



AI 2035: The Legal Profession and the Judiciary in the Age of Artificial Intelligence

Vendor Selection and Risk Assessment for AI Tools

This session provides a practical framework for evaluating and selecting AI vendors, with a focus on due diligence, performance criteria, and integration considerations. Attendees will gain tools to assess risk, compare solutions, and make informed procurement decisions aligned with organizational needs.



Marcus Harris, Partner, Taft

Marcus Harris is a partner at Taft Stettinius & Hollister LLP specializing in software licensing and technology disputes. Marcus advises clients on enterprise software agreements and litigates complex implementation failures. He brings in-house experience from major technology companies. Marcus is widely recognized for his expertise in technology law and cybersecurity.



Chad Main, Founder, Percipient

Chad Main is the founder of Percipient, a legal technology company focused on improving litigation outcomes through data and analytics. Chad began his career as a litigator in Los Angeles and Chicago before launching Percipient. He is a strong advocate for leveraging technology to enhance legal practice. Chad also hosts the Technically Legal podcast. He regularly speaks on legal innovation and the use of data in litigation.



Michael Quartararo, President, ACEDS & Professional Development

Michael Quartararo is President of the Association of Certified E-Discovery Specialists (ACEDS). Michael has more than 25 years of experience training legal professionals in e-discovery and legal technology. He previously held leadership roles at major law firms and has authored books on e-discovery project management. Michael frequently lectures at law schools and industry events. He is a recognized expert in legal technology and information governance.



Moderator: Patricia McCarthy, Attorney at Law

Patty McCarthy is a passionate and accomplished leader with more than 20 years of sales and management experience in the legal industry focused on generating revenue and providing an exceptional customer experience. Her professional path integrates a trifecta of experiences and skills: accounting and business experience, litigation experience, and sales. Patty was most recently a regional sales manager for LexisNexis for more than 20 years.

THE CHICAGO BAR ASSOCIATION PRESENTS:

**AI 2035: The Legal Profession and the
Law in the Age of Artificial Intelligence**

**Vendor Selection and Risk
Assessment for AI Tools**

May 11, 2026

1:30 – 3:00 pm CT



THE
**CHICAGO
BAR
ASSOCIATION**

Speakers



Marcus Harris

Partner
Taft, Stettinius & Hollister
LLP



**Mike
Quartararo**

President
Association of Certified
E-Discovery Specialists
(ACEDS)



Chad Main

Founder
Percipient



Agenda

- 5 min - Introductions and agenda outline
- 10 min - Vendor evaluation for legal teams
- 10 min - Legal AI use cases and the vendor landscape
- 10 min - Baseline vendor due diligence
- 5 min - AI specific evaluation criteria
- 10 min - Security, confidentiality and privilege protection
- 10 min - Ethical and professional responsibilities
- 5 min - Regulatory and compliance risks
- 5 min - Governance and oversight
- 15 min - Q & A

Handouts:

- (1) PowerPoint Slides
- (2) Warner v. Gilbarco (E.D. Mich. 2026)
- (3) USA v. Heppner (SDNY 2026)
- (4) Morgan v. V2X, Inc. (D. Colo. 2026)
- (5) White v. Walmart (S.D. Ind. 4/14/26)
- (3) Vendor Risk Assessment/Checklist

Why Vendor Selection Is Different for Legal Teams

- Confidentiality and privilege obligations
- Ethical and professional responsibility obligations
- eDiscovery and litigation defensibility (methodology, QC, audit trail)
- Risk of sanctions and spoliation exposure from process failures
- Client outside counsel guidelines and security requirements
- Long-term reputational risks





Legal Use Cases

- Initial document drafting
- Early case assessment
- Contract analysis
- Legal research & cite checking
- Summarization & digestion
- Document classification/analysis
- Chronology generation
- Privilege flagging
- Case strategy & issue analysis
- Timekeeping
- Legal intake & triage
- Translation

Legal AI Vendor Landscape

- Legal-specific vs. general AI platforms (contract systems, research)
- eDiscovery platforms (TAR / review acceleration / analytics)
- Deposition & transcript intelligence (summaries, issue tagging)
- Litigation analytics (judge trends, motion outcomes)
- General LLM platforms adapted for litigation workflows
- “AI powered” vs. actual AI



