When 'Ask AI' Becomes Exhibit A: Privilege, Waiver, and the Discovery Risks of Public AI Platforms

By: Jake Krattiger, Nick Merkley, Brian Tully, and Tyler Self

February 23, 2026

Executive Summary

A recent decision from the U.S. District Court for the Southern District of New York confirms that when clients independently communicate with a public AI platform, those exchanges are not protected by attorney-client privilege or the work product doctrine simply because they are later shared with counsel. In other words, these types of searches and inquiries, as well as the results, may ultimately be provided to the opposing party in discovery.

Although the case arose in a criminal context, the court applied traditional privilege principles that apply equally in civil litigation, regulatory enforcement, and internal investigations. The lesson is straightforward: communications with public AI systems may be discoverable, and forwarding them to counsel does not retroactively make them privileged.

United States v. Heppner, No. 25-cr-00503-JSR, 2026 WL 436479 (S.D. N.Y., Feb. 17, 2026). A link to the memorandum opinion is available here.

What Happened

After receiving a grand jury subpoena and knowing he was a target of investigation, the defendant used Claude (Anthropic's AI agent) to generate written analyses outlining potential defenses and legal strategy. He did so independently, without direction from counsel.

Federal agents later seized his electronic devices pursuant to a search warrant. The defendant asserted the attorney-client privilege and work product doctrine over the AI-generated materials.

The Court rejected both claims. New technology did not change old doctrine.

Attorney-Client Privilege

The court concluded that the defendant's exchanges with the AI platform could not be protected by the attorney-client privilege for several independent reasons:

- No Attorney Client Relationship – The AI platform was not a lawyer, and Claude explicitly did not hold itself out as providing legal advice. Privilege protects communications between a client and a licensed attorney (or the attorney's agents), not communications with a third-party technology provider. A software platform, even a sophisticated one, does not owe fiduciary duties.

- No Reasonable Expectation of Confidentiality – Claude's privacy policy allowed retention of user inputs and outputs, use of data for model training, and potential disclosure to third parties, including regulators. The court found that these terms defeated any reasonable expectation of confidentiality, a load-bearing pillar of attorney-client privilege.
- No Communication for the Purpose of Obtaining Legal Advice – Because counsel did not direct the defendant to use the AI tool, the relevant inquiry was whether the defendant sought legal advice from the platform itself. The platform expressly disclaimed providing legal advice, which undermined that argument.

The Court also reaffirmed a fundamental legal principle of black letter law: Documents that are not privileged when they are created do not become privileged when they are later shared with counsel.

Work Product Doctrine

The work product doctrine protects materials prepared by or at the direction of counsel in anticipation of litigation, particularly those reflecting counsel's mental impressions or strategy.

Here, the defendant acted on his own initiative. The AI-generated materials were not prepared at counsel's direction and did not reflect counsel's legal analysis at the time they were created. The fact that they later influenced counsel's thinking did not transform them into protected work product.

Noting that the materials were seized from the defendant at the time of his arrest pursuant to the search warrant instead of being produced as part of pretrial discovery, the federal district court found that Federal Rule of Criminal Procedure 16(b)(2)(A) was "inapplicable on its face." While this rule exempts materials "made by the defendant" from pretrial discovery, "[t]he Government did not request them, and [the defendant] did not produce them, in pretrial discovery."

The doctrine exists to protect the lawyer's mental processes. It does not protect a client's independent strategizing conducted through a third-party platform under the circumstances presented here.

Practical Implications for Companies

This ruling is not anti-AI, but a conventional application of longstanding privilege doctrines. The risk arises from how AI is used, particularly in the context of active or anticipated disputes.

Companies should assume that:

- Communications with public AI systems may be discoverable in litigation or investigations.
- Inputting legal advice, attorney communications, internal analyses, or strategy into a third-party AI platform may waive privilege.
- The intent to later share a document with counsel does not create privilege if it did not exist at the time of creation.
- Use of AI tools after receiving a subpoena, civil investigative demand, regulatory inquiry, or credible threat of litigation presents elevated risk.

If a dispute is on the horizon, a party's unsupervised searches and exchanges with an AI platform could later be used as evidence.

Recommended Steps to Protect the Company, Employees, and Customers

To reduce risk exposure, companies should consider implementing the following safeguards:

1. **Establish Clear Internal AI Use Policies** – Adopt written policies governing employee use of generative AI tools, including restrictions on entering confidential business information, customer data, trade secrets, attorney communications or legal strategy, or any information on pending or anticipated disputes. Policies should expressly state that public AI platforms constitute third parties for privilege purposes.
2. **Restrict AI Use in Legal and Regulatory Matters** – Prohibit independent use of public AI platforms for analyzing claims, defenses, investigation strategy, regulatory responses, or litigation risk without prior involvement of counsel. Require legal department approval before AI tools are used in connection with active disputes or investigations.
3. **Evaluate Data Governance and Vendor Risk** – Review AI platforms' terms of service and privacy policies to understand their data retention practices, model training use, disclosure rights, and any cross-border data implications. Importantly, these issues *may also* implicate customer privacy obligations and contractual commitments.
4. **Train Employees and Management** – Provide targeted training explaining how privilege works, how it can be waived, and why AI platforms are not confidential brainstorming tools.
5. **Recognize that AI is not a substitute for an attorney.**

Conclusion

The court framed this as a novel question, but the reasoning was not new. Privilege requires a lawyer, confidentiality, and purpose. Work product requires attorney direction or protection of counsel's mental impressions. Those principles apply regardless of whether the communication occurs by letter, email, or AI prompt.

Companies should address AI governance proactively. It is far less costly to implement guardrails now than to defend waiver arguments in the middle of litigation. If you have questions about creating or revising AI use policies, conducting internal training, or assessing risk exposure in pending matters, GableGotwals is available to assist.

This Alert was prepared by Jake Krattiger, Nick Merkley, Brian Tully, and Tyler Self. The litigation team at GableGotwals regularly advises clients on privilege, discovery strategy, internal investigations, regulatory inquiries, and high-stakes disputes. For assistance, please contact one of the authors or visit our Litigation Practice page.

Jake Krattiger
405-568-3301
jkrattiger@gablelaw.com

Nick Merkley
405-568-3311
nmerkley@gablelaw.com

Brian Tully
346-200-6017
btully@gablelaw.com

Tyler A. Self
405-235-5589
tself@gablelaw.com