MASSACHUSETTS Lawyers Weekly

Part of the BRIDGETOWER MEDIA network ■ APRIL 17, 2026

Attorney-client privilege in the AI era: What does 'Heppner' mean for practitioners?

■ KURT B. FLIEGAUF AND DANIEL WALSH-ROGALSKI

New York Judge Jed S. Rakoff's ruling in *United States v. Heppner* — that a criminal defendant's written exchanges with AI platform "Claude" are not protected by the attorney-client privilege or the work product doctrine — has spread like wildfire throughout the legal community. And for good reason. As Judge Rakoff noted, "more than half of United States households have adopted AI in some form."

Kurt B. Fliegauf

Daniel Walsh-Rogalski

As AI becomes more ubiquitous, practitioners must be prepared to navigate the complex legal issues left in its wake.

BACKGROUND, PROCEDURAL HISTORY

The defendant in *Heppner* was indicted on charges of securities fraud, wire fraud, conspiracy, making false statements to auditors, and falsifying corporate records. *United States v. Heppner*, 2025 WL 436479, at *1 (S.D.N.Y. 2026).

After the government seized the defendant's computer, defense counsel asserted privilege over his stored communications with Claude. Although the communications had been made by the defendant without instruction from counsel, his attorneys argued that the communications nonetheless should be protected because they outlined anticipated defense strategy and potential factual and legal arguments in anticipation of a potential indictment.

Judge Rakoff concluded that the defendant's AI materials failed to satisfy at least two, if not all three, of the elements of attorney-client privilege.

First, the judge held that the documents were not communications between client and counsel because Claude is not an attorney, and discussions of legal issues between non-attorneys are not privileged.

The judge reasoned that all recognized claims of privilege to date have involved a "trusting human relationship" and found that "[n]o such relationship exists, or could exist, between an AI user and a platform such as Claude."

He also noted that, when prompted, Claude acknowledges it is not a lawyer, that it cannot provide legal advice, and it recommends consulting a qualified attorney.

Second, the judge found the communications were not confidential. He highlighted Claude's written privacy policy, emphasizing that users consent to the collection of inputs and outputs, use of data to train Claude, and disclosure to third parties including governmental authorities, with notice that data may be disclosed in connection with claims, disputes or litigation.

Rakoff reasoned that AI users have limited privacy interests in conversations voluntarily disclosed to a publicly accessible platform that retains such data in the ordinary course. He found that the defendant's AI inputs and outputs were distinct from client notes prepared with the intent of sharing with counsel because the defendant's were first shared with a third party.

Third, the judge acknowledged defense counsel's argument that the defendant used Claude to facilitate discussions with counsel but highlighted that counsel did not direct the defendant's use of AI. If defense counsel had instructed him to use Claude, Rakoff acknowledged that "Claude might arguably be said to have functioned in a manner akin to a highly trained professional who may act as a lawyer's agent within the protection of the attorney-client privilege."

After *Heppner*, the U.S. District Court for the Eastern District of Michigan found that a pro se litigant's use of AI tools was protected by the attorney-client privilege. *Warner v. Gilbarco*, Case No. 2:24-cv-12333, 2026 WL 373043 (E.D. Mich. Feb. 10, 2026).

While an interesting wrinkle, it is likely that the well-reasoned *Heppner* decision will be adopted by most other judges.

WHAT TO ADVISE CLIENTS

Every litigator can imagine a scenario similar to *Heppner*, in which a client, without prompting by their attorney, inputs specific information concerning their legal matter into an AI tool. This may occur prior to when the attorney is consulted, when an individual is in the process of determining whether they have a valid claim or defense.

For example, a human resources director may ask an AI tool to generate a report to determine whether an employee would have a valid discrimination claim if adverse employment action is taken. A

client may input facts into an AI search to determine how they will impact liability if uncovered during discovery. Under the *Heppner* ruling, all of this information is likely discoverable.

In light of the significant risks exposed by the *Heppner* decision, Massachusetts attorneys have begun to sound off how on how to address clients' widespread use of AI.

On a recent webcast, Michelle Peirce, co-chair of the white-collar criminal/government regulatory practices at Hinckley Allen, said: "One big lesson from *Heppner* is that lawyers have to warn their clients — early and often — about the risks of using AI to research their legal matter."

