Beware of Ethical Perils When Using Generative AI!

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

Generative AI is Alluring to Lawyers, but is it Safe?

According to a Lexis Nexis survey released in March 2023, 60% of lawyers have no plans to use generative AI at the present time. Considering that OpenAI's ChatGPT was only released in November of 2022, that's not particularly surprising. Lawyers are certainly not noted for rapidly adopting new technology.

What's astonishing to us is how many lawyers HAVE started working with generative AI, most often ChatGPT, which will largely be the focus of this article. Google's Bard and Microsoft's Bing Chat (based on ChatGPT) are still edged out by OpenAI's ChatGPT in studies – and our own unscientific observation is that far more lawyers are using ChatGPT compared to its rivals. ChatGPT is the fastest growing app ever released with over 100 million active users just two months after its release.

We have been bombarded with requests to present webinars on how lawyers can use ChatGPT in their law practice - in the seminars presented thus far, lawyers have peppered us with questions about how generative AI can be used by lawyers AND questions about its ethical and cybersecurity ramifications.

How is it being used? Our very incomplete list includes prediction of case outcomes, e-discovery, brief composition, contract review, legal research, brief analysis, writing briefs, predictive analytics, deposition questions, document review, billing and litigation support, due diligence, jury screening, online dispute resolution, and composition of emails.

Validate, Validate, Validate

What ChatGPT writes is generally well written. But taking it at face value as the truth would be a mistake. And yes, the human tendency is to do just that.

This was noted by Allen & Overy, which is in the process of globally rolling out OpenAI-based chatbot Harvey. In a directive to its lawyers, it wrote, "You must validate everything coming out of the system. You have to check everything."

Author Nelson can confirm the wisdom of that advice. She asked for case law on two separate issues with hyperlinks to references about the cases. ChatGPT responded with incorrect or partly correct information. Some "facts" appeared to have been made up. And virtually all the

hyperlinks didn't work. Some of that may have been "link rot" because the links were no longer available, but all of them??? Never use an AI provided hyperlink without verifying it!

What is With AI Hallucinations?

Lawyers are simply not used to the word "hallucinations" being used with respect to AI, though it is critical to understand that AI systems do sometimes hallucinate – and yes, that is the word used by its creators.

Generative AI mixes and matches what it learns, not always accurately. In fact, it can come up with very plausible language that is flatly wrong. It doesn't "mean to" but it makes things up – and that is what AI researchers call a "hallucination" - which is certainly not something that a lawyer would wish to cite in a brief! Hallucinations can be so egregious that they are easy to identify because they are clearly not relevant or read like utter nonsense. They are harder to spot when they are simply incorrect!

Competence with Technology/Duty of Confidentiality/Communications with Clients/Supervision

First, remember that the last data dump to ChatGPT was in 2021. So if what you need depends on data after that, it cannot help you. Reportedly, the database will be updated later this year. This is when you need to turn to Bing Chat, as it is internet connected.

Next, AI is largely a "black box" – you cannot see inside the box to see how it works. This is why validation is so critical. It was never intended that AI would "be a lawyer" so lawyers must make sure that the assistance of AI does not substitute for a lawyer's legal judgment.

It is important to discuss and obtain the agreement of clients that AI will be used, and with appropriate safeguards – do you really want to enter identifiable data about a client matter into the AI? How can you ensure that any such data will not become public? What if the AI itself suffers a breach? Also, the output of the AI respecting a client matter should not be shared with unauthorized individuals.

Ah, and one more conversation with clients that you may ethically need. Soon, it may be that you must justify NOT using AI in legal matters, especially where the cost savings would be significant. The duty of candor may play more of a role in an AI world.

We mentioned the law firm Allen and Overy above. The firm talks about using silos to protect firm data, presumably within a single office or perhaps a practice area. While we do not know the specifics (laudable caution on the firm's part) it sounds like they are taking a hardline and prudent approach to the protection of client data, even within the firm itself.

Data breaches of the AI itself may pose a significant threat. ChatGPT has indicated to the authors that AI systems are a prime target for hackers. It has recommended "implementing strong authentication protocols, regularly monitoring systems for vulnerabilities, and using encryption."

It is important to stay current on the latest threats and defenses. Make sure that any AI system you use is designed to ensure privacy and security. Also, make sure you have regular cybersecurity assessments (and the much more expensive penetration testing if you are large enough to warrant it).

It also warned against adversarial attacks, in which an attacker manipulates AI systems, producing inaccurate or misleading results. As it points out, this could be especially damaging in a legal context where the stakes might be very high.

Other Ethical Concerns

There may be bias in the training data. Historically, there have been a lot of court decisions reflecting bias. You don't want that bias reflected in your work.

What will happen if you receive output from AI which is conflicting? Do you get to cherry-pick the language which favors your client – transparency may become an increasingly important ethical concern.

Make sure the material the AI gives you is not plagiarized.

Cite the AI as the source.

Remember your duty of supervision! You must supervise both lawyers and non-lawyers, INCLUDING AI.

Final Words

Lawyers fear being replaced by AI, but we think the future of AI and the profession of law may be summed up as follows (hat tip to Erik Brynjolfsson, Director, Stanford Digital Economy Lab):

"Lawyers working with AI will replace lawyers who don't work with AI"

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional. mmaschke@senseient.com.*