Exploring ChatGPT's Capabilities, Limits, and Risks for Lawyers

By Hong Dao

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

Since the debut of ChatGPT-3.5 in November 2022, this generative AI technology has lawyers both excited and worried. Some are eager for its potential to transform how lawyers work. Others are anxious it could render lawyers obsolete. We've all heard of artificial intelligence powering our smartphones and smart devices like vacuum cleaners, TVs, and speakers, but generative AI is a newer concept for many of us. It is a kind of artificial intelligence that creates new and original content in the form of text, image, video, audio, and more. While many generative AI companies[1] are introducing different products, ChatGPT is making the biggest splash right now.

Part I of this article will provide a basic introduction to ChatGPT by exploring its capabilities, limits, and concerns. Part II will shed light on the possible malpractice risks for lawyers when incorporating it into their practice. By examining these issues, readers can better understand the potential impact of this revolutionary technology on the legal profession—and the precautions to consider.

What is ChatGPT?

An AI-powered chatbot developed by OpenAI, ChatGPT generates human-like responses to user questions by analyzing and synthesizing information from a large dataset. According to the developer, this technology is trained on three sets of data: (1) publicly available information from the Internet (e.g., websites, online databases, social media, online publications and journals); (2) licensed information from third parties (e.g., commercial databases, academic and research sources, copyrighted creative works); and (3) information that its users and human trainers provide. The combination of these three data sources allows ChatGPT to access a vast array of knowledge and provide responses on a wide range of topics.

OpenAI explains how the process works:

"ChatGPT has been developed in a way that allows it to understand and respond to user questions and instructions. It does this by 'reading' a large amount of existing text and learning how words tend to appear in context with other words. It then uses what it has learned to predict the next most likely word that might appear in response to a user request, and each subsequent word after that. This is similar to auto-complete capabilities on search engines, smartphones, and email programs."[2]

ChatGPT is accessed via the Internet and is also available as an app for IOS devices. To use the program, go to the OpenAI website, *https://openai.com*, and create an account. Once done, you enter a prompt in the "send a message" field and ChatGPT will generate a response. The prompt can be a question or query, but it can also be a command, statement, or instruction, such as, "Write a riddle involving eggs for

> "Given its professed prodigious talents and rapid-fire responses, it is understandable that lawyers would want to leverage ChatGPT for legal research and writing, case analysis, contract and document review, defining difficult legal concepts, and answering legal questions."

kindergartners," or "List the 10 most popular places for summer vacation in the Pacific Northwest."

The current free version—ChatGPT-3.5—is the topic of this series. Anyone using ChatGPT-3.5 (the publicly available version) must comply with OpenAI's terms and policies on sharing and publication, usage, and terms of use and privacy policies. These terms and policies are available at: *https://openai.com/policies*.

OpenAI released a more advanced version in March 2023 called ChatGPT-4, which offers more enhanced capabilities as it can handle images as inputs, not just text. It is trained on a wider dataset and has more computing power. As of this writing, however, ChatGPT-4 is only accessible through a paid subscription to ChatGPT Plus or to developers with API access.

ChatGPT's capabilities

In researching what ChatGPT can do, I asked ChatGPT itself this question. It listed the following things: answer questions on a wide range of topics; assist with research; translate different languages; engage in creative writing; assist with programming or coding; provide general advice and suggestions; help define and break down complex concepts; summarize information; proofread and edit; brainstorm ideas; converse as a companion; play word games and riddles; tell jokes and share interesting facts; and more.

These diverse capabilities show how versatile and useful this technology could be. Given its professed prodigious talents and rapid-fire responses, it is understandable that lawyers would want to leverage ChatGPT for legal research and writing, case analysis, contract and document review, defining difficult legal concepts, and answering legal questions. These tasks align closely with ChatGPT's capabilities. In light of the concerns about its current limitations, however, lawyers should carefully assess whether OpenAI's brainchild is truly capable of performing those legal tasks reliably at this stage of development.

Concerns about ChatGPT

While ChatGPT's capabilities are seemingly remarkable, a few key concerns have emerged that are particularly relevant to lawyers and affect the program's reliability and limit its effectiveness.

1. LIMITED WORLD KNOWLEDGE

Despite being trained on a vast dataset, ChatGPT's training on historical data ends in 2021.[3] Its knowledge of the world, events, trends, and developments is based on information up until September 2021. Any new information it now learns is from conversations with its human users. Consequently, when users provide ChatGPT with wrong information, it may "learn" the inaccuracies and incorporate them in its responses. This limited training data and exposure to incorrect information affect its ability to understand nuanced questions, comprehend references to current events, or grasp regional and local context. As a result, it can generate biased, inaccurate, or outdated responses.

2. HALLUCINATION

Another major concern is the issue of "hallucination." ChatGPT has been known to "hallucinate" responses— that is, fabricate information.[4] It creates responses by essentially predicting the next words based on an analysis of the provided data. It does this through learning statistical patterns and relationships between words and phrases and then using these patterns to

"ChatGPT has been known to 'hallucinate' responses."

predict and generate responses. However, there may be gaps in its pattern recognition capabilities that can affect its response. Unfortunately, the technology has no inherent mechanism to verify the accuracy or truthfulness of information it generates—it can't fact-check or validate its own responses. A confounding factor is that ChatGPT does not provide references, sources, or citations for the information it generates. In sum, the chatbot can produce false or incorrect information that may be hard to verify and, ergo, can't be relied upon. You also cannot use ChatGPT to verify its own work product because it has proven unreliable in self-verification.

