FINN DIXON
& HERLING

SDNY Decision Highlights Risks to Confidentiality Posed by AI Tools

Artificial intelligence tools are changing legal work, both within businesses and law firms. While these tools present a number of opportunities and potential efficiencies, they also pose significant challenges and risks. One such risk was illustrated by a recent decision from Judge Rakoff in a criminal case pending in the Southern District of New York, *United States v. Heppner*, which highlights the challenges in maintaining the confidentiality of attorney-client communications and work-product when AI tools are used.

Although *Heppner* arose in a criminal case, its reasoning applies with equal force to civil litigation, regulatory inquiries, internal investigations, and corporate transactions. AI-generated records created today—prompts, outputs, and AI-generated transcripts of meetings—could be sought by adversaries in future disputes, investigations, and regulatory proceedings.

Key Takeaways

- Non-attorney communications with AI tools are not communications with an attorney, and therefore are not privileged and are subject to discovery, even if the AI tool is providing purported "legal advice."
- A client's input of attorney work-product into an AI tool, or use of an AI tool to transcribe attorney-client conversations, may destroy confidentiality and make the materials subject to discovery.
- The level of confidentiality can vary significantly depending on the type of AI deployment: consumer-grade tools offer little if any confidentiality protection; third-party enterprise tools with negotiated privacy terms can offer more protection; and self-hosted or single-user deployments offer the strongest confidentiality protection.
- AI notetaking and transcription tools pose a distinct and significant risk to privilege and confidentiality, particularly when they record conversations with counsel or capture sensitive deal discussions.
- Clients using AI tools in connection with legal matters should carefully consider the data protections and confidentiality provided by the AI tool, input privileged material or attorney work-product only at the direction of counsel, ensure that appropriate steps are taken so that protections from disclosure are maintained, and be aware of the ways in which AI tools can produce discoverable material in future disputes.

Background

The attorney-client privilege and related attorney work-product doctrine are fundamental to the ability of counsel to communicate freely and effectively with clients, without concern that third parties can compel disclosure of confidential communications and documents. The attorney-client privilege protects from disclosure (1) communications between a client and his or her attorney that (2) were intended to be, and in fact were, confidential, (3) for the purpose of obtaining or providing legal advice. Similarly, the work-product doctrine protects from disclosure materials prepared by or at the behest of counsel in anticipation of litigation, to "preserve a zone of privacy in which a lawyer can prepare and develop legal theories and strategies with an eye toward litigation, free from unnecessary intrusion by his adversaries."

The scope and particular application of the attorney-client privilege and work-product doctrine is sometimes complex. But as a general matter, to successfully invoke the protection of either it must be demonstrated that the documents and communications were kept confidential and not disclosed to third parties. *Heppner* demonstrates why both attorneys and clients must be mindful of the ways in which the use of AI tools can undermine this confidentiality.

Judge Rakoff: Claude AI Documents Not Protected From Disclosure

In the case pending before Judge Rakoff, Bradley Heppner is facing charges of securities and wire fraud. At the time of his arrest, agents seized Heppner's electronic devices, which contained a number of documents generated by Claude, Anthropic's large language model AI tool (the "AI Documents"). The AI Documents were generated by Heppner after he had received a grand jury subpoena and learned he was a target of a government investigation. The AI Documents contained Claude's outlines of potential defense strategies and legal and factual arguments relating to the government's anticipated charges, generated based on Heppner's prompts.

Heppner sought to protect the AI Documents from disclosure to the government, arguing that they are privileged or constitute attorney work-product because (1) his prompts to Claude included information that Heppner had learned from his counsel; (2) he had generated the AI Documents for the purpose of obtaining legal advice from his counsel; and (3) he subsequently shared the AI Documents with his counsel.

Judge Rakoff denied Heppner's request to shield the AI Documents from disclosure on several grounds, each of which illustrates important considerations regarding the use of AI tools.

