ALM | LAW.COM

New York Law Journal

Can 'Non-Confidential' Discovery Materials be Uploaded? To an AI Tool for Analysis—Maybe, It Depends!

By Mark Berman & Jessica Copeland

May 4, 2026

In the most recent federal court decision grappling with AI Tool use in litigation, the District Court in Kansas held that no litigation material, whether confidential or not, can be uploaded to an open AI Tool. See *Jeffries v. Harcros Chems. Inc.*, 2026 U.S. Dist. LEXIS 63182 (D. Kan. Mar. 25, 2026). This groundbreaking decision requires counsel to think twice, and perhaps a third time, before uploading discovery materials to an AI Tool for analysis.

Made with AI

Counsel and client alike must know whether the AI Tool shares the uploaded information and analysis with others beyond the party that uploaded it and whether the uploaded information is used to train the AI Tool beyond the analysis being performed just for the uploaded party. *Jeffries* stands for the proposition that only a closed AI tool can be used to ensure confidentiality and security of the uploaded information which, among other things, would allow the uploaded information to be able to clawed back or deleted if necessary.

In *Jeffries*, the court issued a protective order concerning the uploading of Confidential Information to an AI Tool for analysis, and required that the party using the AI Tool to must provide the other parties with notice and an opportunity to object. The court ordered that information uploaded had to be used in a secure environment and that the Confidential Information not be used to train or improve

any AI Tool except one used exclusively for the subject action.

The court further provided that, to the extent that an AI Tool is trained or improved using the uploaded Confidential Information, the information must be destroyed at the conclusion of the action and not made accessible to anyone not authorized to have access to Confidential Information. Critically, the court noted that "as a practical matter, these provisions effectively require parties to use only closed or secure AI Tools (closed AI Tools) for Confidential Information."

Defendants thereafter sought to amend the protective order to expand the AI provisions to apply to all "Discovery Materials"—*i.e.,* all documents and information produced in discovery. The court summarized defendant's argument as seeking to prevent parties from uploading even non-confidential documents into public or «open loop» generative artificial intelligence tools (collectively, open AI Tools)."

Defendants explain that AI Tools rely on sophisticated machine learning models that work by identifying and encoding patterns and relationships in massive amounts of data and then using that information to understand users' natural language requests or questions and respond with relevant new content. But, unlike closed AI Tools, the use of open AI Tools "risks disclosure, loss of control, and uncertainty concerning the security, storage, and other data-handling of that information."

Defendants point out that, because an open AI Tool uses the data submitted to it to continually develop and improve the tool, it is "practically impossible" to claw back data later determined to be privileged, or delete data from the open AI Tool at the conclusion of the action (as required by the deletion clause in the Protective Order) because the information was used to train the AI Tool. Defendants further explain the harm that might result if information cannot be clawed back or deleted—*e.g.,* waiving confidentiality or privilege of information

that was inadvertently disclosed without a "confidential" designation; revealing sensitive data or personal information from the AI Tool's training datasets; and potentially violating counsel's professional duty to safeguard information relating to representation of a client... Lastly, Defendants contend that their proposed amendment is necessary to protect against exposure of critical infrastructure and data breach.

The court addressed plaintiffs' contention that defendants' proposal sought to increase plaintiffs' litigation costs by depriving them of open AI Tools to analyze discovery materials and making it more burdensome for plaintiffs to pursue the litigation. The court did not find that plaintiffs would suffer an undue burden if the court were to grant defendants' motion, noting that plaintiffs and their attorneys initiated this lawsuit knowing that class action litigation is expensive, including the costs of eDiscovery. Further, the court noted that the proposal '"applies equally to all parties and allows all parties to use Closed AI Tools that meet basic security requirements,' thereby

putting the same financial burden on plaintiffs and defendants."

The court rejected plaintiffs' contention that defendants' proposed amended protective order deprived them of their First Amendment right to use and disseminate nonconfidential discovery materials, noting that a protective order would not offend the First Amendment when it is entered based on a showing of good cause, is limited to the context of pretrial civil discovery, and does not restrict the dissemination of the information if gained from other sources.

