Navigating Litigation Privilege Risk in the Age of AI—Key Takeaways for In-House Lawyers From 2 Recent, Novel Court Cases

Law.com Corporate Counsel
March 9, 2026

By absorbing the lessons of these cases—and those to come—in-house counsel can help their clients enjoy AI's efficiencies while minimizing the risk of forfeiting privilege in litigation and investigations.

When considering litigation risk, in-house counsel should treat generative AI as the new email. Just as email reshaped discovery, so too will the rapid adoption of AI in our business and personal lives. Soon, it will become routine for litigants to demand production of generative AI inputs and outputs, just as they currently demand production of emails. Two recent federal court decisions highlight the importance of guarding against the loss of privilege protections from discovery of such materials.

On Feb. 17, 2026, U.S. District Court Judge Jed Rakoff of the Southern District of New York (S.D.N.Y.) issued a written memorandum in United States v. Heppner explaining his Feb. 10 bench ruling that 31 documents, which reflected the defendant's communications with the consumer version of Anthropic's Claude, were not protected by attorney-client privilege or the work-product doctrine. Also on Feb. 10, Magistrate Judge Anthony Patti (E.D. Mich.) ruled in Warner v. Gilbarco, that materials generated using ChatGPT were protected from discovery under the work-product doctrine. While these rulings may appear in tension, they are readily distinguishable. This article examines both decisions and offers practical guidance for in-house counsel navigating AI use.

The 'Heppner' Case

In Heppner, the defendant communicated with Claude after receiving a grand jury subpoena and learning he was a target of the investigation. Acting independently, he prepared reports outlining defense strategy and potential arguments regarding the facts and law. He claimed these reports were prepared in anticipation of indictment and shared the AI-generated content with his attorneys.

In his ruling, Judge Rakoff applied familiar privilege rules to this new technology. The attorney-client privilege applies to communications between a client and his or her attorney; that are intended to be, and in fact were, kept confidential; and for the purpose of obtaining or providing legal advice. Rakoff found at least two, though likely all three, elements lacking. First, the defendant's communications with Claude were not with his attorneys. Second, they were not confidential: Anthropic's user agreement provides that inputs and outputs are not confidential, defeating any reasonable expectation of confidentiality. Third, the defendant did not use Claude to obtain legal advice or at counsel's direction. As to the former, Rakoff noted that Claude disclaims providing any legal advice. As to the latter, he noted that if the defendant had used the AI tool at counsel's direction, "Claude might arguably be said to have functioned in a manner

akin to a highly trained professional who may act as a lawyer's agent within the protection of the attorney-client privilege." But that was not the case.

The court also rejected the defendant's effort to shield his AI communications under the work-product doctrine, which protects materials reflecting attorneys' mental impressions so that they can freely analyze and prepare for their clients' cases. The doctrine applies to materials prepared by or at counsel's direction in anticipation of litigation. Judge Rakoff found that: because the defendant used Claude independently, the materials were not prepared at counsel's direction; and as the defendant's attorneys conceded, they did not reflect counsel's strategy at time of creation.

The 'Warner' Case

In Warner, the defendants moved to compel disclosure of materials the plaintiff prepared using ChatGPT. The plaintiff objected under the attorney-client privilege and work-product doctrine. The court addressed only the latter—likely because the plaintiff was pro se. In holding the materials protected, Magistrate Judge Patti relied on case law recognizing that pro se litigants may invoke the work-product doctrine to protect their mental processes and impressions concerning their case preparations. He further observed that: although waiver requires disclosure to a third person, ChatGPT is a "tool," not a person; and compelling disclosure where a pro se party or counsel uses software to organize, prepare, or draft "would nullify work-product protection in nearly every modern drafting environment, a result no court has endorsed."

Reconciling the Two Cases

Although Heppner and Warner appear at odds, they are largely reconcilable. In Warner, the party asserting protection was representing herself—a crucial differentiator—and the court permitted her to invoke the work-product doctrine for her use of ChatGPT in preparing her case. By contrast, the defendant in Heppner was represented by counsel, but used Claude independently. Moreover, unlike Heppner, Warner did not need to address attorney-client privilege.

