The Risks of Using ChatGPT in the Legal Industry: Confidentiality and Ethical Concerns

April 13, 2023

By: Aaron C. Tifft

The Journal Record

https://journalrecord.com/2023/04/13/gavel-to-gavel-confidentiality-ethical-risks-of-using-chatgpt-in-law/

Privacy and confidentiality are crucial aspects of the legal practice and the attorney-client relationship. Attorneys must protect the confidentiality of their clients, and clients rely on this protection for all their information. When attorneys use artificial intelligence systems that rely on large language models (LLMs), such as ChatGPT, it raises serious concerns about client confidentiality.

ChatGPT is a language model that uses machine learning algorithms to generate human-like responses to text inputs. People have begun to use this system for a wide range of purposes, including drafts of correspondence, communications, and even legal research and writing. However, the use of ChatGPT in the legal industry risks significant confidentiality breaches.

ChatGPT learns from large amounts of data, including past conversations and text inputs provided by its users. ChatGPT's machine learning algorithms will store and analyze any sensitive information included in a draft when an attorney uses it to communicate with clients. This data could easily include personal client information and confidential legal strategies.

After inputting information into the ChatGPT system, an attorney no longer controls who can access it. Third-party servers typically host most machine learning, large language models (like ChatGPT). The data is stored in off-site locations around the world and is likely accessible to others. Other parties could include the company that provides the LLM system, as well as any third-party vendors or contractors with access to the servers. Additionally, if an attorney fails to maintain the security of their access credentials, it could lead to a significant breach of confidential client data, revealing all information provided to the LLM system.

Using ChatGPT in legal communication and writing raises ethical issues. Attorneys have a duty to

provide competent and diligent representation to their clients, which includes ensuring that the attorney fully understands the legal advice and strategies they recommend. ChatGPT is not able to provide the same level of nuanced and contextualized advice that a human attorney can provide.

Large language models are "trained" on large amounts of text, but there is no guarantee the text is accurate, Unsurprisingly, this often results in overly simplistic or incorrect legal analysis. The ChatGPT site itself provides a disclaimer, "ChatGPT may produce inaccurate information about people, places, or facts." A brief test demonstrates that the ChatGPT system will regularly misstate the elements of legal claims, cite cases that do not address the stated proposition, and confidently assert facially incorrect legal premises.

ChatGPT and other LLMs are exciting new tools with many potential applications in the legal industry. As with any tool, attorneys must use them properly and carefully. Attorneys must consider and mitigate the risks associated with using ChatGPT and other LLM systems. This is easily accomplished by limiting the use of ChatGPT to non-confidential communciations (or portions thereof) and drafts for public consumption. Ultimately, the duty to protect client confidentiality and privacy should always remain the top priority for attorneys, and these exciting technological tools must be used with this duty in mind.

Attorneys

- Aaron C. Tifft