ChatGPT May Be Great for Efficiency, But Don't Leave Ethics at the Door

By Angela Kalsi and Rini Roy

Greensfelder, Hemker & Gale, P.C.

TikTok, who? ChatGPT – an artificial intelligence (AI) chatbot developed by OpenAI – is the fastest-growing app of all time, according to analysis by Swiss bank UBS[i]. A natural language processing tool that can engage in human-like conversations on an infinite number of subjects, ChatGPT is trained to follow a prompt and generate a quick and detailed response. Numerous generative AI software programs are emerging alongside it. But with this capability comes risks, limitations, and ethical considerations significant to the legal industry.

The Model Rules of Ethics require attorneys to maintain "technological competency," meaning they must keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. Therefore, attorneys cannot bury their heads in the sand when it comes to ChatGPT and other generative AI technology. In reality, their colleagues and clients are already using it and other programs like it, so it is essential that every attorney understand the risks and benefits.

The emergence of ChatGPT and similar generative AI programs present opportunities for automation and efficiency, but the technology is still in development and cannot be relied upon blindly. ChatGPT is trained on vast amounts of information obtained from the Internet, but it does not always present the most relevant data in generating responses and has been a frequent source of bias and misinformation in its responses to queries. For instance, early attempts to query ChatGPT for case law often yielded cases invented by ChatGPT, which perhaps understood such queries as creative writing prompts rather than as legal research requests. This led to a high-profile case in which two New York attorneys and a law firm were sanctioned for including citations to fake case law created by generative AI in a court filing.[ii] The judge in that case found the lawyers had acted in bad faith and made "acts of conscious avoidance and false and misleading statements to the court," but also noted that there is nothing "inherently improper" in lawyers using AI "for assistance," although existing ethics rules "impose a gatekeeping role on attorneys to ensure the accuracy of their filings." ChatGPT now includes a disclaimer when providing case law, noting that while it can "provide general insights on legal topics and principles, legal databases are essential for in-depth, current, and reliable legal research." It also adds that "if one needs legal advice or detailed legal information, [one should] consult a legal professional," which seems prudent, given that ChatGPT was not designed to specifically evaluate questions of law.

While ChatGPT can still prepare responses on a nearly infinite number of subjects, a lawyer's ethical duty of competence should always take precedence over convenience. Attorneys must do their due diligence by verifying any answers that come from ChatGPT, comparing them to their own knowledge or conducting their own research from reputable sources. Importantly, ChatGPT is limited in its ability to provide sources or evidence to support where it obtained its answers, so it is imperative to independently verify any answers it generates.

Conversations about ChatGPT and attorney ethics must also focus on the duty to maintain client confidentiality. The terms of use for ChatGPT expressly state that any content entered may be reviewed by its human trainers and is not kept private. Therefore, attorneys must ensure that the input provided to ChatGPT does not contain confidential or privileged information, or information from which a current, former, or prospective client's information could be deduced, as doing so could violate a lawyer's ethical responsibility to keep information relating to the representation of a client confidential. Because information entered into ChatGPT is not kept private, attorneys must also expect that any such information would be discoverable in a lawsuit.

In advising their clients, attorneys should warn companies to guard their sensitive business information and trade secrets when using ChatGPT. Earlier this year, Samsung employees unwittingly leaked confidential data while using ChatGPT to help them fix problems with their source code, including inputting the source code itself and internal meeting notes data relating to its hardware[iii]. In response to the incident, Samsung is reportedly developing its own in-house AI for internal use by employees — a great solution for Samsung, but not feasible for every company. Thus, it is prudent for companies to invest in training employees, and attorneys should be ready to advise clients on the appropriate use of AI so they can use it to support and advance their work in a transparent and responsible manner. Company policies and guidelines must also be updated as new technologies emerge.

