Lowndes

Insights

The Bot in the Witness Box: Why Your "Private" AI Chat is a Discovery Goldmine

Article
Lowndes
02.20.2026

Related Attorneys

Alexander Dobrev

Imagine you're the CEO of a major firm. You've just been served a grand jury subpoena. Naturally, you're stressed. Before calling your $1,500-an-hour partner, you open a chatbot to "run some scenarios." You feed it sensitive details, ask about your legal exposure, and even draft a few defensive bullet points to share with your lawyer later.

You think you're being efficient. Judge Jed Rakoff of the Southern District of New York thinks you're creating Exhibit A.

In the recent case of United States v. Heppner (2025), the court delivered a cold shower to anyone treating their AI chatbot like a digital confessional. Here's why your "private" chat with Claude, ChatGPT, or Gemini might just be the most effective witness against you.

The Heppner Heartbreak: A Case Study

Bradley Heppner, the former CEO of Beneficient, was facing serious securities fraud charges. On his own initiative, Heppner used the AI chatbot Claude to analyze his legal situation and prepare defense reports. When the government subpoenaed his devices, they found 31 AI-generated documents.

Heppner's lawyers argued these were protected by attorney-client privilege and the work-product doctrine. Judge Rakoff's response? A swift "No."

Why the Privilege Tanked:

1. AI Isn't Your Lawyer: An AI platform is a third-party commercial entity. Sharing secrets with it is legally identical to venting to a random person at a bar—except the bar keeps a permanent transcript of everything you said.

2. The "Confidentiality" Myth: Most consumer AI terms of service explicitly state that inputs may be reviewed by humans or used for training. By clicking "Agree," you've effectively invited a third party into your conversation, nuking the privilege.
3. No "Retroactive" Protection: You can't wash away the waiver by sending the AI results to your lawyer later. Once the bell of disclosure is rung, it can't be unrung.

Civil Litigation: The New Frontier of Discovery

While Heppner was a criminal case, the shockwaves are hitting civil litigation hard. If you are a defendant in a high-stakes civil suit, expect "AI Prompts and Outputs" to be the new "Slack and Email" in discovery requests. Your interactions are now potentially discoverable, and the implications are significant:

- The "Shadow AI" Trap: Employees often use AI to "ghostwrite" sensitive documents—like termination letters or internal investigative reports—without legal oversight. Every prompt used to "make this sound less discriminatory" is potentially discoverable.
- Executive Brainstorming: A CFO asking an AI to "identify potential loopholes" in a contract creates a digital trail that an adversary's counsel will salivate over during a deposition.
- The Waiver Cascade: If an employee pastes privileged legal advice into a chatbot to "summarize it," they may have waived the privilege not just for that summary, but for the entire underlying legal opinion.

How to Avoid an AI-Induced Legal Disaster

The lesson isn't "Don't use AI." The lesson is "Don't use AI without a leash." To protect your organization, consider these steps:

- Establish an "AI-Attorney Gate": For work-product protection to stick, the AI use must be at the direction of counsel. If an attorney prompts the tool as part of their strategy, the legal "shield" is significantly stronger.
- Enterprise Grade or Bust: Consumer versions of AI tools are for recipes and gift ideas, not legal strategy. Ensure your team uses enterprise-grade tools with strict, contractual data-siloing that guarantees no third-party review.
- Update Your Policies: "Don't share trade secrets" isn't enough. Your policy needs to say: "Do not use AI to analyze, summarize, or discuss any matter involving potential or active litigation without express approval from the Legal Department."

The Bottom Line

Your AI chatbot is a brilliant assistant, but it's a terrible priest. It doesn't owe you a duty of loyalty, it doesn't have a law license, and it will hand over your "private" thoughts the moment a subpoena hits its inbox.

In the words of the court: The privilege protects communications with your lawyer, not your algorithms.