3. COLLECTION OF USER'S DATA & PRIVACY CONCERNS

OpenAI collects your personal information such as IP address, browser details, and data from your interactions with ChatGPT. It may use your personal information for many purposes. OpenAI states that its employees review user conversations to train ChatGPT, improve their system, and to "ensure the content complies with our policies and safety requirements."[5] Your personal information may also be disclosed to third parties without your knowledge.[6] We can assume that OpenAI retains the confidential and personal information that users provide to ChatGPT. Although OpenAI provides the option to delete user data from their system, it's unclear whether the data has already been used for training.
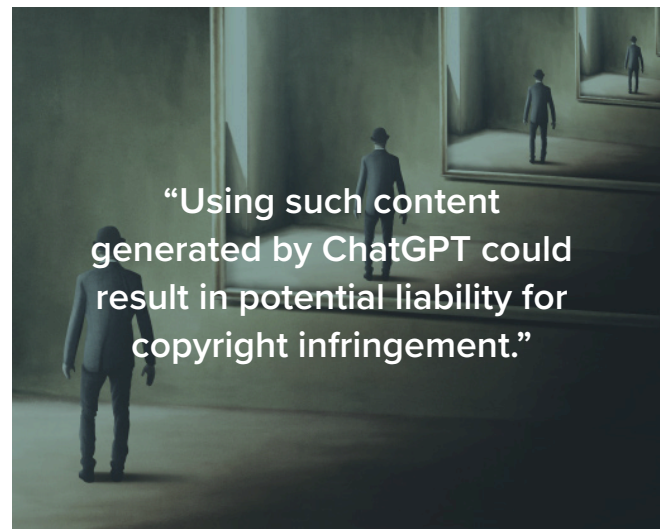
4. DIFFICULTY HANDLING AMBIGUOUS QUERIES

When you use imprecise or vague language, omit context, or provide incomplete information in your query, ChatGPT tends to offer incomplete or irrelevant information in its responses. ChatGPT relies on patterns and examples from its training data. When it receives an ambiguous query, it doesn't have the contextual understanding and background knowledge to fully comprehend the intended meaning. Functionally, it is unable to ask for clarification or follow-up questions and will proceed to reply based on its own interpretation of the query. It is incumbent on the users, then, to provide clear, specific, and complete information

to ensure an accurate and relevant response from ChatGPT. In the case of lawyers, though, confidentiality concerns or complexities in the legal matter present constraints on sharing a lot of details or providing explicit context.

5. PLAGIARISM, INTELLECTUAL PROPERTY, AND LIABILITY

A major concern sweeping across college campuses following the release of ChatGPT-3.5 was plagiarism. In the legal context, the potential for plagiarism is really an issue of copyright infringement.

"Using such content generated by ChatGPT could result in potential liability for copyright infringement."

Although ChatGPT is supposed to generate original content, there is still a risk that its content may be substantially similar to an existing copyrighted work. Using such content generated by ChatGPT could result in potential liability for copyright infringement. The question of who (the user or OpenAI) is liable for the infringement is unresolved at the moment.

According to OpenAI's Terms of Use,[7] users own the "input"—the prompts, questions, or queries you enter when you use ChatGPT. ChatGPT delivers the "output" based on your input. Together, these are called the "content" in the Terms of Use. OpenAI assigns to the users all of its rights, title, and interest in and to the output. The Terms make clear that OpenAI considers the user responsible for the generated content. It remains to be seen whether

the Terms of Use would actually shift the burden of responsibility for infringement entirely to the user, or whether the user and OpenAI would share liability for any such violation. This and many other IP and liability issues will undoubtedly be raised at some point in future litigation and likely make their way to the courts for resolution.

These are just some of the major concerns relevant to the legal profession. Part II of this article will discuss the risks for lawyers of using ChatGPT and offer some guidance on how they can safely leverage this tool in their practice. Please look out for Part II in the next issue of *inBrief*. ◼

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

OTHER WORKS BY HONG DAO

- 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)

1 A comparison chart of generative AI companies and their products is available here: *https://eweek.com/artificial-intelligence/generative-ai-companies/*.

2 OpenAI FAQ on "How ChatGPT and Our Language Models are Developed," *https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed*.

3 OpenAI, "What is ChatGPT?", *https://help.openai.com/en/articles/6783457-what-is-chatgpt*.

4 OpenAI, "What is ChatGPT?", *https://help.openai.com/en/articles/6783457-what-is-chatgpt*.

5 OpenAI, "What is ChatGPT?", *https://help.openai.com/en/articles/6783457-what-is-chatgpt*.

6 OpenAI Privacy Policy, *https://openai.com/policies/privacy-policy*.

7 OpenAI Terms of Use, *https://openai.com/policies/terms-of-use*.