MINNESOTA STATE BAR ASSOCIATION

MAY/JUNE 2023

BENCH+BAR of Minnesota

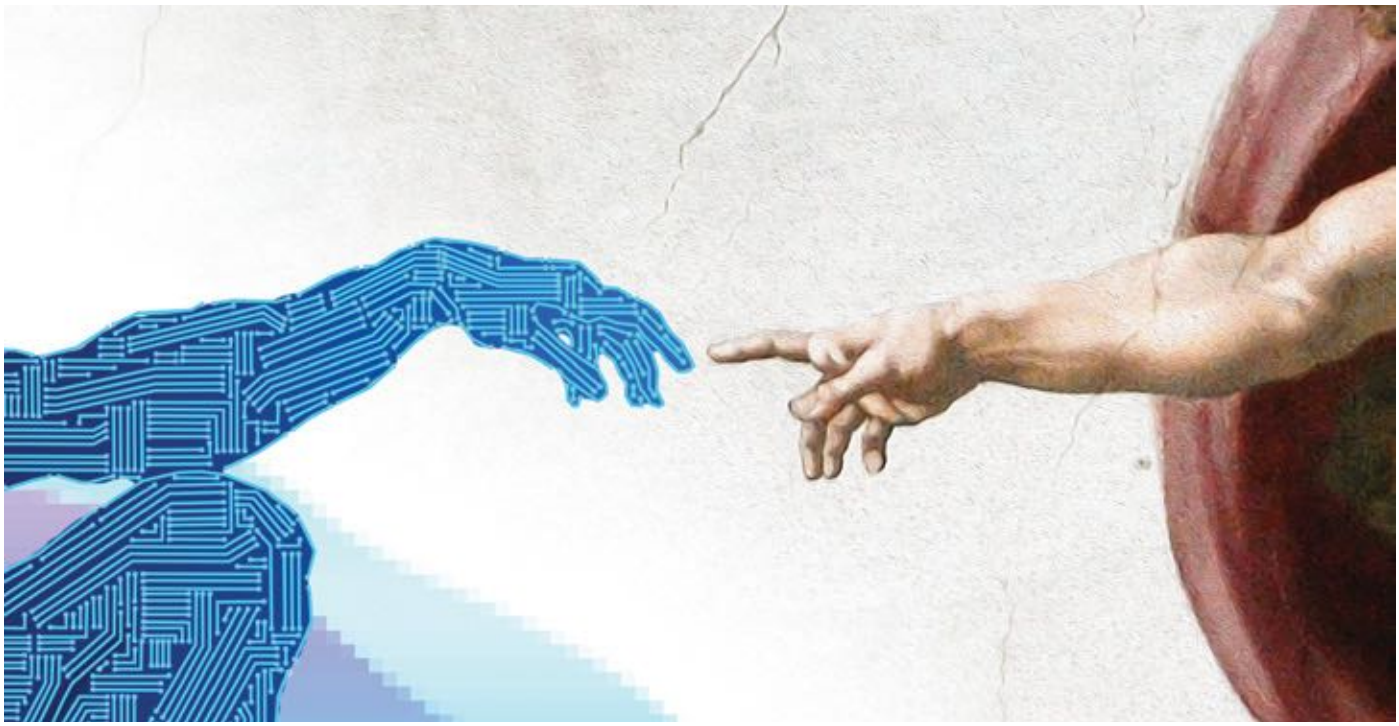
We need to talk about ChatGPT

A lawyer's introduction to the exploding field of AI and large language models

THIS ARTICLE IS HUMAN-WRITTEN

ChatGPT and navigating AI

BY MARK LANTERMAN ✉ *mlanterman@compforensics.com*



MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

Since its release in November 2022, ChatGPT has been met with a wide variety of responses. It's been praised for passing the bar exam.[1] It's been feared for its potential to replace certain jobs. It's been banned in Italy (at least temporarily). Its inherent security and privacy risks have been acknowledged, along with its potential for improving cybersecurity postures. AI has been a much-discussed topic in recent months, and with good reason.

In an open letter titled "Pause Giant AI Experiments" from the Future of Life Institute, signed by the likes of Elon Musk and Steve Wozniak, the question is posed: "*Should* we develop nonhuman minds that might eventually outnumber, outsmart, obsolete and replace us?... Powerful AI systems should be developed only once we are confident that their effects will be positive and their risks will be manageable."[2] The letter asks for a six-month pause on training for "AI systems more powerful than GPT-4," and calls for increased governance, safety protocols, and improvements in accuracy and transparency. The letter was recently referenced by a group of European Union members requesting a global summit on AI to establish governance for its "development, control, and deployment." In an open letter from these EU lawmakers, responsibility and internal cooperation are highlighted as necessary components in ensuring that progress in AI remains "human-centric, safe, and trustworthy."[3]

The utilization of new technology always comes with a caveat—namely, that gains in convenience result in losses to security. AI, and the ubiquity of ChatGPT more specifically, have presented an especially complex and multifaceted conundrum for individuals, organizations, firms, governments, and security professionals, to name a few. The potential benefits seem overwhelming—reduced time spent on simple tasks, improved efficiency in problem-solving, and limited costs to clients being prime examples. In the words of a recent ABA Journal column, "Despite its current shortcomings, ChatGPT has the potential to significantly enhance efficiency in the delivery of legal services... It can be a tremendous time-saver and is a great place to start your research on just about any topic. But whether you use ChatGPT for personal or professional reasons, you'll need to have a full understanding of the issue at hand and should thoroughly review, edit and supplement any results or draft language it provides you."[4]

First drafts, letters, and correspondence with clients could all be supported with the use of AI.

