BCLP. Client Intelligent

Insights

PROTECTING PRIVILEGE AND CONFIDENTIALITY WHEN USING AI TOOLS

Apr 30, 2026

Generative Artificial Intelligence (AI) tools are increasingly being used by businesses, often without the knowledge or direction of their counsel. A recent federal court decision, *United States v. Heppner* (S.D.N.Y. Feb. 17, 2026), illustrates why that approach carries real legal risk. In *Heppner*, the defendant conducted legal research using an AI platform and sent the results to his lawyers, but did so without being directed to do so by counsel. The court held that the materials were not protected by the attorney-client privilege or the work product doctrine. The court's reasoning rested on three grounds:

- the AI outputs were not communications between the client and his lawyers;
- the AI platform's privacy policy reserved the right to share user data with third parties, eliminating any reasonable expectation of confidentiality; and
- because the lawyers had not directed the research, the client was not acting as their agent — meaning the work product doctrine did not apply either.

The lesson is straightforward: **when clients use AI independently, without attorney direction and on non-confidential platforms, the resulting materials are likely discoverable.**

These risks are particularly acute in three important areas:

1. **Internal investigations**: The attorney-client privilege may protect AI-generated investigation materials only when an attorney conducts the underlying interview, or when a non-attorney does so at counsel's direction. Employees who use AI tools to document or analyze interviews independently, outside any attorney-directed process, produce outputs that may not be protected. The work product doctrine may afford limited additional protection, but only when the investigation is conducted by counsel or at their direction.
2. **AI legal research**: The outcome in *Heppner* directly illustrates the risk. The result might have been different if the lawyers directed the research, or if the client used an enterprise AI tool that

contractually obligated the provider to protect the confidentiality of client data and not use it to train or fine-tune the underlying model(s).

3. **AI-enabled meeting and conversation recording**: When AI transcription or meeting-summary tools are active during interviews or calls, confidential information shared in those sessions may no longer be private. Consumer-grade AI tools typically disclaim confidentiality in their terms of service and reserve the right to collect, use, and share user inputs, which means sensitive business information, attorney advice, or witness statements discussed during a recorded meeting could be exposed. Even where a tool operates within an enterprise environment that does not share data with third parties, AI-generated summaries and transcripts are potentially discoverable in litigation and may not be protected by the attorney-client privilege or the work product doctrine, particularly if such outputs are not generated at the direction of counsel.

Separately, at least thirteen states require the consent of all parties before a conversation may be recorded where there is a reasonable expectation of privacy — including California, Florida, Illinois, and Washington — meaning that activating a recording tool without disclosure could expose the company to legal liability independent of any privilege issue. Even in one-party consent jurisdictions such as New York, ethical obligations may independently require disclosure. See N.Y.C. Bar Ass'n Pro. Ethics Comm. Op. 2025-6 (concluding that clients must be notified, and their consent obtained, whenever their calls are being recorded by an AI-empowered system).

Certain AI transcription platforms may go beyond simple recording: some offer face or voice recognition features that could generate biometric identifiers or other biometric data when attributing words to specific speakers. At least five states — California, Colorado, Illinois, Texas, and Washington — have enacted biometric data privacy statutes imposing notice, consent, and data-handling obligations when such identifiers are collected or processed, with Illinois's Biometric Information Privacy Act (BIPA) carrying the greatest risk of private litigation.

BEST PRACTICES

The following guidelines are directed to business teams and in-house stakeholders who use — or are considering using — AI tools in connection with legal matters, investigations, or other activities that may involve privileged or confidential information. In each case, the central principle is the same: coordinate with your legal counsel before deploying AI in these contexts.

INTERNAL INVESTIGATIONS

- Do not use AI to document, summarize, or analyze investigative interviews without first coordinating with legal counsel. Attorney direction is essential to preserve privilege and work product protection.
- If you are a non-attorney conducting an AI-assisted interview, confirm that you are doing so at the express direction of legal counsel. You should also ensure that both your use of AI and the

fact that you are conducting the interview at the express direction of legal counsel are communicated clearly in any interview warnings given to witnesses.

- Be mindful of litigation hold obligations, other preservation requirements, and default retention settings on AI platforms, which may automatically delete inputs and outputs that may be subject to retention obligations.

AI LEGAL RESEARCH

- Always inform your lawyers before using any AI tool to research legal issues, even for background purposes. Lawyers should direct and supervise that research.
- Only use enterprise-grade AI platforms on which the vendor contractually agrees not to use your data to train or fine-tune its models and not to disclose your data to third parties. Consumer AI tools typically disclaim confidentiality in their terms of service.

AI-ENABLED MEETING AND CONVERSATION RECORDING

- Obtain the express, documented consent of all participants before activating any AI recording or transcription tool during an interview or meeting.
- Determine whether the AI tool's speaker-attribution features may capture or process biometric identifiers, and if so, evaluate compliance obligations under applicable state biometric data privacy laws.
- If the AI tool used by your vendor does not operate under a contractual confidentiality commitment, assume that information shared in recorded meetings is not private and limit what is discussed in those sessions accordingly.

If you have any questions about the issues discussed in this alert or would like guidance on implementing these practices, please contact the authors or your relationship partner at Bryan Cave Leighton Paisner LLP.

RELATED CAPABILITIES

- Digital Transformation & Emerging Technology
- Retail & Consumer Products
- Data Privacy & Security

MEET THE TEAM

Ashley C. Bateman

Associate, Seattle

ashley.bateman@bclplaw.com
+1 206 600 6637

Goli Mahdavi

Global AI Lead, San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

John W. Amberg

Senior Counsel, Los Angeles

john.amberg@bclplaw.com
+1 310 576 2280