED STATES POSTAL SERVICE · Statement of Ownership, Management, and Circulation (All Periodicals Publications Except Requester Publications)


UNITED STATES POSTAL SERVICE · Statement of Ownership, Management, and Circulation (All Periodicals Publications Except Requester Publications)

MEMBERS OF THE HOUSE OF DELEGATES

First District
- Mohammed Akber Alam
- Arthur H. Aufses, III
- Simeon H. Baum
- Scott M. Berman
- Karen J. Bernstein
- Delilah R. Chamlin
- Jai K. Chandrasekhar
- Vincent Ted Chang
- David M. Cohn
- Frettra Miller De Silva
- Jacqueline Jamin Drohan
- Bart J. Eagle
- Rosa Maria Ertze
- Nigel Ignatius Farinha
- Margaret J. Finerty
- Aegis J. Frumento
- Janine Malika Gilbert
- Taa R. Grays
- Kaelyn Elizabeth Gustafson
- Noah J. Hanft
- Barbara J. Hart
- Heather A. Hatcher
- Hon. Helena Heath
- Helene R. Hechtkopf
- Scott Harriman Henney
- Andre R. Jaglom
- * Seymour W. James, Jr.
- Marcella M. Jayne
- Brian Kerr
- James B. Kobak, Jr.
- Adrienne Beth Koch
- Diane F. Krausz
- Anne Louise LaBarbera
- Mark Landau
- * Glenn Lau-Kee
- * Bernice K. Leber
- Jiyeon Lee-Lim
- Susan B. Lindenauer
- Margaret T. Ling
- Thomas J. Maroney
- Hon. Kathleen C. Waterman-Marshall
- Michael J. McNamara
- Abja Uttam Midha
- †* Michael Miller
- Ronald C. Minkoff
- Russell D. Morris
- Ivonne Norman
- Michael P. O'Brien
- John A. Owens, Jr.
- Jill Pilgrim
- Rory J. Radding
- Alexander Rayskin
- Michael P. Regan
- Anastasia T. Rockas
- Jorge Rodriguez
- Jeanne Wilms Roig-Irwin
- Tracey Salmon-Smith
- Anne B. Sekel
- Diana S Sen
- Elizabeth Jean Shampnoi
- Jennifer Luise Shufelt
- James R. Silkenat
- Brooke Erdos Singer
- Barry Skidelsky
- Matthew J. Skinner
- Asha Smith
- Hon. Michael R. Sonberg
- Peter R. Stambleck
- Lisa M. Stenson Haggray
- Richard P. Swanson
- Sergio Villaverde
- Philip R. Wagman
- Andrew R. Walker
- Kaylin L. Whittingham
- Anne Rose Wolfson
- Hon. Eric J. Wursthorn
- * Stephen P. Younger
- Gonzalo Salinas Zeballos

Second District
- Andrew Martin Cali-Vasquez
- Hon. Cheryl E. Chambers
- Hon. Barry M Kamins, (Ret.)
- † Domenick Napoletano
- Hon. Joanne D. Quiñones
- Aimee L. Richter

Third District
- Mara Dew Afzali
- Cailin Connors Brennan
- Justina Cintrón Perino
- Michael Davidoff
- Cianna Freeman-Tolbert
- Sarah E. Gold
- †* Henry M. Greenberg
- Matthew J. Griesemer
- Albert C. Hrdlicka
- Daniel Joseph Hurteau
- Hon. Rachel Kretser
- Adam Trent Mandell
- David W. Meyers
- *◊ David P. Miranda
- Bradley Christopher Murray
- David W. Quist
- Nic Rangel
- Dana L. Salazar
- Mark R. Ustin

Fourth District
- Luke John Babbie
- Cynthia F. Feathers
- Margaret E. Gilmartin
- Michelle M. Kulak
- Nancy K. Montagnino
- Dennis J. O'Connor
- Marne L. Onderdonk
- Connor Julius Reale
- Lauren E. Sharkey
- Diana Vance
- Michelle H. Wildgrube