But actually using the information generated by AI tools requires a great deal of discretion and careful review. As of right now, inaccuracies, false information, and misleading statements abound. The time required to fact check, and the efforts required to mitigate any problems resulting from an error slipping through the cracks, may diminish or even negate the convenience factor. Furthermore, many observers are acknowledging the possible negative impact on new lawyers, with AI taking away opportunities for valuable experience. This reality is of great concern outside the legal community as well, as AI may begin to replace the skillsets of human beings. Additionally, ethical questions have arisen as to what can be legally used from a chatbot conversation, since it may contain trademarked, copyrighted, or simply false information.[5]

The double-edged nature of AI is similarly challenging from a cybersecurity perspective. The benefits may include an improved ability to automate security measures, including those needed for monitoring and detection.[6] But it can also be utilized by cybercriminals to assist in the creation of malware or more convincing phishing attacks. Notably, ChatGPT suffered its own data breach in March, which resulted in the leak of users' personal information and conversation content.[7]

The all-too-critical human element of security especially comes into play when analyzing the risks and benefits of this tool. When any new technology is incorporated into an organization, it is important to fully map out how that technology will be used, and then communicate that information clearly to employees. While ChatGPT urges users to avoid entering sensitive information into conversations,[8] confidential data and personal identifiable information are being entered nonetheless; in some instances, employees themselves are entering confidential company information, constituting a data breach. The tool itself is trained on vast amounts of data gathered from the internet, further blurring an important question—is it ethical to use ChatGPT, given the way it was, and continues to be, trained? If yes, what parameters should be created to regulate its use? If no, how will future AI projects be regulated?

At the time of this writing, Italy has banned ChatGPT, citing violations against the European General Data Protection Regulation (GDPR): "OpenAI doesn't have age controls to stop people under the age of 13 from using the text generation system; it can provide information about people that isn't accurate; and people haven't been told their data was collected. Perhaps most importantly, its fourth argument claims there is 'no legal basis' for collecting people's personal information in the massive swells of data used to train ChatGPT."[9] In spite of this list, it may be reinstated by the time you read this should OpenAI comply with a set of hard and fast rules required by the Italian Data Protection Authority. Regardless of the outcome, overarching concerns surely remain.

For a lot of us, the recent conversations surrounding chatbots and AI may feel like a sci-fi movie, with robots overpowering humans and taking over the world. What happens when technology gets *too* smart, if the conveniences afforded by technology become *too* convenient, literally replacing the very human beings who created it and allowed it to flourish? It's certainly an interesting (if scary!) thought, and while not everyone concurs with such an alarming viewpoint, the rapid development of AI certainly requires political attention, careful planning in its applications, and a complete-as-possible assessment of its extensive societal impact.

For the legal community, the question of how to best implement AI will likely be complicated as these issues unfold. While it seems safe to say that many, if not most, organizations will soon be using AI at least in some capacity, law firms are always held to a higher standard in managing client data and ensuring a strong security posture. Though the immediate benefits of a quickly written draft or assistance in correspondence may be tempting, be sure to bide your time in approaching AI and establishing how it will be incorporated into your firm. Specify what data can be entered into conversations, train employees in appropriate use, and establish guidelines for how your firm will use the tool in the most productive and secure way possible. ▲

NOTES

[1] *https://www.abajournal.com/web/article/latest-version-of-chatgpt-aces-the-bar-exam-with-score-in-90th-percentile*

[2] *https://futureoflife.org/open-letter/pause-giant-ai-experiments/*

[3] *https://www.cnbc.com/2023/04/17/eu-lawmakers-call-for-rules-for-general-purpose-ai-tools-like-chatgpt.html*

[4] *https://www.abajournal.com/columns/article/the-case-for-chatgpt-why-lawyers-should-embrace-ai*

[5] *https://news.bloomberglaw.com/us-law-week/employers-should-consider-these-risks-when-employees-use-chatgpt*

[6] *https://www.forbes.com/sites/forbestechcouncil/2023/03/15/how-ai-is-disrupting-and-transforming-the-cybersecurity-landscape/?sh=2c41fff34683*

[7] *https://openai.com/blog/march-20-chatgpt-outage*

[8] *https://help.openai.com/en/articles/6783457-what-is-chatgpt*

[9] *https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/*