PLF *in*BRIEF

ISSUE 144 | DECEMBER 2023

Malpractice Prevention Education for Oregon Lawyers

Exploring ChatGPT's Capabilities, Limits, and Risks for Lawyers—Part II

By Hong Dao

EDITOR'S NOTE: THIS ARTICLE IS PART II OF A TWO-PART SERIES.

In Part I of this two-part series, we looked at ChatGPT's capabilities and concerns about its limitations that can affect its reliability and limit its usefulness for lawyers. Part II focuses on the potential risks legal professionals face when using ChatGPT and offers some guidance on how to safely use this tool in their practice.

Risks of Using ChatGPT

In light of the concerns discussed in Part I, let's look at a few malpractice and ethical risks for lawyers relying on ChatGPT or similar generative AI tools in the practice of law.

EXPLORING CHATGPT... (CONTINUED FROM PAGE 1)

1. INACCURATE LEGAL INFORMATION

Consider this scenario: A lawyer working on a complex contract law matter uses ChatGPT to research relevant case precedents that deal with similar contractual disputes. ChatGPT provides two case citations and a summary of the opinions. The lawyer then uses those citations in their legal argument during a court proceeding. After the opposing party argues that those decisions do not support the lawyer's position, it's discovered that one of the cases does not exist, and the other does not address the legal principles or facts relevant to the lawyer's case. The lawyer has unintentionally presented incorrect information to the court, undermined their own credibility, and weakened their client's argument.

This scenario is the summary of a long response ChatGPT generated when I asked it to give me an example of how a lawyer might face malpractice exposure for relying on ChatGPT.

Legal research and writing seem like a perfect use for ChatGPT as it can explain legal concepts, summarize information, and write briefs, memos, or correspondence. Due to its limited world knowledge and propensity for hallucination, however, ChatGPT will make up legal authorities or case precedents if it doesn't have the requested information in its dataset. The unfortunate scenario above played out for a lawyer who was in the news for citing fictitious authorities provided by ChatGPT in court.[1]

At this stage in development, it is not advisable for lawyers to depend on ChatGPT to conduct legal research and write legal documents without scrutinizing and verifying the information provided to ensure accuracy. The potential for malpractice exposure for a lawyer who relies on incorrect information cannot be overstated.

2. NEGLIGENT ADVICE

Let's consider another scenario: A lawyer representing a client in a personal injury case uses ChatGPT to determine the value of the client's claim. ChatGPT provides an estimate of damages based on general information but fails to consider specific factors relevant to the client's case. The lawyer relies on this estimate and provides negligent advice to the client regarding the potential value of the claim, likely influencing the client's decision to accept a settlement offer or take the case to trial.

This scenario is also a summary of a response from ChatGPT to my prompt on how a lawyer could commit malpractice for relying on ChatGPT.

The challenge here is that ChatGPT has trouble responding accurately to ambiguous queries or overly general prompts. This difficulty is exacerbated by a lawyer's ethical obligation to maintain client confidentiality. This means when lawyers interact with ChatGPT, they may need to communicate in a general manner, use vague language, and omit crucial context and facts. When ChatGPT receives incomplete information, it will generate responses based on its limited understanding of the given input. Lawyers might counsel their clients or make strategic case decisions relying on these incomplete answers, creating a risk of inaccurate advice that can lead to an unfavorable outcome for or harm to the clients.

3. ETHICAL RISKS

Relying on unverified responses from ChatGPT may give rise to other risks that implicate a lawyer's ethical obligations. These include duties of competence (ORPC 1.2) and diligence (ORPC 1.3) for failing to verify the accuracy of the information before using it in their legal work. They also include the duty of communication (ORPC 1.4) when a lawyer uses incomplete or inaccurate information in communicating with clients. The duty of confidentiality (ORPC 1.6) could be implicated if a lawyer inputs client data into ChatGPT without obtaining the client's informed consent or taking appropriate measures to protect confidentiality. Additional rules such as ORPC 5.1 and 5.3 (staff supervision) and 3.3 (candor to the court) may also come into play.

> "...ChatGPT has trouble responding accurately to ambiguous queries or overly general prompts... This means when lawyers interact with ChatGPT, they may need to communicate in a general manner, use vague language, and omit crucial context and facts."

Tips on Using ChatGPT

Given these significant risks, is there a safer way for legal professionals to use this technology in their law practice? Consider the following tips when interacting with ChatGPT to reduce your exposure.

1. VERIFY THE OUTPUT

Lawyers need to conduct further research to determine the accuracy and reliability of ChatGPT's responses. You should cross-reference responses with primary and secondary legal authorities such as statutes, regulations, case law, and legal treatises by using established legal research tools like Fastcase, LexisNexis, or Westlaw. Lawyers must also conduct their own independent research to delve deeper into the legal issues, which can help confirm or disprove the information received from ChatGPT. With a more thorough understanding of the topic, you can identify gaps or inconsistencies in the answers provided. These are not the only ways to verify ChatGPT's responses, but they are crucial to the process.