Fifth District
- Hon. Tonastacia S. Dennis-Taylor
- Donald C. Doerr
- Hon. Danielle Fogel
- Donald Richard Gerace
- * Michael E. Getnick
- Karl E. Manne
- Hon. James P. Murphy
- Courtney S. Radick
- Sarah C. Reckess
- * M. Catherine Richardson
- Laura Lee Spring
- Madeline R. Thibault
- Kimberly Wolf Price

Sixth District
- Dawn Joyce Lanouette
- †* Richard C. Lewis
- * Kathryn Grant Madigan
- Bruce J. McKeegan
- Rachel Ellen Miller
- Alicia Christine Rohan
- Elisabeth Marie Rossow
- Adam J. Spence

Seventh District
- †* T. Andrew Brown
- Eileen E. Buholtz
- A. Vincent Buzard
- Kimberly Fox Duguay
- Sareer A. Fazili
- Mark D. Funk
- Jon P. Getz
- Meredith Monti Boehm Lamb
- Timothy P. Lyster
- Richard A. Marchese, Jr.
- Anthony Robert Palermo
- Heather C.M. Rogers
- * David M. Schraver
- Sharon P. Stiller

Eighth District
- Robert L. Boreanaz
- Robert Brucato
- Craig Robert Bucki
- Michael A. de Freitas
- Andrew Michael Debbins
- * Vincent E. Doyle, III
- Kristen Viola Elmore-Garcia
- Norman P. Effman
- Andrew J. Freedman
- †* Sharon Stern Gerstman
- Lindsay V. Heckler
- Harry G. Meyer
- Karen L. Nicolson
- Leah Rene Nowotarski
- Maura ODonnell
- Thomas M. O'Donnell
- Elliot Samuel Raimondo
- George E. Riedel, Jr.
- †* Kathleen Marie Sweet
- Keisha A. Williams
- Oliver C. Young

Ninth District
- * Mark H. Alcott
- Michael S. Baker
- Prof. Jay C. Carlisle, II
- Stamatia Dewbury
- Laurie A. Dorsainvil
- Hon. Lissette G. Fernandez
- Hon. Keri Alison Fiore
- Paul S. Forster
- Richard A. Glickel
- Evan M. Goldberg
- Sylvia Goldschmidt
- †* Claire P. Gutekunst
- Amanda M Henderson
- †* Sherry Levin Wallach
- Lawrence D. Lissauer
- Julianne Lusthaus
- David Evan Markus
- Courtney E. McGowan
- Irma K. Nimetz
- Christopher C. Palermo
- John A. Pappalardo
- Eric David Parker
- Brian J. Rayhill
- Steven R. Schoenfeld
- Hon. Adam Seiden
- Judah S. Shapiro
- Andrea C. Soto
- Hon. Susan M. Sullivan Bisceglia
- Richard Lawton Thurston

Tenth District
- Robin S. Abramowitz
- Michael J. Antongiovanni
- Joseph John Bambara
- Sharon N. Berlin
- Lois Bladykas
- Justin M. Block
- John P. Bracken
- Michael Cardello, III
- Dorian Ronald Glover
- David A. Goldstein
- Rezwanul Islam
- Christie Rose Jacobson
- Scott M. Karson
- Robert H. King
- Jennifer Lang Koo
- Tammy Rose Lawlor
- Hon. John J. Leo
- Steven G. Leventhal
- * A. Thomas Levin
- Peter H. Levy
- Ellen G. Makofsky
- Peter J. Mancuso
- Michael A. Markowitz
- Seth M. Rosner
- Yana A. Roy
- Sherwin Figueroa Safir
- Sanford Strenger
- Peter D. Tamsen
- Rosemarie Tully
- Glenn P. Warmuth
- Richard A. Weinblatt
- Alyssa L. Zuckerman
- Richard K. Zuckerman

