

INSIGHTS + NEWS

New Tech Meets Old Law: Further Clarification on the Discoverability of AI Output

BY PAUL M. ROBERTSON • APRIL 7, 2026

Two recent federal cases, *Warner v. Gilbarco, Inc.*, No. (E.D. Mich. Feb. 10, 2026), and *United States v. Bradley Heppner*, No. 1:25-cr-00503-JSR (S.D.N.Y. Feb. 17, 2026), provide further clarity on how the attorney-client privilege and work product doctrine will be applied to AI output.

The takeaway is straightforward: the technology is new, but the governing legal principles are not. The rules governing the attorney-client privilege, the work product doctrine, and core duties of confidentiality still control. But how lawyers and their clients *use* AI will often determine whether protections are retained or lost.

The two rulings reflect a tension on how settled privilege principles apply to AI-assisted workflows. The *Warner* court held that a pro se plaintiff's self-initiated use of a public AI platform in connection with litigation did not waive work product doctrine and **were not subject to discovery**. The *Heppner* court, on the other hand, held that a criminal defendant's self-initiated uses of a similar AI tool constituted neither attorney-client communications nor work product and thus **were discoverable**.

The *Warner* court reasoned that AI platforms are “tools, not people,” and that the pro se civil plaintiff's use of AI was protected as work product because there had been no disclosure to an adverse party in the case.

The *Heppner* Court, on the other hand, focused on the fact that the AI platform warned that data would be retained and could be disclosed to third parties, specifically including the government. The court reasoned that the attorney-client relationship applies to communications with a “trusting human” attorney, not automated bots, that there could be no expectation of privacy in light of the platform's disclosure about retention and third-party disclosure, and, because the no claim that legal advice was being requested where the platform specifically disclaimed that it “can't provide legal advice.”

Heppner is likely fact-specific, driven by the platform's express warnings concerning data retention and third-party disclosure to the adverse party. On the other hand, read broadly, the *Heppner* decision could be read to stand for the proposition that communications between any party and an “in-human” AI tool can never be considered a protected communication with a “trusted attorney.”

How then can the *Warner* ruling be read consistently with the application of these same rules? In *Warner*, the court focused on the fact that the civil party was proceeding pro se and that work product protection can apply in such circumstances. The Court further focused on the fact that the work product protection applies to prevent discovery of materials prepared in anticipation of litigation “by or for another party,” and that no attorney need be involved. The

pro se defendant's AI use did not waive work product protection because disclosure to AI, which is a "tool" and not a "person," did not rise to the level of disclosure to an **actual adversary**.

Critically, the Court pushed back on the published thought pieces that warn that use of generative AI creates a risk of disclosure, writing that no court has ever endorsed such a broad waiver argument, and that compelling disclosure would "nullify work product protection in nearly every modern drafting environment."

Read together, the cases suggest that AI does not alter privilege doctrine, but it does amplify the importance of understanding the nature of the platform being used and the context in which that use occurs. Where a platform's terms or functionality undermine a reasonable expectation of privacy, privilege is unlikely to attach. Where AI functions as a controlled tool within a confidential legal workflow, traditional protections are likely to remain available.

KEY TAKEAWAYS

Read broadly, the *Heppner* case, would result in the waiver of privileges any time a "non-human" platform is used, including Gmail, Westlaw, or Lexis, or when an eDiscovery platform is relied upon for document review. That broad reading was rejected by the *Warner* court. It is settled law that the engagement with such tools, and even actual third-party humans, does not, per se, constitute a waiver of the attorney-client privilege. See, e.g., *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961) (establishing that attorney-client privilege can extend to legally necessary communications with accountants and other non-lawyer professionals).

There is a reasonable probability that the law will expand in this area, allowing the use of properly protected AI platforms to be considered *Kovel*-like agents of the attorney that provide functionality similar to an internal team member.

In *Kovel* terms, however, the unanswered question is whether AI is acting like an agent facilitating legal advice or instead a third-party receiving disclosures. Also relevant to the analysis is Federal Rule of Evidence 502, which stands for the proposition that not all disclosures equal waiver and that reasonableness and precautions must be considered.

POTENTIAL RISKS

With the unsettled nature of the law in mind, these two rulings do further highlight some risks that can and should be addressed.

1. Most off-the-shelf AI programs – Chatgpt, Claude, Copilot – specifically advise users that prompts and output are retained, are used for LLM training purposes, and may be publicly available. Attorneys and clients seeking to protect confidentiality rights **should engage with AI platforms that provide for Zero Data Retention ("ZDR"), no training on customer data, and no third-party disclosure**. Although there is no reported decision that guarantees that these precautionary steps will guarantee protection against disclosure, they do provide a more reasonable expectation of confidentiality.
2. Do not lose sight of the distinction between work product and attorney-client protections. The *Warner* court has it right – that in most circumstances, AI should be treated as a tool, akin to Gmail or Westlaw, and that its use, per se, should not be considered a waiver of work product protections. **For attorneys, the work-product protection likely applies in the context of AI material that reflects the mental impressions or litigation strategy of counsel, and where appropriate (read, ZDR) AI platforms are used.**
3. Talk to your client about these issues. They should be advised that with AI, interactions are *not* currently considered protected attorney-client communications. Work product privilege *may* apply when appropriate AI platforms are used, but that right is put at risk where the subject material was not prepared at counsel's direction and does not reflect counsel's mental impression or litigation strategy. **Where confidentiality is at stake, keep an AI-informed lawyer in the loop with respect to client AI interactions.**

In sum, although AI does not alter the governing legal principles, it creates new and unforeseen contexts in which rights may be deemed waived. Courts have not held that the use of AI alone waives confidentiality or privilege; however, they have found that such rights may be waived when AI is used without appropriate safeguards.