1. "The AI Documents are not communications between Heppner and his counsel."

Judge Rakoff held, relying on well-established principles, that the fact Heppner's communications were with Claude, not with an attorney, precluded protection under the attorney-client privilege. Communications with a non-attorney—albeit communications regarding legal issues—are not protected by the privilege. Clients should be mindful when using AI tools internally that the fact that the documents or communications generated discuss or relate to legal issues does not itself protect them from disclosure. Even if the prompts or documents generated rely on information learned from counsel, the prompts and AI-generated documents are not communications between a client and an attorney, and therefore are not privileged.

2. "The communications memorialized in the AI Documents were not confidential."

Judge Rakoff also held that Heppner's communications with Claude were not confidential. Anthropic's written privacy policy (to which Heppner, like all users, consented) provides that Anthropic collects data on users' inputs and outputs, and that such data is used to "train" Claude and may be disclosed to third parties. Applying the same rationale applied by courts with respect to voluntary disclosure to third parties in other contexts (e.g., search engines, internet service providers, and phone companies), Judge Rakoff concluded that Heppner had no reasonable expectation of confidentiality in his communications with Claude.

AI tools differ significantly with respect to their protection of users' data. Attorneys are beginning to use tools that are created specifically for the provision of legal services and therefore have appropriate data privacy protections in place to protect the confidentiality of client data. The same is not true for consumer-grade AI tools—such as the free or individually paid versions of Claude or ChatGPT—which do not adequately protect confidentiality and can undermine protections from disclosure.

It is important to recognize that not all products marketed as "enterprise" or "business" AI tools provide equivalent protection. The level of confidentiality varies based on the nature of the deployment, and organizations should carefully evaluate the protections afforded by their AI tools:

- **Consumer-grade AI tools** are governed by standard terms of service that generally allow the collection of user inputs and outputs for model training and may also specifically permit disclosure to third parties. These tools present particular concerns not only for the confidentiality of legal materials and communications, but also confidential business information and trade secrets.
- **Enterprise cloud AI with negotiated agreements** may allow for confidentiality protections and preclude use of user data for model training and restrict the circumstances allowing for third-party disclosure. These tools nonetheless still present concerns, as user data is hosted and often retained by third parties, which may reserve disclosure rights and/or be subject to subpoena or discovery procedures.
- **Self-hosted or single-tenant AI deployments** that are operated and hosted by the user would generally provide the greatest confidentiality protections, as use would not require transmission of data to a third party. But even these tools present concerns regarding record creation and retention, and maintaining appropriate constraints on the dissemination of information within an organization. For example, wide dissemination of otherwise privileged communications or attorney work-product within an organization can present challenges to protecting the material from disclosure.

3. "Heppner did not communicate with Claude for the purpose of obtaining legal advice."

That Heppner communicated with Claude in order to facilitate future discussions with his counsel did not protect the AI Documents from disclosure. Judge Rakoff held that the non-privileged communications with Claude were not transformed into privileged ones simply because the communications/documents were (or were intended to be) later shared with counsel.

Clients sometimes use AI tools to generate questions for counsel, or to generate documents for counsel's review. The subsequent provision of documents to counsel does not generally render the documents privileged. The analysis focuses on the communications with the AI tool itself, which is not a communication with counsel for the purpose of obtaining legal advice, even if the client intends to later share the communication or the AI output with counsel.

This principle has particular significance for M&A transactions and corporate operations. Deal team members routinely analyze legal exposure, evaluate indemnification risk, assess regulatory issues, and draft internal summaries of counsel's advice. The use of AI tools can create detailed records of the client's internal assessments and deliberations that could be discoverable in postclosing disputes, including earnout litigation, indemnification claims, and alleged breaches of representations and warranties. The fact that the analysis was later shared with deal counsel does not retroactively protect it.

4. "The AI Documents do not merit protection under the work product doctrine because . . . they were . . . not prepared by or at the behest of counsel" and did not "reflect defense counsel's strategy."

