CYBERSECURITY AND DATA PRIVACY
INFORMATION MEMO
JANUARY 23, 2024

ChatGPT – Hallucinating Case Law, Instigating Attorney Sanctions and Stealing Privilege – Oh My!

In 2023, use of generative artificial intelligence (Gen AI) tools such as ChatGPT went viral. Generative AI platforms can be utilized to create a host of efficiencies across businesses and professions such as drafting emails, summarizing meetings or writing or debugging lines of code. However, the widespread adoption of ChatGPT and other Gen AI resources quickly revealed the inherent risk embedded in these platforms. Chief among those risks for attorneys are ethical and privacy concerns based on how these platforms are exploited.

Ethical Concerns

The meteoric rise of open source Gen AI tools (e.g., Google's Bard, ChatGPT, Dall-E, etc.) exposed the risks that certain users may face when trusting these tools. Concerningly, a rapidly increasing number of lawyers have turned to ChatGPT and the like to perform their legal research and writing tasks. By now, most readers of this post have not only heard of the two New York attorneys sanctioned for filing legal briefs created by ChatGPT, that cited "hallucinated" court cases to support their argument. In addition, many may also tracking the latest and greatest on Michael Cohen – Donald Trump's former lawyer, who similarly may face sanctions for citing to "hallucinated cases" he found using Google's Bard. These are prime illustrations of why a user, especially an officer of the court, should not blindly rely on the material generated by these Gen AI tools.

This spur of sanctionable attorney activity has prompted several state bars, courts and individual judges to issue AI guidelines. Particular to an attorney's ethical obligations, California's guidelines provide that attorneys should consider disclosure to their clients when using Gen AI to create work product.[1]

Privacy Concerns

Users of Gen AI tools should be just as concerned with the information entered into Gen AI tools as the information generated by the platforms. For reference, ChatGPT and similar open source platforms, are built on large language models (LLMs) that use machine-learning algorithms to enable users to have a human-like conversation with the platform. Generally, this means that these tools will retain the input information to help it generate responses to future prompts. These Gen AI models are sometimes referred to as "black boxes" because users cannot determine exactly how the tool generated a response or what information the tool relied upon to provide the response. This creates glaring privacy concerns as the platform will store the information entered by a user and potentially provide that same information to another user.

The privacy policy posted on OpenAI's website, provides that "When you use our Services, we collect Personal Information that is included in the input, file uploads, or feedback that you provide to our

[1] A follow up information memo will provide more detail on state and federal court guidelines and/or rules related to use of Gen AI tools.

Services." Simply stated, there is no guarantee that information entered into ChatGPT will be treated as private or confidential.

With that, entering confidential information creates risk of an inadvertent disclosure, waiver of legally protected communications or violation of confidentiality. That means that an attorney entering client information to help generate legal arguments most likely waives attorney-client privilege over certain communications; or a school administrator entering student records could violate Family Educational Rights and Privacy Act (FERPA) privacy rules; or casual use by a company employee may lead to the inadvertent disclosure of a trade secret or other confidential or sensitive information.

Indeed, Chief Justice John Roberts in the Supreme Court's Year-End Report recognized that "any use of AI requires caution and humility. Some legal scholars have raised concerns about whether entering confidential information into an AI tool might compromise later attempts to invoke legal privilege."

As a general rule, users should avoid entering any privileged or protected information into Gen AI tools. Organizations should adopt policies regarding the risks and usage of Gen AI platforms to avoid any inadvertent disclosures by employees. When using a Gen AI tool, it is important to keep in mind that anything entered by the user may be shared with others.

Bond attorneys regularly assist and advise clients on drafting data privacy and cybersecurity policies. For more information regarding data privacy matters, please contact Jessica Copeland, Jackson Somes or any attorney in Bond's cybersecurity and data privacy practice.

Bond has prepared this communication to present only general information. This is not intended as legal advice, nor should you consider it as such. You should not act, or decline to act, based upon the contents. While we try to make sure that the information is complete and accurate, laws can change quickly. You should always formally engage a lawyer of your choosing before taking actions which have legal consequences. For information about our firm, practice areas and attorneys, visit our website, www.bsk.com. Attorney Advertising.