

August 6, 2026

ASKING AI ABOUT YOUR LEGAL PROBLEM MAY CREATE DISCOVERABLE EVIDENCE

A recent case holds that a non-lawyer's interaction with an AI system is not protected by the attorney-client privilege and therefore is discoverable in litigation.

Also, using AI notetakers without the consent of all participants may be a crime, depending on the particular states of the participants.

Businesses and individuals increasingly use artificial intelligence tools to evaluate legal problems, test arguments, summarize documents and prepare for discussions with counsel. Recent federal decisions provide a direct warning: communications between a non-lawyer and an AI provider are not protected by the attorney-client privilege or, except in rare circumstances, the work-product doctrine—and therefore may later be obtained and used by an opposing party or the government.

KEY TAKEAWAYS

❖ ***An AI is not your lawyer.*** Asking an AI tool for legal advice does not, by itself, create an attorney-client relationship or make the exchange privileged.

❖ ***Your prompts and the AI's responses generally are discoverable.*** The provider probably retains them, and copies may also exist in browser histories, downloaded files, screenshots, emails or local devices. Even if you use a paid version of the AI and your interactions are not used to train the AI, the AI provider likely retains the interactions for a significant period of time.

❖ ***Including legal advice in a prompt can compound the risk.*** Restating what counsel told you to an AI provider probably breaks the attorney-client privilege on the restated advice, as the AI is considered a third party.

❖ ***A litigant who is representing himself in litigation (a "pro se" litigant) may benefit from the protection of the work-product doctrine, but this is not true of a person who has engaged counsel or who has not timely and unequivocally elected to represent himself in litigating an interest personal to him.*** Thus, merely researching a legal problem before engaging counsel does not, without more, make a non-lawyer a pro se litigant. *Iannaccone v. Law*, 142 F.3d 553, 558 (2d Cir. 1998).

❖ ***AI notetakers create separate recording-law and privacy risks.*** Because these applications capture audio and generate recordings or transcripts, they should be considered as recording devices. Some states (such as California) require every participant's consent before a confidential call may be recorded, and violating this requirement is a crime.

❖ ***Do not delete existing AI conversations after a dispute arises.*** If litigation or an investigation is pending or reasonably anticipated, deletion may violate your obligations to preserve relevant evidence.

❖ ***Speak with counsel before using AI to analyze or record a live legal matter.*** Counsel can determine whether an approved tool may be used and establish safeguards appropriate to the matter.

THE HEPPNER DECISION

In *United States v. Heppner*, 820 F. Supp. 3d 292, 294-95 (S.D.N.Y. 2026), a criminal defendant used Claude (Anthropic) to evaluate potential defenses after receiving a grand-jury subpoena and while represented by counsel. Federal agents later seized approximately 31 documents memorializing those exchanges. When the government moved for a ruling permitting inspection, the defendant argued that the documents were protected by attorney-client privilege and the work-product doctrine.

The court rejected both arguments. The communications were not privileged because Claude is not an attorney, the exchanges were not communications between the defendant and his counsel, and the defendant had shared the information with a third-party platform. *Id.* at 296-98. The work-product doctrine likewise offered no protection because, “even assuming, arguendo, that [the materials] were prepared ‘in anticipation of litigation,’ . . . they were nevertheless not ‘prepared by or at the behest of counsel,’” nor did they reflect defense counsel’s strategy. *Id.* at 298.

Although this does not seem to be an essential element of the court’s conclusion, the court emphasized the absence of a reasonable expectation of confidentiality when using a consumer AI platform whose privacy policy permitted the provider to collect, use and disclose submitted information. *Id.* at 296-97. An AI conversation may feel private, but legally it generally will be deemed a communication with an outside company that stores and processes the exchange.

WARNER DOES NOT PROVIDE A SAFE HARBOR FOR REPRESENTED CLIENTS

Another federal court dealt with a related question in *Warner v. Gilbarco, Inc.*, 820 F. Supp. 3d 629, 636-37 (E.D. Mich. 2026). There, a *pro se* litigant used ChatGPT in connection with her lawsuit. The court denied a request for documents and information concerning that use, concluding that the requested material was not discoverable under Federal Rule of Civil Procedure 26(b)(3)(A) and, even if discoverable, was protected work product. *Id.* The court also distinguished work-product protection from attorney-client privilege, explaining that voluntary disclosure to a third party does not, by itself, waive work-product protection unless the disclosure is to an adversary or makes adversary access likely. *Id.* at 637.

