ECKERT SEAMANS
ATTORNEYS AT LAW

June 1, 2026

Legal Update

When Clients Use AI: Privilege, Waiver, and the Evolving Discovery Frontier

By E. Duffy Myrtetus and Annemarie DiNardo Cleary

Introduction

The use of generative artificial intelligence has quietly migrated from novelty to habit. Business executives test arguments in chatbots. Employees summarize disputes before calling counsel. Individuals facing litigation turn to AI tools to "think through" strategy before ever picking up the phone.

What feels efficient—and even prudent—could be legally catastrophic.

Courts are now confronting a deceptively simple question with significant consequences: **when a client uses artificial intelligence to analyze or plan a legal claim, are those communications protected?** Early decisions suggest a clear trajectory. Applying settled doctrine, courts are finding that such interactions are often neither privileged nor protected work product—and therefore fully discoverable.

Familiar Concepts Meet a New Technology

In *United States v. Heppner*, 820 F. Supp. 3d 292 (S.D.N.Y. 2026), a federal court held that a litigant's communications with a publicly available AI platform were not protected by the attorney–client privilege or work-product doctrine. The court emphasized three traditional requirements: confidentiality, attorney involvement, and agency. Finding none, it ordered disclosure.

The reasoning tracks long-standing precedent. Privilege protects confidential communications between client and counsel (or their agents) made for the purpose of obtaining legal advice. See, e.g., *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) (privilege applies to confidential communications for legal advice); *Fisher v. United States*, 425 U.S. 391, 403 (1976) (privilege protects communications, not underlying facts). Where communications are disclosed to third parties, the protection is generally lost. See *In re Horowitz*, 482 F.2d 72, 81 (2d Cir. 1973) (disclosure to third party waives privilege absent necessity).

In the view of the *Heppner* court, the AI provider did not qualify as an agent. Courts have extended privilege to certain third parties under *Kovel* where the third party is necessary to facilitate legal advice. *United States v. Kovel*, 296 F.2d 918, 921–22 (2d Cir. 1961) (extending privilege to accountant assisting counsel). But that extension is narrow and functional. See *In re Grand Jury Subpoenas*, 265 F. Supp. 2d 321, 329 (S.D.N.Y. 2003) (requiring that third party's involvement be necessary, not merely useful). Public AI platforms—designed for broad use and governed by terms permitting data retention—rarely meet that standard.

The Quiet Erosion of Confidentiality

At the center of privilege lies confidentiality. Without it, the doctrine collapses.

Many AI platforms retain prompts, log outputs, and use inputs to improve models. From a court's perspective, entering sensitive facts into such a system can resemble disclosure to a third party—akin to sharing information with a non-confidential vendor. See *United States v. Jacobs*, 117 F.3d 82, 87 (2d Cir. 1997) (privilege waived where communication shared with third party lacking confidentiality obligation).

Imagine a CFO who, anticipating a shareholder dispute, inputs internal emails and a draft timeline into a public AI tool to "stress test" possible defenses. The tool generates a litigation strategy memo. Months later, in discovery, the opposing party requests "all AI-generated analyses concerning the dispute." Absent counsel direction and confidentiality safeguards, both the prompts and outputs are likely discoverable.

Work Product Without a Lawyer?

If privilege fails, litigants often invoke the work-product doctrine. That doctrine protects from discovery materials prepared "by or for another party or its representative" in anticipation of litigation. Fed. R. Civ. P. 26(b)(3).

In *Warner v. Gilbarco, Inc.*, 820 F. Supp. 3d 629 (E.D. MI 2026), a federal court in Michigan rejected an employer's attempts to compel the production of the *pro se* plaintiff's use of AI tools in connection with the lawsuit. The court cited the rule and its protection of a party's internal analysis and mental impressions concerning a case. In contrast to *Heppner*, the *Warner* court rejected the argument that the plaintiff's use of generative AI programs, which the court called "*tools, not persons,*" waived the protections of the work product doctrine.

The different approaches in *Heppner* and *Warner* underscore the lack of certainty in protecting pre-litigation use of AI platforms. Frequently, courts require a meaningful nexus to counsel for the protections afforded under the work product doctrine to apply. See *United States v. Nobles*, 422 U.S. 225, 238–39 (1975) (work product extends to materials prepared by agents of counsel); United States v. *Adlman*, 134 F.3d 1194, 1198 (2d Cir. 1998) (documents must be prepared because of litigation). When a client independently uses AI—without direction or supervision of counsel—there is a significant risk the doctrine will not protect the work.