Eleventh District
- Frank Bruno, Jr.
- Desiree Marie Claudio
- Alyssa Eisner
- Richard M. Gutierrez
- Tyear Middleton
- Hon. Sharifa Milena Nasser-Cuellar
- Estelle J. Roond
- Joel Serrano

Twelfth District
- Hugh W. Campbell
- Shantel Marie Castro
- Hon. Karen M.C. Cortes
- Michael A. Marinaccio
- Suzanne McElwreath

Thirteenth District
- Hon. Alison M. Hamanjian
- Daniel C. Marotta
- Sheila T. McGinn
- Claire C. Miller
- Catherine F. Schiavone
- Karen B. Soren

Out of State
- Jonathan P. Armstrong
- † Hong-Yu Chen
- Dean Matthew Diller
- Susan L. Harper
- Torsten M. Kracht
- Helen C.C. Naves
- Vivian D. Wesson

† Delegate to American Bar Association House of Delegates   * Past President   ◊ Leave of absence

Technology Takes Center Stage at the 2027 Annual Conference

When the New York State Bar Association gathers at the New York Hilton Midtown in January for its 2027 Annual Conference, attendees will find something new alongside the section programs and receptions that anchor the week: A full technology summit built into the heart of the meeting. The lineup includes a live artificial intelligence competition critiqued by judges, a startup pitch contest decided by audience vote, a multi-track slate of technology CLE programs, an expanded vendor expo and, for the first time in years, a conference app that puts all of it in attendees' pockets.

The summit is the work of NYSBA's Committee on Technology and the Legal Profession, working with association leadership and staff, and it reflects a simple premise: Technology programming should no longer be a single breakout session tucked into a corner of the schedule. This January, it will be a headline attraction. Please see President's Message on Page 4 for more details.

A Competition Where the Judges Grade the Lawyers

The centerpiece is the Prompt-a-thon, a live competition in which teams of attorneys receive a legal challenge on the spot and must solve it, unrehearsed, using AI tools while the audience watches. A panel of judges will then critique not just the results but the process itself, including the prompts, follow-up questions, verification steps, and judgment calls made along the way, before scoring the teams and crowning a winner.

"There is nothing quite like watching an approach get dissected in real time by someone who reads legal work product for a living," said Alexander Paykin, chair of the Committee on Technology and the Legal Profession and a member of the ABA TECHSHOW Planning Board. "The audience will learn more about effective prompting and ineffective prompting in 90 minutes than they would from any written guide. And yes, lawyers being graded in public remains every bit as compelling a spectacle as it was in law school."

The committee took the format for a test drive at a smaller event this summer, with members of the New York judiciary serving as critics, before scaling it up for Annual Conference.

A Startup Competition Decided by the Audience

The summit will also feature a startup competition in which emerging legal technology companies pitch their products live from the stage. Attendees will score the contenders in real time, with the results tallied instantly and the winners announced on the spot. Attendees can meet the founders and try the products for themselves.

"Some of these companies will be gone in a year; others will be the tools your entire office depends on in five years," Paykin said. "I have personally invested in more than one startup I tripped over at a conference expo, and so far, I have no regrets. This is a chance to see what is coming before your adversaries do, whether you want to buy early, keep a watchful eye or even write a check."

The CLE Slate

Surrounding the competitions will be a multi-track program of technology

Alexander Paykin

CLEs running across multiple days of the conference. Planned sessions include putting AI to work in day-to-day practice; the ethics of AI use and supervision; effective prompting techniques; cybersecurity for firms of every size; social media best practices; and hands-on mastery of the tools lawyers use every day, including Microsoft Word.

That last category may sound modest next to AI, but organizers expect it to deliver some of the fastest returns of the entire conference. "Most lawyers believe they know how to use Microsoft Word, and most lawyers are wrong," Paykin said. "The gap between how we use this program and what it can actually do represents hundreds of hours a year of wasted attorney and staff time. A little instruction goes a very long way, and your bottom line will notice."

