Proskauer

Developing Litigation Issues

June 2023

The seventh Webinar in the “Age of AI” series focused on the risk factors at the intersection of litigation and AI. The presenters started with a brief background on AI and the practice of law and shifted to guidance in advising clients in this area, particularly with respect to the liability of AI platforms, FTC scrutiny of AI tools, and AI-related issues in ethics and antitrust.

The advent of AI and generative AI feels new, untested and perhaps of limited utility for some industries, such as for the practice of law. The presenters compared the current sentiment about AI with the reticence felt by many industries when the internet first started to grow in popularity and use in the mid- to late 1990s, even noting how one state bar ethics opinion advised attorneys doing legal research on the internet to ensure the information is reliable. The presenters opined that these same types of issues and concerns are once again arising with today’s new technology applications involving AI.

The Practice of Law and AI

It is possible that using AI tools could result in a waiver of attorney-client privilege and the confidential nature of information, particularly when using publicly facing AI tools such as ChatGPT, which, by default, shares user inputs with the developer for training purposes. Some potential methods to mitigate such risk include the use of AI tool APIs (e.g., ChatGPT API data is not used to train or improve the ChatGPT model but is only retained for 30 days to monitor for “abuse and misuse” and even non-API users can change default settings to disable training and data retention). The presenters noted that the safest action for practicing law is to simply avoid inputting any confidential information into an AI tool, suggesting that caution be taken in the way a lawyer frames a query, as even an apparently plain-worded query, if disclosed, could reveal hints as to confidential work or issues that a lawyer is analyzing for an active litigation, for example.

Practitioners might also consider a bespoke enterprise license from an AI provider that would typically offer more robust data protections than a publicly facing product and would be structured as an internal AI tool that is siloed but relies on a base AI for general knowledge. One important question in such an arrangement, according to the presenters, is whether the developer allows the customer to control the incremental knowledge that is gained through internal queries to the AI tool; such issues must be carefully considered, along with practical issues such vendor lock-in (as, depending on the underlying agreement, the customer could conceivably only control such incremental knowledge gain as long as it is still a customer) and the potential pricing power a licensor would have over the licensee in such a situation.

As to the rules of professional conduct, the presenters noted several issues that are relevant with the use of AI, including the duty of confidentiality, duty of competence in the benefits and operation of technology and a duty of candor to the tribunal. The latter concern was a principal issue in an ongoing litigation that made the news when plaintiff's counsel in motion papers cited six non-existing cases that were produced by ChatGPT, and later spotted as "bogus" by opposing counsel, prompting the court to set a date for a hearing on possible sanctions. This incident prompted some federal judges from other jurisdictions to require attorneys to make certain attestations regarding court filings that were drafted with the assistance of AI tool (with no judge instituting an outright ban on the use of AI tools for legal filings).

Another topic in this area is AI and legal document creation, which is one step beyond using AI to search for information, rather using AI to create a legal document such as a contract, legal brief or something else. The presenters pointed out the benefits of AI-assisted work product, such as expediting the creation of legal documents and other uses in discovery or detecting errors in basic forms and contracts, but noted that, in the short term, AI tools are not advanced enough to replace a lawyer's function but can only assist in certain basic efficiencies. Importantly, the presenters pointed to the New York State Bar Rules of Professional Conduct, Rule 1.4(2), which concerns disclosure to clients about how the client's objectives are to be accomplished. Thus, the presenters stressed that if a lawyer is intending to use AI to research issues, draft documents or perform similar functions, it likely makes sense that the lawyer should ensure the client agrees with the use of such technological methods, with such issues perhaps memorialized in the client engagement letter.

The presenters closed their discussion about AI and the practice of law with a brief mention of investment advisors and AI. Like the practice of law, a core foundational duty of an investment advisor is a duty of care and a duty of loyalty. For example, as pointed out by the presenters, a duty of care in in this instance would require the investment advisor to act in the best interest of the client, including a duty to provide advice suitable to the client, which includes a reasonable investigation into the investment and to avoid basing investing advice on material inaccurate or incomplete information. Thus, according to the presenters, one could see how the use of generative AI tools, which contain disclaimers about the fabricating of content, by an investment advisor could implicate these principles (e.g., an investment advisor using AI to make investment decisions for a client could implicate both duties). On a related note, the SEC has expressed concerns on AI and its programming. For example, the SEC has pointed out the potential for concentrated risk from multiple trading platforms using the same predictive analytics AI tools to make investing decisions and mitigate risk could actually produce wide-ranging risk in the markets if multiple platforms relied on the same AI-produced analysis.

