"The perils of dabbling": AI and the practice of law

By Tony Petruzzi, Esq., and Helena Guye, Esq., Tucker Ellis

SEPTEMBER 11, 2023

I. Implications of AI advancements

In the last year, rapid advancements in AI technologies have captivated public attention. With more AI systems being made available to the public, AI has progressed from the theoretical to an imminent reality. However, the prospect of widespread adoption of AI systems has also triggered numerous concerns, as this technology threatens to radically alter many aspects of life and work.

As with many other industries, the advancement and integration of AI technologies promises to make the practice of law more efficient and cost-effective. In fact, certain AI technologies have already been incorporated into the practice of law. For example, AI technology has long been used to optimize the review of legal documents, automate the process of discovery, and aid in legal research.

More recent innovations in generative AI technologies (applications like ChatGPT or DALL-E that generate new content, including text and images) have the potential to transform the legal industry even further. Despite AI technology's great potential, the ethical concerns surrounding these systems are especially relevant to the practice of law. Legal professionals in particular must take into account the potential risks associated with these emerging technologies.

II. Implementing AI in the practice of law

As rapidly advancing AI systems continue to disrupt the practice of law, legal professionals must ensure they maintain technological competency. Comment 8 to ABA Model Rule 1.1 provides: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*" (emphasis added). Many states have implemented similar rules imposing an ethical duty of technological competency.

As legal professionals test AI systems, it is imperative to understand the potential pitfalls, including: (1) the risks of relying on generative AI systems like ChatGPT to conduct legal research, and (2) the risks of disclosing sensitive information to these systems.

A. AI systems may generate incorrect information

One of the dangers posed by AI systems is the generation of false information. Generative AI systems can create new content, including text, images, audio, code, and video. For example, the wildly popular interface ChatGPT is a generative AI system that responds to user-inputted textual prompts with natural-language responses.

However, as included in a prominent disclaimer on ChatGPT's homepage, it "[m]ay occasionally generate incorrect information." The generation of incorrect information is due to ChatGPT's very design — ChatGPT does not access a database in order to generate its responses; instead, the chatbot is a "language model" that has been trained on large amounts of data to recognize language patterns and generate responses it predicts are relevant to a user's prompt.

Despite AI technology's great potential, the ethical concerns surrounding these systems are especially relevant to the practice of law.

The risk that generative AI will generate incorrect information came to the forefront in the widely publicized case of *Mata v. Avianca*, No. 22-CV-1461 (PKC) (S.D.N.Y.), in which a lawyer submitted nonexistent cases generated by ChatGPT.

In that case, an attorney submitted prompts to ChatGPT such as "argue that the statute of limitations is tolled by bankruptcy of defendant pursuant to montreal convention" and "provide case law in support of bringing case in state court for accident occurring on international airline." ChatGPT dutifully complied with each request, and the cases cited and quoted in ChatGPT's responses were incorporated in a document filed with the court.

When opposing counsel and the court questioned the existence of the cases cited, the attorney again utilized ChatGPT to verify his previous research with prompts like "Is Varghese a real case" and "Are the other cases you provided fake?" As shown in screen captures filed by the attorney on May 25, 2023, ChatGPT responded affirmatively, stating that the cases it generated "indeed exist and can be found on legal research databases such as Westlaw and LexisNexis." Again, the attorney relied on the accuracy of ChatGPT's responses, believing its answers were generated "based on publicly available information, including publicly available case law," when, in fact, the cases did not exist.

This case demonstrates a fundamental misunderstanding of ChatGPT's functionality. In his declaration filed in response to the court's order to show cause why he ought not be sanctioned, the attorney stated he believed that ChatGPT worked "essentially like a highly sophisticated search engine," and he "conducted the search in question in the same general manner" as any other legal research database.

The offending attorneys requested leniency, remarking that their actions demonstrated "the perils of dabbling." Ultimately, the attorneys were sanctioned by the court for these submissions. As the court explained, "Technological advances are commonplace and there is nothing inherently improper about using a reliable artificial intelligence tool for assistance. But existing rules impose a gatekeeping role on attorneys to ensure the accuracy of their filings."

B. AI systems may not be private or secure

Another underappreciated risk of AI systems is a lack of privacy protection or security. For example, ChatGPT's developers can review the input and conversation history of its users. According to the applicable privacy policy, users' personal information, including log and usage data, may be used to analyze, improve, and develop ChatGPT's services. Further, users' personal information may be disclosed to third parties like vendors and affiliates of ChatGPT.

ABA Model Rule 1.6 establishes the duty for lawyers to maintain the confidentiality of their clients' information and requires that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Attorneys thus have an ongoing obligation to evaluate the level of security of the technology used in storing, accessing, and transmitting client information.

Because ChatGPT's terms allow it and third parties to access user data, any input of confidential information into ChatGPT could qualify as an unauthorized disclosure and an ethical violation. This very vulnerability has led companies such as Samsung to ban the use of generative AI after its employees input into the chat bot confidential information, including sensitive source code. See "ChatGPT fever spreads to US workplace, sounding alarm for some," Reuters.com, Aug. 11, 2023. Legal professionals, too, must take care when utilizing new AI technologies to avoid potential disclosures of confidential information, attorney client communications, and work product.

The security risks and challenges posed by emerging technologies like AI are not necessarily unprecedented in the context of legal practice. For example, legal professionals have already confronted security concerns surrounding the integration of then-new technologies such as email or cloud computing. For legal professionals, acquiring a commercial license with nondisclosure and nonuse provisions for these otherwise vulnerable third-party technologies would afford a reasonable expectation of privacy that would protect client confidences.

In the absence of a commercial license that includes nondisclosure and nonuse provisions, publicly available applications remain potentially vulnerable to disclosing confidential information to third parties. Similar web-based services like Google Translate are susceptible to these same dangers — like ChatGPT, Google collects user data in order to maintain and develop its services. Legal professionals have and should continue to make reasonable efforts to assess the security issues involved in the use of new technologies. A careful review of data collection and privacy terms is critical when utilizing new AI systems.

III. Conclusion

While the potential of new AI systems continues to fascinate and inspire, legal professionals must be wary of its potential risks. In particular, lawyers must be aware of the danger of AI generating incorrect information and lacking security measures before utilizing these new technologies.

About the authors

Tony Petruzzi (L), chair of the **Tucker Ellis** eDiscovery group and an active member of The Sedona Conference, is a frequent speaker on areas of eDiscovery, both locally and nationally. In addition to counseling clients in all areas of eDiscovery, his practice focuses on white collar criminal defense, corporate investigations, and business litigation. He is resident in the firm's Cleveland office and can be reached by email at anthony.petruzzi@tuckerellis.com. **Helena Guye** (R) is an intellectual property attorney at the firm. She focuses her practice on trademark, patent, copyright, and trade secret litigation and enforcement, and advises clients on strategies to acquire and maintain their intellectual property assets. She is resident in the firm's Los Angeles office and can be reached by email at helena.guye@tuckerellis.com.

This article was first published on Reuters Legal News and Westlaw Today on September 11, 2023.