Preserving Privilege in the Age of AI: Key Lessons from *United States v. Heppner*

By Elaine F. Harwell

A federal court in the Southern District of New York has handed down what already may be one of the most consequential legal technology rulings in 2026. In ***United States v. Heppner***, No. 25 CR. 503 (JSR), 2026 WL 436479, (S.D.N.Y. Feb. 17, 2026), the court addressed important questions of first impression: whether, when a user communicates with a publicly available AI platform in connection with a pending criminal investigation, the AI user's communications are protected by attorney-client privilege or the work product doctrine. In both instances, the court answered no.

Factual Background

Bradley Heppner was indicted in October 2025 on charges of securities fraud, wire fraud, conspiracy, making false statements to auditors, and falsifying corporate records in connection with his alleged misconduct as a business executive. After receiving a grand jury subpoena, Heppner used a publicly available AI platform (Claude) and created approximately thirty-one documents memorializing what his counsel eventually described as communications outlining defense strategy and potential legal arguments. Heppner asserted privilege over these documents, arguing that he had inputted information learned from counsel, had created the documents to facilitate conversations with counsel, and had subsequently shared the documents with counsel. In considering whether the documents were protected by attorney-client privilege or the work product doctrine, the court ultimately rejected all of Heppner's arguments and granted the government's motion to compel production of the AI-created documents.

Attorney-Client Privilege

Generally, the attorney-client privilege attaches to communications (1) between a client and his or her attorney (2) that are intended to be, and in fact were, kept confidential (3) for the purpose of obtaining or providing legal advice. The court found that Heppner's AI-generated documents failed at least two, if not all three, of these elements.

First, the court found the AI documents were not communications between Heppner and his counsel. Perhaps obvious, but important for the court's analysis, the court found that Claude is not an attorney. This alone disposed of Heppner's claim of privilege. The court was unmoved by the argument that AI inputs are more analogous to the use of cloud-based word processing software, reasoning that all recognized privileges require a trusting human relationship and, in the attorney-client context, a relationship with a licensed professional who owes fiduciary duties and is subject to discipline. No such relationship existed, or could exist, between an AI user and a platform such as Claude.

The court also found the communications with the AI platform were not confidential. Specifically, the court noted that Heppner communicated with a ***public*** third-party AI platform which required users to consent to their privacy policy. The privacy policy disclosed that Anthropic (the private company operating Claude) collected data on both users' inputs and Claude's outputs, used such data to train Claude, and reserved the right to disclose such data to a host of third parties, including governmental regulatory authorities. The court further noted that AI users do not have substantial privacy interests in their conversations with a publicly accessible AI platform, which users voluntarily disclose to the platform and which the platform retains in the normal course of its business.

Heppner also did not communicate with Claude for the purpose of obtaining legal advice. Although Heppner's counsel asserted that he communicated with Claude for the express purpose of later talking to counsel, counsel also conceded that Heppner did not do so at the suggestion or direction of counsel. The court also rejected the argument that sharing the AI documents with counsel retroactively conferred privilege finding that it is black-letter law that non-privileged communications are not somehow changed into privileged ones upon being shared with counsel. Critically important was the court's finding that even if certain information that Heppner input into Claude was itself privileged, he waived that privilege by sharing the information with Claude and Anthropic, just as if he had shared it with any other third party. In light of Anthropic's privacy policy, Heppner had no reasonable expectation that the inputs would not be shared with other third parties.

Work Product Doctrine

The work product doctrine provides qualified protection for materials prepared by or at the direction of counsel in anticipation of litigation or for trial, and its availability in reference to materials in the possession of a client depends upon the existence of a real, rather than speculative, concern that the thought processes of the client's counsel in relation to pending or anticipated litigation would be exposed.

In ***Heppner***, the court found the AI documents did not merit work product protection because, even assuming they were prepared in anticipation of litigation, they were not prepared by or at the direction of counsel. Heppner's counsel confirmed they were prepared by Heppner on his own volition and while the AI documents did affect counsel's strategy going forward, they

BACK to Inside this issue
Continued on page 17

Preserving Privilege in the Age of AI... | *continued from page 16*

did not reflect defense counsel's strategy at the time Heppner created them. As Heppner was not acting as his counsel's agent when he communicated with Claude, the doctrine's core purpose of protecting the mental processes of the attorney was not implicated.

Key Lessons from *Heppner*

In light of ***Heppner***, attorneys should consider the following immediate and practical steps when using or advising clients about AI tools:

- Avoid inputting privileged client information into any public AI platform. If AI assistance from a public platform is used, ensure that factual inputs are anonymized or limited to non-privileged information.
- Consider using AI tools offered through enterprise agreements with robust confidentiality controls, data use and retention restrictions, and contractual prohibitions on third-party disclosure. Unlike public platforms, these arrangements may better support a claim of privilege or confidentiality.
- For work product purposes, the attorney should direct the AI-assisted task, actively review and edit the output, and ensure that the final work product reflects the attorney's own judgment and strategy.
- Counsel clients to use caution when undertaking use of AI tools. Consider advising clients not to independently use AI tools to generate materials related to pending or anticipated litigation without attorney guidance, and explain the potential waiver risks.
- As with all AI outputs, conduct rigorous reviews. The risks of inaccurate legal citations and fabricated authorities are a well-documented phenomenon that has already resulted in sanctions in several high-profile cases. All AI outputs should be independently verified before use.
- Check any specific disclosure obligations required by local court rules. Many local court rules, as well as evolving guidance in this space, require or encourage disclosure of AI-assisted work product.

Generative AI is truly a new frontier, but AI's novelty does not mean that its use is not subject to longstanding legal principles, and it does not alter the fundamental requirements of privilege. Maintaining traditional safeguards, exercising careful supervision over AI-assisted work, and employing the same diligence applied to any other legal work are not optional in the AI era. In addition, attorneys should expect more courts to weigh in on the discoverability of AI inputs and outputs as we continue to see widespread adoption of these tools.

Elaine F. Harwell is a partner at Procopio, Cory, Hargreaves & Savitch LLP.