



When AI Becomes a Witness

Protect confidential info with policies & training

by: Greg Goldberg, BTA General Counsel

Artificial intelligence (AI) has entered the marketplace at a blazing speed. Employers and employees alike now routinely use large language models such as ChatGPT, Claude, Gemini and other AI platforms to draft emails, summarize documents, analyze contracts, prepare presentations and solve day-to-day problems. The productivity gains are substantial, but so are the legal risks. Some of the noted downsides previously highlighted in this space include automated decision-making bias, data leakage and hallucinations.



The United States District Court for the Southern District of New York has added a significant new risk that should serve as a stark warning for businesses that have not yet established acceptable AI use policies. The recent decision in *United States v. Heppner* holds that communications and documents generated through public AI platforms are not protected by the attorney-client privilege or the attorney work product doctrine.

Heppner involved an increasingly common fact pattern. Bradley Heppner, a corporate executive charged with securities and wire fraud, used Claude to generate more than 30 documents outlining the strategic details of his criminal defense. During an authorized search of his home, federal agents seized the documents and prosecutors sought to introduce them as evidence at his trial. Heppner's attorneys objected, citing the attorney-client privilege and attorney work product doctrine. Historically, the attorney-client privilege applies to confidential communications between attorneys and clients made for the purpose of obtaining legal advice. The attorney work product doctrine generally protects materials prepared by an attorney in preparation for litigation.

Rejecting both arguments, the court reasoned that information voluntarily disclosed to third-party AI providers lacks the confidentiality required for privilege protection, and that materials independently created through AI without counsel's explicit direction are not protected work product. In other words, AI chatbots are not attorneys, so communications with AI chatbots do not fall under the attorney-client privilege. Moreover, AI outputs are not prepared by attorneys in anticipation of litigation, so those outputs are not attorney work product.

Although Heppner arose in a criminal context, its implications extend far beyond the parties involved. Business owners should view the decision as a wake-up call regarding the information their employees may be entering into AI systems every

day. The court's ruling suggests that many publicly available AI platforms may be treated as third parties for privilege purposes. Thus, an employee who copies confidential legal advice into an AI chatbot and asks for a summary or strategic analysis may waive privilege over that information. Likewise, an executive who uploads sensitive facts and asks an AI model to evaluate legal exposure may find those communications subject to discovery in future litigation.

If employees routinely feed confidential information into consumer-grade AI systems without restrictions, future litigants may argue that the company failed to take adequate steps to protect its proprietary information. Consider a couple of common workplace scenarios: (1) A sales manager uploads a confidential customer list and asks an AI model to identify cross-selling opportunities. (2) An HR employee pastes an internal investigation report into an AI platform and requests a summary. In each case, information that the company would ordinarily treat as highly confidential has been transmitted to an outside platform whose terms of service may permit data retention, review or disclosure.

Many employees may not appreciate the distinction between using AI as a productivity tool and communicating with a trusted internal system. They may assume that because the interaction feels private, it is legally protected. Heppner underscores that such assumptions can be dangerous. Courts are likely to continue applying traditional confidentiality principles to emerging technologies rather than creating entirely new privilege rules for AI.

Business leaders should not interpret this development as a reason to prohibit AI altogether. Instead, companies should focus on implementing data governance tools and adopting acceptable AI usage policies.

The lesson from Heppner is straightforward: If an employee would not freely hand a document to a stranger outside the company, that employee should think carefully before handing it to an AI chatbot. In the age of AI, protecting confidential information requires more than locking file cabinets and securing networks. It requires clear policies, employee training and recognition that every AI prompt may someday become discoverable evidence. ■

Greg Goldberg, partner at Barta | Goldberg, is general counsel for the Business Technology Association. He can be reached at ggoldberg@bartagoldberg.com or (847) 922-0945.