Liability surrounding AI Tools

While the first part of this webinar presentation outlined the many ways that use of AI tools might go wrong, the next question is: Who is going to be liable? Liability risk, wherever it may fall, has important implications, such as steering developers into altering their products to reduce such risks. The presenters started the discussion about potential methods AI generators can use to limit liability, such as through:

- **Disclaimers**: AI generators have used disclaimers on their websites to seek to limit potential liabilities (e.g., “May occasionally generate incorrect information”; “May occasionally produce harmful instructions or biased content”). Are these sufficient? The presenters noted that perhaps such contractual disclaimers could be deemed enforceable against the user who is presented with such disclaimers and continues to use the service. However, such disclaimers may not necessarily protect against liability when the service impacts third parties.
- **Third party liability**: As the presenters noted, AI generators would necessarily have to consider whether Section 230 of the Communications Decency Act (CDA) would provide immunity from claims that seek to treat the service as the publisher or speaker of any information provided by another information content provider.

The presenters framed the issue this way: Are there claims that you can bring against an AI generator or generative AI platform that do not depend on it being the publisher of third party content? Would the generative AI platform be deemed the content creator of output (no immunity) or merely the publisher of third party content and prior training data (potential immunity under CDA Section 230)? The presenters noted that one might argue that generative AI tools, merely by their name, suggest they "generate" content and thus would not enjoy CDA immunity like a social media platform that hosts user-generated content. On the other hand, one could make an alternative argument that a generative AI tool is not a person or entity creating independent content, rather an algorithm that arranges third party training data in some useful form in response to a user prompt, and thus should be protected by CDA immunity for output. To this point, courts have not ruled on this issue, so the area remains unsettled, particularly when the Supreme Court recently declined the opportunity to comment on CDA immunity as it pertains to algorithmically-organized content in the *Twitter* and *Gonzalez* To be sure, based on those Supreme Court decisions, an AI developer may not even need to rely on CDA immunity to avoid secondary liability for certain actions if it has released a lawful, general-purpose, neutral tool that was subsequently employed unlawfully by users.

- **FTC scrutiny – deceptive advertising**: On another front, the presenters reminders viewers about the FTC's own enforcement powers over unfair and deceptive trade practices. The agency released guidance stating how "AI can turbocharge fraudulent practices" and that "firms should be on notice that systems that bolster fraud or perpetuate unlawful bias can violate the FTC Act" and that "there is no AI exemption to the laws on the books." In fact, the FTC recently released a report about how it is concerned that "AI tools can be inaccurate, biased and discriminatory by design" and that the agency would focus its enforcement priorities on the use of AI with regard to deceptive advertising and unfair competition: "The FTC has also warned market participants that it may violate the FTC Act to use automated tools that have discriminatory impacts, to make claims about AI that are not substantiated, or to deploy AI before taking steps to assess and mitigate risks." The presenters asked that, given these statements by the FTC, entities should consider building extra protocols if an AI generator's product is going to be used for to generate advertising. Even given the use of conspicuous disclaimers, the law remains unsettled as to these questions.
- **FTC scrutiny – antitrust**: The FTC is focused on whether the changes that AI will bring into our society is consistent with antitrust laws. Already, FTC Chair Lena Khan has noted that there is already the risk that established players in the AI industry will be tempted to unlawfully restrain new entrants to maintain their dominance and that "a handful of powerful businesses control the necessary raw

materials that start-ups and other companies rely on to develop and deploy AI tools." Thus, as the presenters noted, it all comes down to data. Current AI tools are trained on huge datasets of information scaped from the web. However, now content and media companies that before unknowingly provided data for the development of generative AI have asked for payment or a license for future use of their content. It should also be noted that standard website terms of service typically prohibit the scraping of their content using automated means and thus such web content may not be "free" or available to train AI, as a matter of contract. The open question is: Are such restrictive website terms lawful, and can they be enforced in these instances? The FTC has hinted that such "take-it-or-leave-it" web contracts might constitute unfair methods of competition, in certain circumstances, but this issue is certain to play out in the future development of generative AI and whether the FTC will bring enforcement actions against entities that attempt to stop developers from using publicly-available website data for AI training purposes.

- **Additional antitrust issues**: From a high-level perspective, the presenters noted that innovation and disruption routinely breed antitrust concerns, and in in the current climate, we may see incumbents seek to unlawfully restrain AI companies that may be perceived to be threatening established businesses. On the other hand, incumbents could also seek to use AI to maintain their competitive positions. The presenters stated that just as agreements to block AI use and development could be deemed anti-competitive, so can agreements to adopt it (e.g., competing firms entering into separate agreements with a single AI platform that uses a common pricing algorithm could be alleged to be collusion). From an enforcement perspective, the presenters also noted that regulators and enforcers have taken note that in bringing such cases, a company's use of algorithms leaves behind a digital trail that could be examined by regulators.

Related Professionals

- **Colin Kass**
  Partner
- **Timothy W. Mungovan**
  Chairman of the Firm