Think Before You Prompt: AI Use May Waive Your Attorney-Client Privilege

Client Alert

4.30.26

What You Need to Know

- A New York federal court recently held that materials created using consumer AI tools are not protected by attorney-client privilege or the work product doctrine, meaning they may be subject to disclosure in legal proceedings.
- The ruling stemmed from a case in which a defendant used an AI tool to analyze his legal situation after receiving a subpoena; the court found these communications were not protected because they were not made for the purpose of obtaining legal advice or at the direction of counsel.
- To avoid discovery risks, it is prudent to consult with your legal counsel before using AI in relation to any matters where litigation is anticipated.

By: Alan S. Naar and Sukrti Thonse

In our practice, we are seeing increasing numbers of clients using consumer artificial intelligence (AI) tools – including ChatGPT, Claude, and similar platforms – to find answers to legal, regulatory, and business questions. While these platforms can be helpful, a recent federal court ruling highlights significant risks that are not widely understood and may have real consequences.

What Happened?

In February 2026, a judge of the U.S. District Court for the Southern District of New York issued a ruling in *United States v. Heppner* holding that materials created using a consumer generative AI tool are not protected by the attorney-client privilege or the work product doctrine, a legal rule that protects documents and tangible

materials prepared by or at the behest of an attorney in anticipation of litigation from being discovered by opposing parties during a lawsuit.

In this case, Bradley Heppner was arrested on charges of securities and wire fraud. During a search of his residence, FBI agents seized documents containing communications between Heppner and Anthropic's generative AI tool, Claude. Heppner had utilized Claude, after receiving a grand jury subpoena, to analyze his situation and prepare written summaries of potential legal arguments. He later shared those materials with his lawyer and claimed they were protected from disclosure to the government.

The court disagreed and held that the materials were not protected from disclosure by either the attorney-client privilege or the work product doctrine.

Why Did the Court Reach That Finding?

The court focused on a few key points:

- The materials were created through a third-party AI platform, undermining confidentiality – a key element of the attorney-client privilege. The written privacy policy to which Claude users consent allows Anthropic to collect data on users' "inputs" and Claude's "outputs" and to use such data to "train" Claude. Anthropic reserves the right to disclose such data to third parties including governmental regulatory authorities.
- Communications with Claude were not communications with Heppner's lawyer.
- Heppner could not change unprivileged documents into privileged ones by later sharing them with counsel.
- Heppner did not communicate with Claude for the purpose of obtaining legal advice and did not do so at the suggestion or direction of his counsel.
- The work product doctrine did not apply because the materials were created independently by Heppner of his own volition and not by or at the behest of counsel.

Why Does This Matter?

While this is just a single non-binding ruling, it might influence how other courts approach AI-related privilege issues. Although *United States v. Heppner* is a criminal case, the same principles could apply to civil cases where parties request discovery of inputs and outputs using consumer AI tools.

In practical terms, it is critical to remember that information you input into consumer AI tools and the outputs you receive may not be confidential and therefore may not be protected from disclosure to third parties.

This has several implications:

- **Privilege risk:** You may lose the attorney-client privilege and the work product doctrine over sensitive information
- **Discovery risk:** AI prompts and outputs may be requested in litigation or investigations
- **Strategy exposure:** Early thinking or analysis could become evidence against you

What You Should (and Should Not) Do

We recommend a few simple guardrails:

- Do not input sensitive or confidential information into consumer AI tools
- Avoid uploading:
  - Contracts or drafts of legal documents that counsel provides
  - Legal questions tied to active matters or matters where litigation is reasonably anticipated
  - Business strategies or financial data
- Use only approved enterprise AI tools (if any), particularly those that:
  - Do not train on your data
  - Maintain strict confidentiality protections
- When in doubt, consult with counsel before using AI for legal or regulatory questions

Bottom Line: A Note on Where the Law is Going

This is an evolving area of law, and courts may ultimately distinguish between consumer AI tools and enterprise platforms designed to preserve confidentiality. That said, until clearer guidance develops, the decision in this case reflects where things currently stand and how regulators and litigators are beginning to approach AI use.

AI can be a powerful tool, but when it comes to legal and regulatory matters, if it's important enough to ask AI, it's important enough to ask your lawyer first. We're happy to help you think through how to safely incorporate AI into your business while protecting privilege, confidentiality, and compliance.

Greenbaum is continually monitoring legal developments related to the use of AI and will keep you informed accordingly. Please contact the authors with questions concerning the issues covered in this Alert or to discuss your specific circumstances.

Related Attorneys

Alan S. Naar

Partner
732.476.2530
Email

Sukrti Thonse

Associate
732.476.2480
Email