KIRKLAND & ELLIS

Kirkland Alert

A Federal Court Charts a Path on AI, Protective Orders and Work Product in Discovery

20 May 2026

A federal court in Colorado has issued one of the first detailed AI-specific protective order provisions governing large language model use in litigation. In *Morgan v. V2X, Inc.*, No. 25-cv-01991 (D. Colo. Mar. 30, 2026), Magistrate Judge Maritza Dominguez Braswell approved protective order language permitting AI use so long as certain confidentiality measures are met. The court also held that a pro se litigant's use of AI in litigation preparation is entitled to work product protection under Federal Rule of Civil Procedure 26(b)(3), though this protection does not extend to disclosure of the AI tool's identity. The decision follows two recent cases reaching differing conclusions on AI and work product protection: *United States v. Heppner*, 2026 WL 436479 (S.D.N.Y. Feb. 17, 2026) and *Warner v. Gilbarco, Inc.*, 2026 WL 373043 (E.D. Mich. Feb. 10, 2026).

The dispute arose because both parties used AI but disagreed about how AI should interact with confidential information under the existing protective order, which provided that confidential information "shall not, without the consent of the designating party or further Order of the Court, be disclosed" except under limited circumstances. The defendant sought an amended protective order restricting AI use with confidential materials and an order compelling the pro se plaintiff to disclose which AI tool he was using. The plaintiff did not oppose amending the protective order in principle but resisted disclosing his AI tool, arguing the defendant sought to "create an unfair 'technological gap' by barring a pro se litigant from using modern analytical aids."

The court first addressed whether Rule 26(b)(3) applies to pro se litigants, concluding that it does based on the rule's plain language protecting materials "prepared in anticipation of litigation or for trial by or for another party or its representative." Judge Braswell emphasized that the importance of these protections is "magnified in the

context of AI—one of the most powerful knowledge tools ever to become available to the masses," and rejected any reading that conditions work product protection on attorney involvement. The court found that conditioning work product protection over AI materials on the involvement of counsel "finds no support in the rule's text and would further disadvantage unrepresented litigants."

The court distinguished *Heppner*, where the U.S. District Court for the Southern District of New York declined to extend work product protection to AI materials prepared by a represented criminal defendant acting without counsel's direction. Judge Braswell noted two key differences: (1) *Heppner* was a criminal matter, whereas *Morgan* is a civil case governed by Rule 26(b)(3), which broadly protects the work product of a party, not merely counsel; and (2) unlike *Heppner*, where the defendant acted entirely apart from his lawyer, no party-attorney gap exists in the pro se context, where the litigant is both the party and the advocate.

The court also rejected the argument that inputting information into a publicly available AI tool automatically waives work product protection. Looking to Fourth Amendment precedent, including *Carpenter v. United States*, 585 U.S. 296 (2018), the court noted the Supreme Court's holding that "the mere fact that information is held by a third-party intermediary does not automatically extinguish reasonable privacy expectations." Judge Braswell found that "routing information through a third-party system does not forfeit all privacy." This aligns with *Warner*, which found that "ChatGPT and other generative AI programs are tools, not persons," and the disclosure is therefore not "to an adversary or in a way likely to get in an adversary's hands."

However, work product protection did not extend to the AI tool's identity. The court found the plaintiff failed to demonstrate how disclosing the tool's name would reveal mental impressions or case strategy, and the defendant's request was "legitimate and reasonable" to assess whether confidentiality had been compromised.

Turning to the protective order, the court rejected both parties' proposals. The plaintiff's language permitting AI use in "a secure, closed-circuit environment" addressed concerns about unauthorized access rather than the distinct confidentiality risks posed by widely available platforms. The defendant's proposal was overly protective and appeared "crafted to fit the precise bounds of Defendant's contractual engagement with AI providers."

Judge Braswell instead adopted a provision prohibiting any party from inputting confidential information into any modern AI platform (including generative, analytical or large language model-based tools) unless the AI provider is contractually prohibited

from storing or using inputs for training and from disclosing inputs to third parties except where essential to service delivery. The provision also requires that the provider allows the ability to delete confidential information upon request and that parties retain written documentation of these protections.

> *No party or authorized recipient may input, upload, or submit CONFIDENTIAL Information into any modern artificial intelligence platform, including any generative, analytical, or large language model-based tool ("AI"), unless the AI provider is contractually prohibited from: (1) storing or using inputs to train or improve its model; and (2) disclosing inputs to any third party except where such disclosure is essential to facilitating delivery of the service. Where disclosure to a third party is essential to service delivery, any such third party shall be bound by obligations no less protective than those required by this Order. In addition, the AI provider must contractually afford the party or authorized recipient the ability to remove or delete all CONFIDENTIAL information upon request. A party intending to use AI that it contends meets these requirements must retain written documentation of these contractual protections.*

The court acknowledged this provision will likely prevent use of "most, if not all, mainstream low-to-no-cost AI" for processing confidential information and that enterprise-tier accounts may be available only through organizational procurement or at costs a pro se litigant is unlikely to bear. The court cautioned against over-designation of confidential materials and noted in a footnote "a growing problem in the age of AI: as large firms pour thousands of dollars into enterprise-grade AI and make their use of AI more secure, efficient, effective, and powerful, how will a pro se litigant or a litigant who cannot afford big-ticket legal services and better AI keep up?"

Morgan demonstrates that laws addressing AI-related discovery and privilege disputes continue to evolve, with significant practical implications. Key considerations arising from the decision include:

- The impact of counsel's direction and supervision when using generative AI in connection with litigation or investigations, given *Morgan*'s emphasis on the party-advocate distinction.
- The sufficiency of negotiated provisions in protective orders that address use of AI.
- The impact of using enterprise-tier accounts that offer additional controls around the use and retention of confidential information.
- The effect of AI providers' privacy policies that permit data collection, model training and third-party disclosure on confidentiality and privilege determinations.

- The potential requirement to disclose the AI tool used to process confidential information, given the holding in *Morgan* that the identity of an AI tool may not be protected work product.

Authors

Amber L. Whipkey

Partner / Washington, D.C.

Dana R. Bucy Miller

Partner / Washington, D.C.

Related Services

Practices

- Litigation
- eDiscovery Strategy
- Artificial Intelligence & Related Fields

Suggested Reading

- 10 March 2026 Kirkland Alert Two Federal Courts Chart Diverging Paths on the Discoverability of LLM Interactions
- 17 February 2026 Kirkland Alert Illuminating AI: The EU's First Draft Code of Practice on Transparency for AI-Generated Content
- 01 August 2024 Kirkland Alert AI Act Arrives: EU Equips AI With a New Rulebook