Is Your AI Use Protected from Disclosure? It's Complicated.

By Adam Gutbezahl on August 6, 2026



Americans are rapidly turning to generative artificial intelligence ("GenAI") tools like ChatGPT, Claude, and Gemini for everything from travel planning and creative writing to mental health and legal questions. The instantaneous responses provided by large language models ("LLMs") afford users a certain comfort. The ability to get responses tailored to the user's specific prompts and requests has also caused many people to provide personal information to these GenAI systems. Users, however, should pause to consider just how personal they get with an LLM and for what reasons they use these systems.

Is your use of an LLM confidential? The answer to that question is most likely **no**. Unless you created the LLM and/or have direct control over the operation of its underlying algorithm, you are providing information to a third party. You should most certainly consult an attorney before entering confidential information into an LLM.

What happens when someone uses an LLM for legal purposes? Can that use be privileged or protected as work product? The emerging answer is unsettled, but courts are increasingly requiring disclosure.

The Heppner Decision

This question first got a lot of attention following a decision issued in February 2026 from the Southern District of New York. In that case, ***United States v. Heppner***, the defendant was aware of a forthcoming indictment charging him with various securities-related crimes. The FBI seized electronic devices pursuant to a search warrant, which included approximately 31 documents showing communications with Claude. Heppner—without any suggestion from his attorney—prepared reports outlining potential defense strategies.

Heppner argued that these communications were protected because they were prepared in anticipation of a potential indictment. The court rejected these arguments. According to Judge Rakoff, the Claude communications and documents were not covered by the work product doctrine because they were not prepared by an attorney or at the direction of an attorney.

These materials were also not shielded by the attorney-client privilege because they (1) were not communications between a client and an attorney, (2) could not be considered confidential, and (3) were not for the purpose of obtaining legal advice. The court noted that since "Claude is not an attorney…that alone disposes of Heppner's claim of privilege." Judge Rakoff also stated that the communications with Claude cannot be considered confidential because the terms in Claude's privacy policy could not lead to any reasonable

PROFESSIONALS

Adam G. Gutbezahl

PRACTICES

Litigation

expectation of privacy. This included Claude's collection of data to train its LLM model and the right to "disclose personal data to third parties in connection with claims, disputes or litigation." Finally, Heppner's use of GenAI could not be considered to be for purposes of obtaining legal advice because he did not do so at the suggestion or direction of his attorney.

A footnote in this decision underscores the risk of using GenAI and how it may affect privilege. Heppner's attorney argued that the Claude communications should be protected because they incorporated information that counsel provided to Heppner over the course of representing him. In response to this argument, the court stated that any such action by Heppner constituted a waiver of privilege as to that information:

> *At oral argument, Heppner's counsel suggested in passing that the AI Documents may be privileged because they "incorporated information that we had conveyed to Mr. Heppner over the course of our representation."* ***But even if certain information that Heppner input into Claude was privileged, he waived privilege by sharing that information with Claude and Anthropic, just as if he had shared it with any other third party****....*

In other words, if you take information provided to you by your attorney and then input that information into an LLM, your actions very likely constitute a waiver of the attorney-client privilege.

Approaches Taken Following *Heppner*

Many jurisdictions are following the Heppner model when faced with similar questions. For example, here in Massachusetts, a recent Superior Court decision found that the use of GenAI is discoverable. In ***Shealy v. Seaside Investments, LLC***, the plaintiff's romantic partner generated documents through ChatGPT and then sent those documents to the plaintiff. Judge Squires-Lee rejected the claim that the ChatGPT conversations and documents were protected by the work product doctrine. The court noted that the work product doctrine focuses on the work of attorneys and does not extend to actions taken by one's romantic partner. The plaintiff – who was represented by counsel – and his romantic partner elected to use GenAI without the input of counsel. Since no attorney was involved in that process, no attorney work product protection applies.