Kenneth Thayer, a business litigation partner at Conn Kavanaugh added: "While Massachusetts courts have not yet addressed this issue, attorneys should assume, at least for the time being, that a client's use of public, non-enterprise AI tools would likely waive any privilege. Accordingly, we should advise our clients not to use those tools in connection with their cases — and certainly to refrain from inputting any information into those tools that could be construed as an admission of wrongdoing or a weakness in their case, as such information could end up being produced in discovery."

Matthew Costello, counsel at Nixon Peabody, similarly weighed in on the overarching impact of *Heppner*, noting that litigators in particular should focus on the issue:

"Heppner should prompt every litigator to consider having an early conversation with clients about their use of AI. Many clients may already be turning to widely used consumer AI tools to research their legal exposure before they ever call a lawyer, and under Heppner, those communications could well be discoverable. Practitioners should consider treating AI usage the way we treat document preservation: advising clients at the outset of any dispute to exercise caution before inputting case-related facts into consumer AI platforms. On the flip side, AI chatlogs and prompts are worth considering as standard items in discovery requests — they may reveal a party's unfiltered, candid assessment of their own case."

The risk of disclosure of a client's highly sensitive information shared with AI is sufficiently significant and novel that law firms even should consider warning their clients against the practice in their engagement letters. As Conn Kavanaugh litigation partner Michael Rossi put it: "We can't possibly include every warning in an engagement letter, but AI is so new, and the consequences if it's used incorrectly are so significant, that it may make sense to flag it right at the start of a matter."

Attorneys must be aware, and make sure that their clients are aware, that communications and data exchanged with the most popular AI tools lack the confidentiality necessary for protection under the attorney-client privilege.

Practitioners should advise their clients not to use AI platforms in connection with their legal disputes, as the content of any information that is inputted into such platforms by a client is likely discoverable.

FURTHER AI CONSIDERATIONS FOR LEGAL PRACTICE

What about lawyers' use of AI? Is a lawyer's communications with an AI tool at risk of being discoverable? It likely depends on the AI tool that is utilized.

In Heppner, the judge relied on Claude's terms of service and highlighted that Claude's privacy policy provides that Anthropic, the company that operates Claude, collects data input by users and utilizes that data to train its AI model.

The Heppner court's reliance on Claude's terms of service is significant as Claude is one of the three most commonly used AI tools by the general public, along with ChatGPT and Google Gemini. All three AI tools have similar terms of service. Accordingly, practitioners must be aware that under the policies of the three most commonly used AI tools, any information that is entered — including information entered by counsel — is subject to disclosure.

To maintain confidentiality, lawyers should use only "non-custodial" AI tools — i.e., AI tools that do not employ user prompts to improve their products, and do not retain data in a format that can be accessed by anyone other than the user.

AI platforms such as Thomson Reuters' AI tool CoCounsel and Google's business version of Gemini contain different privacy terms and reportedly do not utilize user prompts to improve their products. Open AI's terms of use also allow users to "opt-out" of the use of user data to train its models.

Presumably, information shared with such "non-custodial" AI systems will be deemed confidential, such that an attorney's work product used in connection with AI is not deemed waived. Indeed, lawyers regularly share confidential information on technology platforms that are stored by third parties, such as email and voice mail that is stored "in the cloud."

So long as the hosting platforms are unable to access the data, then the attorney-client privilege and/or work product doctrine should apply. The same analysis should apply to "non-custodial" AI tools.

CONCLUSION

Attorneys must remain diligent, especially since federal courts are already diverging in their approaches to interpreting AI use. Not only is this a matter of common sense, but ABA Ethics Opinion 512 generally advises that attorneys are obligated to familiarize themselves with AI and keep apprised of the development of this technology.

As AI continues to evolve, so will its impact on the practice of law, and Massachusetts practitioners must be ready.

Kurt B. Fliegauf is a litigation partner, and Daniel Walsh-Rogalski a litigation associate, at the Boston-based law firm Conn Kavanaugh Rosenthal Peisch & Ford, LLC. They can be contacted at kfliegauf@connkavanaugh.com and dwalsh-rogalski@connkavanaugh.com, respectively.