Clients who already have engaged lawyers, or who have not yet done so but who do not plan to litigate *pro se*, should take no comfort from *Warner*. Its reasoning materially relied on the plaintiff’s ability, as a *pro se litigant*, to assert work-product protection over her own litigation materials and mental impressions. *Id.* A client who has counsel but who independently interacts with an AI provider about legal questions is differently situated and is faced directly with the decision in *Heppner*. A person who interacts with an AI provider about legal questions before engaging a lawyer also is faced with *Heppner*.

AI NOTETAKERS MAY TRIGGER RECORDING LAWS

AI meeting assistants and notetaker applications do more than create convenient summaries. They typically capture a call’s audio and use it to produce a recording, transcript, or a summary (even all three). Clients should therefore treat an AI notetaker as a recording device—not merely as a silent software participant—and should consider privilege, confidentiality, data-retention, recording-consent and potentially applicable biometric-privacy requirements before allowing one to join a call.

Recording laws vary by jurisdiction. California, for example, makes it a crime to intentionally record a confidential communication using an electronic amplifying or recording device without the consent of all parties. Cal. Penal Code § 632(a) (West 2026). A violation may result in a fine, imprisonment or both. *Id.* The statute applies only where the communication is “confidential”—that is, where the circumstances reasonably indicate that a participant expects the communication to remain between the parties—but business, legal and strategy calls may satisfy that standard. *See id.* § 632(c).

If a client would like to use a notetaker application, the client should obtain affirmative consent from each party on the call to reduce the risk of violating applicable state wiretapping, recording-consent or biometric-privacy laws. The organizer should identify the application, explain that it will record or transcribe the discussion, and obtain an affirmative response from every participant before activating the application.

If a third party wishes to use a notetaker and a participant does not consider it advisable, that participant should clearly state that the participant does not consent. The participant may explain that recording can inhibit the free flow of discussion. If the participant agrees to the recording, the participant should consider conditioning consent on receiving a complete copy of the recording and transcript after the call. If consent

is absent or any participant objects, the notetaker should be disabled or removed. On privileged calls, the safer course is ordinarily not to use an external notetaker at all unless counsel has approved the specific tool and arrangement.

Recording warning: Do not assume that an automated notice, a bot's appearance in a participant list or another person's invitation supplies legally sufficient consent. Obtain an affirmative response from every participant before recording or transcribing a confidential call.

WHAT CLIENTS AND POTENTIAL CLIENTS SHOULD DO NOW

- i. ***Do not use consumer AI tools to discuss a live legal matter.*** Do not enter confidential facts, potential claims or defenses, litigation strategy, witness information, investigation details, contract disputes, regulatory concerns or summaries of counsel's advice into a public or consumer AI service unless counsel has specifically approved that use.
- ii. ***Assume prompts and outputs may be retained.*** Paid access does not necessarily mean that a tool is confidential, privileged or suitable for legal matters. Retention periods, model-training practices, human review, sub-processors and deletion rights vary by provider and subscription. Even where a provider promises not to train its model on customer data, it may retain prompts and outputs for security, abuse monitoring or other purposes.
- iii. ***Obtain affirmative consent before using an AI notetaker.*** Treat an application that captures, records or transcribes a call as a recording device. Identify the tool and its function, obtain affirmative consent from every participant and preserve an appropriate record of that consent. If a third party proposes using the tool and you object, clearly state that you do not consent. If you consent, consider conditioning consent on receiving a complete copy of the recording and transcript. If consent is absent or uncertain, do not record or transcribe the call.
- iv. ***Tell counsel about prior AI use.*** If you have used an AI tool in connection with an investigation, dispute, or other legal issue, or allowed an AI notetaker to record a relevant call, tell counsel promptly.
- v. ***Preserve relevant AI materials if litigation is underway or might reasonably be anticipated.*** Once litigation or an investigation is pending or might reasonably be anticipated, AI prompts, outputs, recordings, transcripts and account histories may constitute relevant electronically stored information. Do not delete, alter or attempt to conceal those materials. Preservation decisions should be made with counsel.
- vi. ***Use approved tools, if at all, only under counsel's direction.*** Not all AI use presents the same risk. Enterprise legal platforms may operate under contractual protections that restrict retention, training and disclosure. Those protections can materially improve confidentiality, but they do not automatically establish privilege, satisfy recording-consent laws or eliminate the need for legal judgment. For a matter involving confidential or legally sensitive information, the tool, configuration and proposed use should be reviewed in advance with counsel.

CONTACTS

Robert MacDonald

Partner

rmacdonald@dvmlaw.com

Tel.: +1 646 513 3287

Della Hill

Partner

dhill@dvmlaw.com

Tel.: +1 646 513 3256

The articles published on Dunning Vallejo & MacDonald's website and LinkedIn site are for reference purposes only. They do not constitute legal advice and should not be relied upon as such. Specific legal advice should always be sought separately before taking any action.