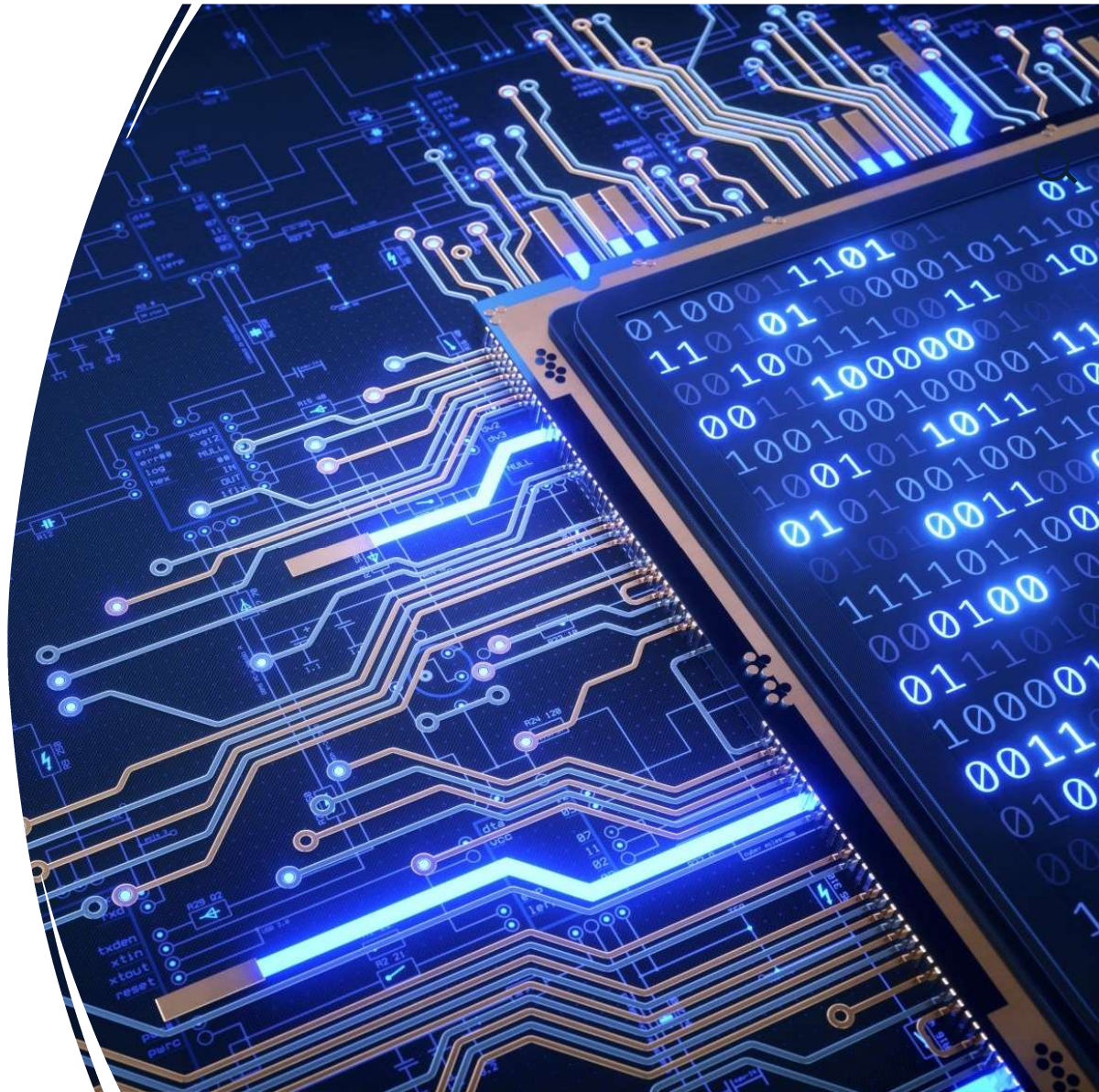
Baseline Vendor Due Diligence

- Company stability, roadmap, and continuity
- Legal industry experience
- Litigation references and evidence of scale (matters, data volumes)
- Product maturity
- Implementation and support models (Terms of Service)
- Pricing clarity (users, data, usage-based AI fees)