The court noted that defendants conceded that their proposed amended protective order "does not in any respect affect how all parties—consistent with applicable law, ethical requirements, and professional standards—can publicize non-confidential documents by posting such documents to a website, making documents available to the media, or attaching documents to a court filing."

Plaintiffs "never directly address defendants' argument that clawing back or deleting data submitted to an open AI Tool is impossible as a practical matter because such data is used to continually develop and improve the tool." The court found that the "use of widely available AI Tools presents the opportunity for a centralized repository that makes information available to the public at a scale that was not historically available and ignores the very real security risks of public AI Tools, including the inability to effectively claw back information from the AI Tool." Finally, the court stated:

It is indisputable that generative AI may automate many time-consuming tasks in the eDiscovery process, such as significantly accelerating document review, quickly summarizing documents, streamlining privilege review and logging, identifying named entities like key people and organizations, extracting important topics, and automating writing tasks, such as drafting deposition questions, creating narrative timelines from evidence, and drafting legal briefs. But defendants' proposal does not foreclose a party from using *any* AI Tools; it only prohibits using open AI Tools while allowing the use of closed AI Tools—for good reason. The wholesale submission of discovery materials to an open AI Tool for these eDiscovery tasks could expose massive amounts of data. These actions may violate

U.S. data privacy laws and the stricter GDPR disclosure rules, which set a high standard for protecting individuals' information and requires documented consent to be "freely given, specific, informed and unambiguous."

In conclusion, the court reasoned that:

If the court were to allow a party to upload all non-confidential documents and materials produced by another party to an open AI Tool, thereby making all such data amenable to public consumption, parties may err on the side of underproducing potentially responsive documents or seek to make extensive redactions of irrelevant or non-responsive information. Defendants' proposed amendment allowing the use of closed AI Tools, as opposed to open AI Tools, will facilitate discovery by incentivizing more fulsome document productions.

The significance of the holding in *Jeffries* is that it evolves the judicial conversation about AI use in litigation beyond discrete misuse issues and into the architecture of discovery itself. Rather than treating AI use as merely a question of lawyer competence or convenience, the court framed the issue as one of control over litigants' data and discovery materials: whether information can be clawed back, deleted at the end of the case, and kept from being absorbed into a public-facing system.

In that respect, *Jeffries* is especially significant because it extends those concerns to non-confidential discovery materials, reasoning that open-platform ingestion also creates privacy, privilege, and production-integrity risks and may distort party behavior by encouraging underproduction or excessive redaction.

Jeffries also fits within an emerging line of AI-use decisions, but its rationale both overlaps with and departs from the two recent cases—*United States v. Heppner,* 2026 U.S. Dist. LEXIS 67939 (S.D.N.Y Feb. 17, 2026) and *Morgan v. V2X*, 2026 U.S. Dist. LEXIS 32697 (D. Colo. March 30, 2026). Like *Heppner, Jeffries* is skeptical that users can assume meaningful confidentiality when they submit litigation-related materials to an open AI platforms that may retain, train on, and/or disclose inputs; but *Heppner* was limited to whether AI exchanges were protected by attorney-client privilege or work product doctrine in a criminal case and held they were not where the defendant acted without counsel's direction and used a publicly available platform.

Morgan, by contrast, arose in the civil protective-order context and distinguished *Heppner,* holding that a *pro se* litigant could still invoke Rule 26(b)(3) protection for some AI-assisted litigation work, even though the court required disclosure of the AI platform used for Confidential Information and imposed strict limits on uploading Confidential Information to open and freely available AI tools lacking contractual safeguards.

Read together, the three decisions suggest that courts are converging on a practical rule: AI may be used in litigation, but only with careful attention to confidentiality, contractual guardrails, and the legal doctrine implicated by the particular use case, and calling into question an open AI platform.

Mark A. Berman *and* **Jessica L. Copeland** *are members at Bond, Schoeneck & King PLLC.*