Final program titles, descriptions and faculty will be announced this fall through the NYSBA website and email updates.

An Expo Built for Exploring

The vendor expo will feature established legal technology companies demonstrating practice management platforms, research tools, AI systems and more. To keep attendees moving through the hall, organizers are planning a conference-wide scavenger hunt run through the app with QR codes placed at sponsor booths and at key conference moments.

Also under development is a matching feature that would let attendees describe the problems they are trying to solve, connect with the vendors best positioned to solve them and schedule one-on-one meetings before anyone sets foot in the hall.

Finally, an App

Tying it all together is a new mobile app built specifically for Annual Conference and slated to launch in early December. The app will let attendees browse the full conference agenda; add any program to their personal calendars, complete with room, speakers, and description; download CLE materials as PDFs rather than hunting for handouts; navigate the Hilton with maps of the event space; and, for those who opt in, share contact information with fellow attendees and connect through LinkedIn.

"The plan is simple: Your entire conference in your pocket," Paykin said.

Registrants will receive download instructions by email when the app goes live, with a reminder in early January for those who wait until the last minute. It would not be a legal conference otherwise.

Mark Your Calendar

More details, including program titles, faculty, the competition lineup and the full schedule will roll out through the fall. In the meantime, the message from the organizers is simple: Reserve the dates, register early and arrive with a fully charged phone.

"Technology is no longer a specialty topic," Paykin said. "It is the water we all swim in, and the lawyers who understand it are already outperforming the lawyers who do not. Come see where the profession is heading. We will handle the rest."

A Guide to Streamlining Your NYSBA E-Communications

We get it. You're deluged with emails from everywhere. Add social media notifications, subscriptions and more from colleagues, family, associates, clients and advertisers, and it can be overwhelming.

At NYSBA, we strive to provide you with all the resources you need for your career. We want to make sure to keep you informed of all the latest news, events and CLE programs and publications. As a NYSBA member, you receive communications designed to keep you informed about professional development opportunities, legal updates, member benefits, events and resources relevant to your practice.

We also understand that you might need to streamline the communications you receive. We've put together the information below to help you do just that.

Please use this as a reference to help you quickly identify which communications are most relevant to your practice, your professional interests and your day-to-day needs, so you can stay informed without feeling overwhelmed.

Did you know that you can update your communications settings to receive only the content you need and reduce the number of emails hitting your inbox? Below will help you get started on managing your NYSBA e-communications.

How To Manage Your NYSBA Communications

My NYSBA Profile

Members can:

- Update email preferences.
- Select topics and sections of interest.
- Review subscription settings.

Online Communities

Separate from NYSBA profile communications preferences (visit link in member profile communications preference tab).

You can manage:

- Daily Consolidated Community Digest.
- Weekly Consolidated Community Digest.
- Discussion email settings.
- Specific community notifications.

Types of Emails

Below is a description of the types of emails we send and who they go to. These go to all members unless otherwise indicated, or members opt out in their communications settings.

General NYSBA Updates

- Association-wide news and announcements
- Advocacy updates
- Notifications about member benefits and major initiatives
- Messages from the president, House of Delegates, legislative updates, promotions and more
- Section communications pratice-area specific news, events, publications and resources
- Information about section-specific programs and activities
- Delivered only to members who have joined sections or indicated areas of practice or interest in their My NYSBA profile
- Especially valuable for members seeking substantive legal updates and networking opportunities

CLE Programs

- Information about CLE offerings, educational programs and training opportunities, including in-person events, webinars and more.
- Delivered to members based on indicated areas of practice or interest in their My NYSBA profile.

Newsletters

- **NYSBA Weekly**

  A weekly eNewsletter highlighting news and timely member-written content from NYSBA.

- **CasePrepPlus**

  A weekly summary of recent and significant New York appellate cases.

