ARTIFICIAL INTELLIGENCE AND CYBERSECURITY AND DATA PRIVACY
INFORMATION MEMO
APRIL 6, 2026

No Counsel, No Privilege: Courts Signal That Client AI Use May Fall Outside Attorney-Client Privilege

A recent decision in the Southern District of New York is continuing to garner attention in the legal community. In February, Judge Rakoff issued a landmark decision rejecting attorney-client privilege and work-product doctrine protections for documents generated using artificial intelligence (AI).

In *United States v. Heppner*, the Court addressed whether a criminal defendant's interactions with a publicly available generative AI platform, Claude, were privileged. The court held that both information entered into, and materials generated by, an AI tool were not protected by attorney-client privilege or the work product doctrine. *See United States v. Heppner*, 2026 WL 436579 (S.D.N.Y. Feb. 17, 2026).

The court emphasized that attorney-client privilege generally protects only confidential communications between a client and an attorney, or an attorney's agent, made for the purpose of obtaining or providing legal advice. In *Heppner*, attorney-client privilege did not apply because, while this may be shocking, an AI tool is *not* an attorney or an attorney's agent. The Court also explained that the defendant was not seeking legal advice from the AI tool. Defendant later asserted that by sharing the AI-generated content with their counsel, the material should retroactively constitute privileged material or work product. This argument failed as well. In *Heppner*, the defendant created the documents without instruction or direction from counsel, and counsel did not direct the use of the AI platform for investigative or strategic purposes. Documents created independently, without attorney direction and later provided to counsel do not retroactively become privileged or protected work product. Furthermore, Judge Rakoff noted that Claude's terms of service expressly disclaimed the provision of legal advice and instructed users to consult qualified counsel. Judge Rakoff's decision also cautioned that use of publicly available AI tools risk loss of confidential information as there are clear representations in certain AI tool privacy policies and terms of service that reveal limited data protection. In this case, Claude's privacy policy explicitly stated that user input and generated outputs would be used to train Claude, and that information collected may be disclosed to third parties. Judge Rakoff determined, based on these representations, that *Heppner* could have no reasonable expectation of confidentiality in communications with Claude.

Notably, the conclusions made in this case apply not only to AI-generated outputs, but also to the information provided as an input. Sharing summaries of legal advice received from an attorney, factual narratives prepared for litigation or draft legal theories with an AI tool may result in a waiver of privilege as to the underlying information and any conclusions generated therefrom.

The *Heppner* decision serves as a cautionary example of the risks associated with the unsupervised use of AI in legal matters. Careless use of AI during litigation, investigations or other legal efforts can expose sensitive information and undermine established legal protections. Importantly, this decision sets the stage for in-house counsel to train their internal clients on the importance of avoiding self-help. Similarly, outside counsel should remind their clients of the need to obtain counsel before sharing any potential legal material with a third-party, including AI tools.

While very instructive, *Heppner* was narrowly decided on the platform selected, timing of communication and disclosure of information to third parties. What *Heppner* does not speak to is the propriety of using AI tools curated for legal work, and the use of such tools by your legal counsel or at the direction of your legal counsel.

Organizations should recognize that the Court's decision here, rejecting a claim of attorney-client privilege, is fact-specific and depends on both the nature of the communications and the AI platform involved. Generative AI tools should not be used to develop litigation strategy, legal documents or memorialize legal advice without the involvement and direction of legal counsel. Where AI tools are used, pay close attention to platform terms, confidentiality protections, and internal policies governing permissible use.

Reflecting the unchartered territory of the legal landscape in an AI world, the District Court for the District of Colorado recently addressed similar issues and arrived at varied conclusions. In *Morgan v. V2X, Inc.,* the Court held that a pro se civil litigant could invoke Rule 26(b)(3) work-product protection for AI-assisted litigation materials, and that use of an AI platform did not automatically waive that protection merely because information passed through a third-party intermediary. *Morgan v. V2X, Inc.,* No. 25-cv-01991-SKC-MDB, 2026 U.S. Dist. LEXIS 67939. Notwithstanding the protection afforded to the information generated by the AI tool, the Court held that the work-product doctrine did not provide protection for identification of the specific AI tool used. The Court went on to require an amendment to the existing protective order to restrict the parties from submitting confidential information to publicly available AI platforms, unless the AI platform was contractually prohibited from using or disclosing the data and could delete it upon request. *Morgan* therefore aligns with *Heppner* in recognizing the confidentiality risks posed by public AI tools and in refusing to treat AI use as categorically protected. However, it distinguishes from *Heppner* on both the governing framework and the relationship between the user and counsel: *Heppner* involved a represented criminal defendant seeking privilege and work-product protection for materials created independently of counsel, whereas *Morgan* involved a pro se litigant proceeding under Rule 26(b)(3), where the Court reasoned that there was no comparable gap between party and advocate. Taken together, the decisions suggest that courts are likely to scrutinize AI-assisted litigation materials through a highly fact-specific lens, with the availability of protection turning on the doctrine invoked, the user's role and the safeguards surrounding the platform at issue.

What does this mean for clients and legal counsel? The decisions in *Heppner* and *Morgan* send a clear signal: courts are paying close attention to how AI tools are used for legal matters and questions regarding confidentiality, work-product and attorney-client privilege will continue to persist. Organizations and their counsel should quickly establish clear policies and procedures governing AI use and implement training on the legal implications of AI use and risks of waiving protections. These policies should address appropriate use for AI platforms and place limitations on disclosure of confidential information. Organizations should consult legal counsel before using any AI tool in connection with legal matters and consider implementing contractual protections with vendors leveraging AI or AI platform providers to limit exposure

Bond attorneys regularly assist and advise clients on matters involving the use of artificial intelligence. For more information regarding AI matters, contact Jessica L. Copeland, CIPP/US Amber Lawyer, CIPM, CIPP/US, CIPP/E or any member of Bond, Schoeneck & King PLLC's artificial intelligence or cybersecurity and data privacy practice.

Thank you to Associate Ariyana DeWitz for assisting in the drafting of this memo.

BOND SCHOENECK & KING ATTORNEYS