Notably, ChatGPT's terms of use place the onus of data security and privacy on the user, stating that, by using ChatGPT, users are representing to OpenAI that they are processing data in accordance with all applicable laws. The terms of use go further to state that users "must provide legally adequate privacy notices and obtain necessary consents for the processing of [any personal] data" on the platform. This position is likely the result of ChatGPT's perceived noncompliance with certain privacy regulations, such as the European Union's General Data Protection Regulation (GDPR). That law governs how companies collect and use data, and one of its core tenets is the "right to be forgotten" or to have one's information deleted upon request. Data generally cannot be retrieved or deleted once entered into ChatGPT, as it is stored on the servers belonging to OpenAI. Each time users chat with the AI, the conversations and user inputs are saved as an ongoing conversation thread to help improve the AI's accuracy over time. Italy, in fact, temporarily banned the use of ChatGPT in March 2023, citing concerns for privacy violations. The ban was lifted shortly thereafter, and OpenAI claims to have fulfilled the conditions Italy wanted satisfied. Those included adding information on its website about how it collects and uses data, the ability to opt out if users do not want their data used for training, and a form for users to request deletion of their personal data. Users can now find a toggle switch on the Settings menu under "Data Controls," which gives users the option to turn off chat history. Conversations that are started when chat history is disabled will not be used to train and improve the ChatGPT model and will not appear in the history sidebar. However, even conversations with chat history turned off are kept for 30 days and can be reviewed under certain circumstances. Furthermore, there has been debate over whether the personal data deletion function is technically even possible, given how complex it can be to separate specific data once it has been churned into ChatGPT's training data.

In sum, ChatGPT's compliance with privacy regulations is still an open question, and many other privacy laws may be implicated by ChatGPT. For instance, if a hospital uses ChatGPT to streamline letter writing to patients' insurers, it may in fact be violating HIPAA if it has entered any individuals' sensitive medical information into the platform. If an education provider uses ChatGPT to quickly organize and collate student attendance data, it may be violating the Children's Online Privacy Protection Act, which forbids putting online any personal information from children under age 13. Therefore, it is important for attorneys to understand the potential risks and consequences for their clients based on their specific uses of ChatGPT.

Another area of uncertainty is the risk of violating someone's intellectual property in using ChatGPT responses. According to ChatGPT, the user owns the rights in the user's prompts and the generated responses the user receives. However, multiple lawsuits filed over the past year have alleged that ChatGPT trained on copyright protected works without permission from the originators, including the first copyright infringement case filed against ChatGPT by two authors claiming their books were used to train ChatGPT without their consent, credit, or compensation.[iv] The lawsuit claims that because ChatGPT can accurately summarize the authors' books, ChatGPT was trained on their book content, which they surmise was taken from a shadow library of pirated works. Notably, the lawsuit does not specify which specific parts of the authors' novels have been unlawfully copied and reproduced in the summaries, but only faults the way AI has received such information and the sources of its data.
The court's ultimate decision will be important to watch for, especially considering Google's success in overcoming legal challenges to its online book library in 2016, when the U.S. Supreme Court rejected the

authors' claims that digitizing millions of books and showing small portions of them to the public amounted to copyright infringement[v] and a more recent statement by a California federal judge presiding over an AI art copyright class action lawsuit noting that an artist with registered copyrights has "likely asserted a cognizable claim of direct infringement" against one of the plaintiffs for copying her work at the training stage.[vi] Therefore, as seen here, it is possible that responses generated by ChatGPT may infringe upon someone else's copyright. Accordingly, users should proceed with caution when using any content created by ChatGPT, always reword any content in the user's own voice, and generally use such content for internal informational or educational purposes only.

By understanding the limitations of generative AI technology and being mindful of the ethical considerations summarized above, there is potential for ChatGPT to be used in a way that is both innovative and ethical. Furthermore, generative AI programs focused on legal research designed specifically for lawyers are already in development and may alleviate some concerns. At present, however, attorneys must continue to critically assess and implement generative AI technology responsibly to ensure they uphold their ethical obligations and protect client interests.

[i] https://news.yahoo.com/chatgpt-fastest-growing-app-history-142338104.html

[ii] https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/

[iii] https://www.techradar.com/news/samsung-workers-leaked-company-secrets-by-using-chatgpt?fbclid=IwAR1ktiDjeL85IdZo6PciwNrmKO6HZppNiIJ_lxyIf7NcwDOR5YX-mtXgpQQ

[iv] https://www.theguardian.com/books/2023/jul/05/authors-file-a-lawsuit-against-openai-for-unlawfully-ingesting-their-books

[v] https://www.reuters.com/article/us-google-books/google-defeats-authors-in-u-s-book-scanning-lawsuit-idUSBRE9AD0TT20131114

[vi] https://www.thefashionlaw.com/court-inclined-to-dismiss-claims-in-lawsuit-over-ai-art-generators/#:~:text=the%205%20billion%20images%20it,her%20work%20at%20the%20'input'