SQUIRE
PATTON BOGGS

Recent Federal Court Decision Highlights Privilege Risks of Consumer AI Use

US – March 2026

A recent decision from the US District Court for the Southern District of New York highlights the risk for companies and individuals using consumer generative Artificial Intelligence (AI) tools in sensitive matters.

In *United States v. Heppner*, No. 25-cr-00503-JSR (S.D.N.Y. Feb. 17, 2026), the court held that materials created by a nonlawyer criminal defendant using a public, nonenterprise version of an AI tool were not protected by the attorney-client privilege, or the work product doctrine.

The ruling is among the first to squarely address how traditional privilege principles apply to a client's independent use of generative AI, and it offers important guidance for organizations navigating AI adoption.

Factual Background of *United States v. Heppner*

Federal prosecutors charged Bradley Heppner with various criminal offenses arising from his alleged role in a scheme that defrauded investors of more than US$150 million. During a search of his home, FBI agents seized several documents reflecting Heppner's exchanges with a consumer AI platform. Without any suggestion from counsel that he do so, Heppner used an AI tool to prepare reports on potential defense strategies. He later shared these AI-generated materials with his attorneys. After the government came into possession of the materials, Heppner argued that they should be protected by the attorney- client privilege and the work product doctrine.

Key Holding: No Privilege for Independent Consumer AI Use

The attorney-client privilege protects communications between an attorney and client that were intended to be confidential and made for the purpose of obtaining legal advice. The court's analysis rested on this settled doctrine, not on any AI specific rule. First, the court held that there was no attorney-client privilege because the AI chatbot "is not an attorney," and "that alone disposes of Heppner's claim of privilege." Second, even if that were not dispositive, the interactions occurred on a third-party AI platform whose privacy policy permitted collection of user "inputs" and "outputs," use of that data to "train" the AI model and disclosure to "third parties," including governmental authorities. Because the defendant voluntarily shared information under those terms, the court found no reasonable expectation of confidentiality. The court also rejected the argument that privilege could be created retroactively by later providing the AI-generated materials to counsel.

No Work Product Protection Either

Distinct from the attorney-client privilege, the work product doctrine protects material prepared by, or at the direction of counsel in anticipation of litigation. The court held there was no work product protection for Heppner's AI-generated materials because they were not prepared by counsel, or at counsel's direction and did not reflect counsel's legal strategy. As the court emphasized, the work product doctrine is designed to protect attorneys' mental impressions, not a client's unilateral research conducted through a consumer-level AI tool.

Narrow Decision, but Broad Implications

The court carefully limited its ruling to the facts before it. It did not address whether enterprise grade AI tools with stronger confidentiality and data protection controls should be treated differently, nor whether AI research conducted at the direction of counsel could qualify for work product protection. Even so, *Heppner* provides a clear warning that courts will evaluate AI use through the lens of traditional privilege principles, including attorney involvement, confidentiality and third-party disclosure.

Practical Takeaways for Businesses and Legal Teams

The decision offers several practical lessons. Consumer AI tools are not confidential by default and prompts and outputs may be treated as communications shared with a third-party. Sharing AI-generated materials with counsel after the fact does not create privilege retroactively. Work product protection likewise requires attorney direction; client only AI use, even for legal research, will not qualify. Tool selection therefore matters, as enterprise AI platforms with contractual confidentiality and limited data use present materially different risks than free or consumer tools. Finally, organizations should adopt clear policies and training governing AI use in matters involving legal, regulatory or litigation risk.

Legal departments should educate employees that inputting sensitive, proprietary or legally privileged information into consumer AI tools may waive privilege or create discoverable evidence. Where AI is used in connection with legal work, counsel should be involved early to assess whether the use is appropriate and to preserve any potential work product protections.

Bottom Line

Heppner reinforces that generative AI does not change the fundamentals of privilege law. What matters is who used the tool, for what purpose and under what confidentiality protections. As AI becomes further embedded in business workflows, careful governance and coordination with legal counsel will be essential to avoid unintended waiver of critical protections.

Should you have any questions or require specific advice, please reach out to your usual contact at the firm.

Contact

Steven Delchin
Senior Attorney, Cleveland
T +1 216 479 8278
E steven.delchin@squirepb.com

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.