Some tension remains, however, in each court's treatment of modern software in litigation preparation. Judge Rakoff emphasized that commercial generative AI terms of use disclaim any expectation of privacy, such that disclosure to the software vitiates protection. Notably, Judge Rakoff did not address enterprise AI tools, which ostensibly function as closed environments. Judge Patti took a different approach, rejecting the premise that use of a software tool waives work-product protection and instead focusing on the practical (undesired) consequence that, in a world where "modern drafting environments" are ubiquitous, compelling such discovery may effectively eliminate valuable protections against disclosure in almost every instance.

The In-House Lawyers' Task

Considering Heppner and Warner, and the growing use of generative AI in business, in-house counsel must take proactive steps to manage resulting privilege risks. These decisions underscore how use and governance of AI affect privilege and confidentiality. As organizations increasingly integrate these tools into their workflows, in-house counsel should work with colleagues throughout their organizations to review and update policies, systems, IT security, and training to address these evolving challenges.

Policy Development: Defining Clear Boundaries for AI Use
Heppner and Warner underscore the need for clear, detailed policies governing AI use across legal and business functions. Whether advising regulated or unregulated clients, counsel should begin from the premise that—like e-mails—interactions with, and materials generated by, generative AI may be discoverable in litigation. To mitigate risk, organizations should adopt policies specifying whether, how, and which tools may be used. Key steps include: mandatory legal review of an AI tool's (even an enterprise tool's) data and confidentiality terms before use, including how data is processed, stored, shared, or used for training; strictly prohibiting the use of nonenterprise AI tools for privileged or confidential information—e.g., personal ChatGPT or Claude accounts; and guidance on segregating and labeling AI-generated materials. Regulated entities must ensure compliance with sector-specific standards, while others should assess risk tolerance, contractual obligations, and operational needs.

Training Initiatives: Equipping Teams for Responsible AI Engagement
Policy, IT guardrails, and product selection cannot substitute for robust, ongoing education across relevant users and business units. Drawing from the divergent outcomes in Heppner and Warner, in-house legal teams should work with IT to develop and monitor regular, scenario-based training for lawyers and nonlawyers. Such programs must practically explain when AI use might jeopardize privilege. Training should also address the risks of inputting sensitive company or client information into commercial AI services and outline best practices for maintaining confidentiality, including the need for legal supervision in legal or investigatory contexts.

Distinguishing Between Open- and Closed-Universe Generative AI: Practical Considerations
Heppner and Warner both highlight the significance of the AI platform. Open models like ChatGPT and Claude are typically governed by broad terms that disclaim confidentiality and permit access to user data—a central premise in Heppner. By contrast, closed systems such as Harvey and Vincent are designed to address privacy and control through segregated, enterprise-specific data environments and customizable access controls. Even so, organizations must implement appropriate usage and access policies and closely scrutinize licensing terms to ensure alignment with privilege and confidentiality expectations.

Implementation and Oversight: Sustaining Effective Practice
Cross-departmental collaboration is critical. Legal, compliance, IT, and business leadership should jointly oversee AI protocols, maintain clear channels for raising privilege concerns, and adapt policies as technologies and the legal landscape evolve. Periodic reviews, real-time feedback, ongoing training, and transparent compliance metrics can build and reinforce a culture of compliant, responsible AI use.

Conclusion
Heppner and Warner mark only the beginning of the judiciary's engagement with generative AI and privilege. By absorbing the lessons of these cases—and those to come—in-house counsel can help their clients enjoy AI's efficiencies while minimizing the risk of forfeiting privilege in litigation and investigations. Thoughtful policy design, user education, and careful AI

procurement are essential to balancing innovation with the need to preserve privilege. In-house lawyers now sit at the center of this complex and evolving issue and will increasingly be called upon for their wisdom and counsel.

Eliad S. Shapiro *is a partner in Herrick, Feinstein's litigation department. A commercial litigator and real estate litigator, he handles complex, bet-the-company matters at both the trial and appellate levels.*

Maxim M.L. Nowak *is a partner in the firm's white collar criminal defense and securities litigation and enforcement groups. He defends corporations and individuals in high-stakes matters brought by the DOJ, SEC and other regulators.*