Not all jurisdictions, however, have gone as far as Heppner. In ***Tate Group Automotive, LLC v. Legacy Automotive Capital, LLC***, defendants sought conversations between Kris Tate, an individual affiliated with the plaintiff, and ChatGPT. The Texas Business Court held that the ChatGPT conversations were protected by the work product doctrine. The rationale here did not focus on ChatGPT's use of data or the use of a third-party platform. Instead, the court based its decision on the fact that these LLM chats were never disclosed to an adversary or made in a manner that substantially increased the likelihood that an adversary would obtain the materials. Judge Dorfman noted that this protection is premised specifically under the Texas Rules of Civil Procedure and that this protection is limited. Although ChatGPT's output was protected, not all of Tate's input into the LLM received protection. Judge Dorfman ordered disclosure of the discovery materials shared with ChatGPT. The result was limited protection: ChatGPT output remained protected, but materials shared with the tool had to be produced.

Judges have been more lenient toward pro se litigants' use of GenAI. For example, in ***Warner v. Gilbarco, Inc.***, the Eastern District of Michigan denied a request that the pro se plaintiff produce documents concerning her use of GenAI tools in connection with the lawsuit. The court held that the pro se plaintiff's use of GenAI was done in anticipation of litigation. Magistrate Judge Patti took a similar approach to waiver as that in the Tate

Automotive decision by finding that any waiver must be to an adversary or done in a way "likely to get in an adversary's hands." Most telling from this decision, however, is the court's consideration of GenAI.

> *ChatGPT (and other generative AI programs) are **tools, not persons**, even if they may have administrators somewhere in the background.*

The cases show a key distinction between a court's view on whether GenAI is a third-party recipient or a litigation tool. Heppner and the decisions following its rationale (such as Shealy) consider GenAI platforms and LLMs as though they are third parties with whom a party is communicating. The pro se cases, such as Warner, however, provide stronger protections for the use of these platforms. Instead of considering the pro se litigant as communicating with a third party, these cases view the pro se litigant as using a tool to assist them throughout litigation.

Takeaways

Courts have not settled whether GenAI use is protected in litigation, but the safest assumption is that it may be discoverable – especially when no attorney directed or supervised the use.

The problem here is that many users treat GenAI as a private tool when courts are considering that use as a communication with a third party. To ensure appropriate protections can take place, individuals should change their thought process—and do so quickly. Individuals should not use LLMs for any legal purposes without first consulting with an attorney about that use.

ChatGPT is **not** your chum.

Claude is **not** your confidante.

Yes, these LLMs provide a lot of narrowly tailored information in an impressively short period of time. Yes, the LLMs help people synthesize their thoughts and potentially assist in understanding complex situations. Most concerning, however, is that this same LLM use provides a written record of the user's thought process, which can then be handed over to the other side in litigation. Your "haste" in using the LLM will result in "waste" by handing your issues over to the other side on a proverbial silver platter.

***Adam Gutbezahl** is a shareholder in the firm's **Litigation Department** and its **Commercial Real Estate**, **Construction Law**, and **Employment Law Groups**, where he handles complex commercial, employment, land use, and real estate disputes with extensive jury and bench trial experience. He is also a recognized thought leader on Generative AI's legal implications, publishing the monthly newsletter **ChatAdamG** on AI's impact in the workplace. Adam can be reached at **agg@riw.com** or **(617) 570-3502**.*

***Madison Pellegri** is a 2026 summer law clerk at the firm, where she has gained hands-on experience in construction litigation, land use, commercial real estate, and M&A through discovery, drafting, and research work alongside RIW's attorneys. She is a rising 3L at Suffolk University Law School, where she serves as a member of the Journal of High Technology Law. Madison previously served as a judicial intern to Associate Justice Georges at the Supreme Judicial Court and to Judge Rubin at the Land Court.*

POSTED IN: **ARTIFICIAL INTELLIGENCE**, **NEWS**