- **New York State Law Digest**

  A monthly eNewsletter on significant procedural developments.

- **At a Glance eNewsletter**

  A bi-weekly eNewsletter highlighting upcoming programming, newly released and featured publications and exclusive member benefit offerings.

- **Lawyer Assistance eNewsletter**

  A bi-monthly eNewsletter highlighting Lawyer Assistance Program initiatives and programs.

- **Career Center Job Opportunities eNewsletter**

  A bi-weekly eNewsletter highlighting employment opportunities.

- **Global eNewsletter**

  A bi-monthly eNewsletter for attorneys who practice internationally.

  Delivered to members of the International Section and any members with international law listed as an area of interest in their profile.

- **Student eNewsletter**

  Information on legal opportunities for law students.

  Delivered to law student members.

What Should I Read?

If you want to:	Read these emails:
Stay informed about all NYSBA activities	General updates
Build expertise in your practice area	Section communications
Earn CLE credits	CLE announcements
Get legal insights and articles	Newsletters and publications
Track your registered events	Event registration reminders
Keep up to date on NYSBA committees and sections	Community notifications

Publications

- Updates and promotions on various legal books, forms and other resources for your practice.
- Delivered to members based on indicated areas of practice or interest in their My NYSBA profile.

Event and Registration Reminders

- Automated reminders for events you registered for.

Community Notifications

- Messages notifying section members of activity within their exclusive online communities.

Which Emails Are Most Important for Me?

Below is a quick overview of which emails might be right for you.

Law Students

- Section communications
- Student eNewsletter
- Career Center Job Opportunities eNewsletter

New Attorneys

- General NYSBA Updates
- Young Lawyers Section communications
- CLE announcements
- At a Glance eNewsletter
- Career Center Job Opportunities eNewsletter

Experienced Practitioners

- Practice-specific section emails
- Legislative and regulatory updates
- CLE programs
- NYSBA Weekly
- CasePrepPlus
- New York State Law Digest
- At a Glance eNewsletter
- Leadership opportunities
- General NYSBA updates

ABA To Honor Pamela McDevitt Posthumously With Award for Excellence in Law Practice Management

By Jennifer Andrus

The American Bar Association's Law Practice Division is honoring the New York State Bar Association's late executive director Pamela McDevitt with its Samuel S. Smith Award.

The award recognizes a lifetime of exceptional contributions to the advancement of law practice management. It is the division's highest honor and will be presented posthumously during the ABA Law Practice Division Fall Meeting in Boston on Oct. 8.

"McDevitt's career exemplified the award's purpose: innovation, leadership and unwavering dedication to strengthening the legal profession," according to the ABA press release. "McDevitt's professional journey reflected a rare combination of strategic vision, operational excellence and deep commitment to the legal community."

A former Army Judge Advocate General Corps lawyer, McDevitt began her civilian legal career practicing law in Schenectady before moving into bar leadership roles that would define her national impact. She joined the ABA in 2010 after a four-year tenure as the director of law practice management at NYSBA. McDevitt rose to lead the ABA Law Practice Division as director until 2017 when she left Chicago to return to the capital region to lead the New York State Bar Association as executive director.

McDevitt guided NYSBA through a period of significant change including making technological advances in online CLE coursework, expanding attorney well-being services and broadening the association's global reach. Her vision led to the groundbreaking subscription-based membership model that began at NYSBA in 2025.


150 Years
NYSBA
2027
PRESIDENTIAL
GALA
BUILDING A BETTER BAR
Together
THURSDAY, JANUARY 21, 2027
CIPRIANI 42ND STREET | NEW YORK, NY
NYSBA.ORG/2027PRESIDENTIALGALA

Periodicals

ADDRESS CHANGE – Send To:
Member Resource Center
New York State Bar Association
One Elk Street
Albany, NY 12207
(800) 582-2452
e-mail: mrc@nysba.org