Although Heppner shared and discussed the AI Documents with counsel, the documents were not protected from disclosure as attorney work-product because they were not generated at the direction of his counsel, and did not reflect his counsel's litigation strategy.

Clients should be aware that inputting attorney work-product—like drafts, memos, or transcripts of conversations with counsel—into an AI tool may preclude a future assertion that the material is protected from disclosure as attorney work-product. While there are certain circumstances when sharing attorney work-product with a third party may not prevent future assertion of the work-product doctrine (e.g., work product shared at the direction of counsel with an accountant for the purpose of facilitating legal advice), disclosure to an AI tool is unlikely to qualify for this exception. A *client's* disclosure of attorney work-product to an AI tool—particularly absent an *attorney's* direction to do so—may destroy the confidentiality needed to preserve the attorney work-product doctrine.

It is worth noting that on the same day *Heppner* was decided, a court in the Eastern District of Michigan reached a different conclusion in *Warner v. Gilbarco Inc.*, finding that a pro se litigant's use of ChatGPT to draft litigation documents was protected work product because the AI functioned as a "tool," akin to word processing software, and did not constitute disclosure to a "third party." More courts will be asked to address these issues going forward, and a uniform doctrinal framework is unlikely to become clear any time soon.

AI Notetaking and Transcription: A Distinct and Significant Risk

AI meeting assistants and transcription tools (*e.g.*, Zoom AI Assistant, Microsoft Copilot in Teams) present particular risks. These tools convert spoken conversations into verbatim transcripts, and often generate purported summaries of the conversations that are e-mailed to participants.

As illustrated by *Heppner*, sharing an otherwise privileged conversation with an AI tool for transcription or summary presents risks that that the privilege will be destroyed, making AI-generated transcriptions and summaries of conversations with counsel potentially subject to disclosure. **Therefore, AI meeting assistants should be disabled for conversations involving in-house or outside counsel.**

AI meeting assistants pose dangers even if the meetings are not otherwise privileged or are between non-attorneys. The transcription or summary of business conversations creates potentially discoverable records of conversations that would otherwise not be subject to scrutiny and misinterpretation by adversaries, regulators, or courts, including offhand or informal comments, preliminary assessments or opinions, board discussions, internal strategy sessions, and due diligence calls. AI-generated transcripts and summaries, even if not accurate, may be sought in discovery and used by adversaries or regulators. **Clients should carefully consider whether the use of AI meeting assistants should be allowed internally, and under what circumstances. If allowed at all, companies should ensure that appropriate data management and retention policies are in place with respect to the AI-generated outputs.**

We will continue to monitor developments in this area. Please contact us if you have any questions about your organization's use of AI tools and how such use may impact your legal interests.

- David R. Allen, 203-325-5003 or dallen@fdh.com
- Andrew M. Calamari, 203-325-5057 or acalamari@fdh.com

Finn Dixon & Herling LLP is a law firm with extensive experience providing corporate, transactional, investment management, securities, tax, executive compensation, bankruptcy and litigation counsel. Our clients include large and small corporations, venture capital and private equity firms, financial institutions, hedge funds, private equity funds, other investment funds, investment advisers, commodity pool operators, commodity trading advisers, broker-dealers, family offices, institutional investors, public and private businesses, executives, management teams and entrepreneurs.

These materials are intended to inform our clients and friends about developments in the law. They are not intended to constitute a legal opinion or advice or to address any client's legal issue or specific situation. The format of these materials, and the complex nature of the subject matter, required the making of general statements that summarize complex bodies of law and that may be incomplete in some respects. In addition, these materials speak as of the version date set forth below and may not reflect subsequent developments in the law or interpretations thereof. Accordingly, the reader is cautioned against using any of this material in specific situations without obtaining the advice of competent counsel. In light of the foregoing, and the general nature of these materials, these materials should not be regarded, or relied upon, as legal advice.