Discovery's Expanding Horizon

AI-generated materials fit comfortably within the definition of ESI. See Fed. R. Civ. P. 34(a)(1)(A) (ESI includes writings, drawings, graphs, charts, and data compilations stored in any medium).

Courts have long taken an expansive view of discoverability. See *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (relevance construed broadly for discovery). In practice, that means the following may be discoverable:

- Prompts (factual narratives, questions);
- Outputs (analyses, drafts);
- Chat logs and histories; and
- Iterative versions and refinements

may be discoverable.

State Law: Consistency in Principle, Variation in Emphasis

Across jurisdictions, the same fault line appears: disclosure beyond the protected relationship risks waiver.

- **Pennsylvania:** Privilege codified at 42 Pa. Cons. Stat. § 5928; strictly construed. See *Commonwealth v. Chmiel*, 889 A.2d 501, 528 (Pa. 2005) (privilege applies only to confidential communications for legal advice).
- **New York:** C.P.L.R. 4503; narrow construction and waiver upon third-party disclosure. See *People v. Osorio*, 75 N.Y.2d 80, 84 (1989) (confidentiality is essential element).
- **Delaware:** Functional approach with potential agency extensions. See *In re Teleglobe Commc'ns Corp.*, 493 F.3d 345, 359 (3d Cir. 2007) (discussing joint-client and agency principles under Delaware law).
- **New Jersey:** N.J.R.E. 504; confidentiality required; waiver upon disclosure. See *State v. Mauti*, 33 A.3d 1216, 1227 (N.J. 2012).
- **Massachusetts:** Strict common-law approach. See *Comm'r of Revenue v. Comcast Corp.*, 901 N.E.2d 1185, 1193 (Mass. 2009).
- **Virginia:** Common law privilege; narrow exceptions. See *Commonwealth v. Edwards*, 370 S.E.2d 296, 301 (Va. 1988).

Public AI tools will rarely satisfy confidentiality or agency requirements in these jurisdictions.

Managing the Risk

Artificial intelligence has expanded how we think about legal problems—but it has not expanded the protections that shield those thoughts from discovery. Courts are applying familiar rules with renewed clarity: **without confidentiality, without counsel, and without agency, there is no privilege.**

Careful AI governance can increase the likelihood that AI-generated information will be protected:

- **Selecting AI Tools:** Engage in thorough due diligence when selecting AI tools for your business. Review and understand the platform's privacy policy and data retention practices. If a LLM uses your prompts to train its underlying algorithms, that information could potentially be transmitted to other users. You should select a platform that guarantees in its Terms of Service or enterprise agreement that it strictly prohibits using user inputs, prompts, and output for training, retraining, or improving the model. Additionally, the platform should be a "closed," enterprise-grade system that partitions data with a secure, firm-controlled or client-controlled environment featuring strict access controls, encryption (at rest and in transit), and compliance with major security standards such as SOC 2.
- **AI Usage Policies:** Develop and periodically review your AI usage policies. Understand which AI tools your employees are using and how.
- **Restrictions on AI Use:** Prohibit the input of privileged, confidential, or sensitive information into consumer-grade AI platforms. Consider investing in an enterprise-system platform and regulate its usage. As the adoption and utilization of AI notetaking and transcription grows, address and regulate its use at the outset of matters and meetings. If a party insists on using these tools, ensure you establish and document the agreement and tool choice *before* privilege questions arise.

- **Train Employees:** Ensure employees understand the risks of AI use and consider the implications before inputting privileged, confidential, or sensitive information into AI platforms. Emphasize that privilege may be waived by unauthorized AI use.
- **Involve Counsel:** Application of the attorney-client privilege requires the involvement of counsel.
- **Preservation Duties:** Litigation hold notices should mandate the retention of AI-generated materials.

In an era where even preliminary legal thinking may be recorded and retrievable, the question that matters most may be the oldest one in privilege law: *who, exactly, did you tell?*

ECKERT SEAMANS ATTORNEYS AT LAW