2. ANCHOR TO A SOURCE OF TRUTH

At the ABA TECHSHOW in March 2023 , AI expert Pablo Arredondo of Casetext repeated a key phrase in the context of using ChatGPT: "We must anchor it to a source of truth." This refers to the practice of providing ChatGPT with reliable and authoritative sources of information to ensure that its responses align with accurate and verifiable facts. Lawyers using generative AI need to specify the source of truth and guide the technology to generate responses that are reliable, by including specific references or citing reputable sources directly in your prompt. You can also explicitly instruct ChatGPT to consider a particular source as a basis for its responses, mitigating the risk of inaccurate or misleading information by grounding its answers in verified and trusted knowledge or facts.

3. SAFEGUARD CONFIDENTIAL AND PROPRIETARY INFORMATION

To safeguard client and firm data, lawyers and law offices should prohibit inputting client information and proprietary data into ChatGPT or similar tools. This precaution is crucial to prevent staff from inadvertently disseminating information, because ChatGPT incorporates user input into its training. Samsung's case serves as a cautionary example: Business Insider reported that Samsung banned its employees from using generative AI tools after its engineers accidentally leaked internal source code to ChatGPT.[2] Firms should have a written policy on AI usage, including these prohibitions.

Additionally, lawyers can enhance data protection by disabling their chat history to opt out of contributing to OpenAI's model training. Go to ChatGPT settings, click on "Data Controls," and toggle off the "Chat history & training" option.

4. USE FOR NON-LEGAL AND ADMINISTRATIVE TASKS

Delegating non-legal and administrative tasks to ChatGPT is a safer way for legal professionals to use the tool. For example, lawyers can use ChatGPT to generate content for marketing or social media; draft routine office emails; proofread documents for errors and inconsistencies; create checklists for client onboarding or office procedures; produce office forms and client satisfaction questionnaires; brainstorm ideas for event planning, team building, or employee engagement; and even generate agenda items for meetings. None of these tasks require ChatGPT to rely on legal authorities, case precedents, intimate knowledge of legal matters, or client information to provide reliable and accurate responses.

5. INTEGRATE VIA AN API

Another safe way to interact with ChatGPT is to use an application, product, or service that integrates with this AI technology. The integration occurs through an application programming interface (API), which allows software developers to access ChatGPT's functionality.

Integration offers a significant advantage over using ChatGPT in its raw form. Software developers can leverage their external databases, knowledge sources, or structured data to supplement or refine the answers generated by ChatGPT. When ChatGPT retrieves information from these verified sources—rather than relying solely on its pre-trained knowledge—it provides more accurate and relevant responses. Acting as a form of guardrail, integration addresses some of the limitations discussed in Part I.

While it's not practical for lawyers to build their own software, you can explore tools like CoCounsel (by Casetext), Copilot (by LawDroid), Alexi, and Spellbook (by Rally) to harness ChatGPT's capabilities for document review, legal research, drafting, and contract analysis. These applications and services offer a valuable and more accessible way to use ChatGPT or similar AI technology for legal tasks. Even with these advanced tools, the lawyer still bears the ultimate responsibility for ensuring accuracy, legal applicability, and ethical compliance.

6. OTHER TIPS

While not all lawyers use ChatGPT, it's likely that their clients do. Clients, like many consumers, turn to the internet for answers, including seeking legal advice through AI. They may not realize, however, that the information could be incorrect or contextually flawed. You must educate clients about the tool's limitations and foster open discussions to emphasize that it can't replace your expertise, judgment, and counsel. Clients need to recognize the importance of critically assessing ChatGPT's responses and relying on your guidance in their legal matters.

Regardless of your awareness about your clients' ChatGPT usage, document your advice through emails or letters. A paper trail clarifies the source of advice and helps clients differentiate between AI-generated responses and your professional legal counsel.

Conclusion

Whether lawyers like it or not, ChatGPT is here to stay and will likely reshape the legal profession. Products powered by generative AI will become as ubiquitous as email or Westlaw, with technology like Microsoft's Bing and 365 Co-Pilot already integrating ChatGPT into everyday tools. It's just a matter of time before other programs commonly used in law offices today follow suit. Legal professionals must educate themselves as generative AI becomes integral to our professional landscape. ■

Hong Dao is the Director of the PLF Practice Management Assistance Program.

OTHER WORKS BY HONG DAO

- Exploring ChatGPT's Capabilities, Limits, and Risk for Lawyers: Part I (*in*Brief, August 2023)
- Plugging the "Knowledge Drain:" How to Retain Knowledge to Ensure Your Firm's Continued Success (*in*Practice blog post, September 13, 2022)
- Don't Wait Until the Last Minute to File and Serve Your Complaint (*in*Practice blog post, June 15, 2021)
- Tommy and the Secure Tunnel: Virtual Private Networks (*in*Practice blog post, April 23, 2021)

ENDNOTES

i "ABA Journal, "Judge finds out why brief cited nonexistent cases—ChatGPT did research," (5/30/23), *https://www.abajournal.com/news/article/judge-finds-out-why-brief-cited-nonexistent-cases-chatgpt-did-the-research*

ii Business Insider, "Samsung bans employees from using AI tools like ChatGPT and Google Bard after an accidental data leak, report says," (May 2, 2023), *https://www.businessinsider.com/samsung-chatgpt-bard-data-leak-bans- employee-use-report-2023-5*