AI-Specific Evaluation Criteria

- Type of AI in use
- Training data sources
- Accuracy and validation
- Hallucination risk and controls for generative features
- Validation methods (sampling, benchmarks, precision/recall)
- Explainability and audit logs for defensibility; governance
- Human-in-the-loop guardrails and escalation paths



Security, Confidentiality, and Privilege Protection

- Open systems vs. private systems
- Data storage and training sources
- Encryption, access controls, data security
- Data residency, retention, and verified deletion
- No training on client data by default (opt-in only, if ever)
- Incident response SLAs and breach notification obligations





Ethical & Professional Responsibility in the Use of AI

- Duty of competence
- Supervision of AI-assisted work
- Accuracy obligations in filings and representations to court
- Privilege, work product, and the confidentiality of client information
- Bias and fairness concerns in analytics and summaries

What are the courts saying?

White vs. Walmart, No. 1:25-cv-01120-RLY-TAB (S.D. Indiana 4/14/26) (plaintiff failed to satisfy the meet and confer requirements under FRCP because counsel exclusively relied on a generative AI program to identify discovery deficiencies and plaintiff did not confer in good faith; the court ordered plaintiff to exercise independent human discretion over the generative AI outputs and to serve complete discovery responses by a specified deadline)

Morgan vs. V2X, Inc., No. 25-cv-01991-SKC-MDB (D. Colo. 3/30/26) (*pro se* employment discrimination plaintiff must disclose the use of AI tool because identifying the tool itself does not reveal mental impressions or case strategy)

United States vs. Heppner, No. 1:25-CR-9593 (SDNY 2/17/26) (defendant who, without knowledge of counsel, used public version of Claude LLM to generate “case strategy” reports in response to indictment waived privilege and is not entitled to privilege or work product protection over documents generated by LLM)

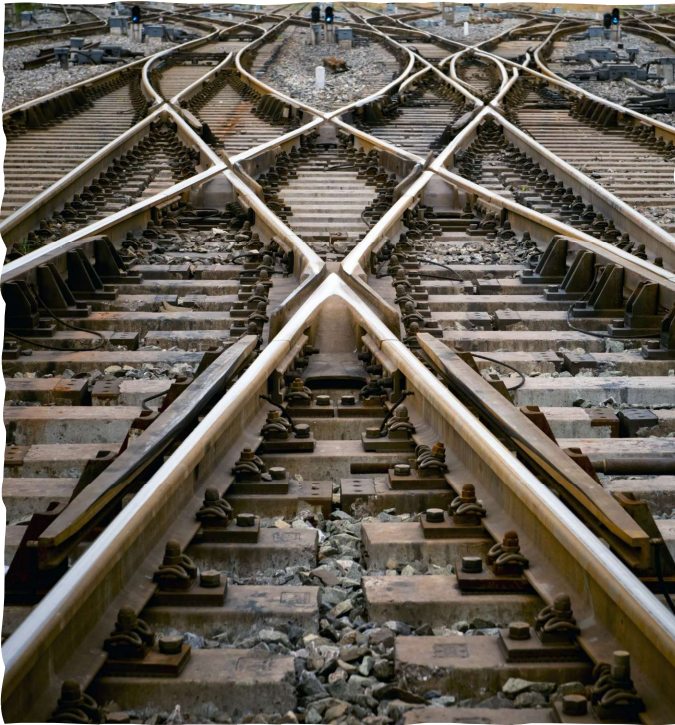
Warner v. Gilbarco, No 2.24-CV-12333 (E.D. Mich. 2/10/26) (sustaining plaintiff’s work product objections to defendant’s request for documents concerning use of third-party AI tools)

Regulatory and Compliance Risk

- Emerging AI regulatory landscape
- Privacy and data protection law and obligations
- Cross-border data issues for multinational matters
- Auditability, logs, and retention requirements
- Vendor compliance maturity and independent attestations



Governance and Oversight



- Data ownership, permitted use, and confidentiality terms
- AI governance committees and policy development
- Usage training and monitoring
- IP rights in outputs; restrictions on vendor reuse
- Indemnification, liability caps, and dispute support
- Pilot programs, proof of concept, data gathering
- Exit plan: data return, portability, verified deletion

Key Takeaways

- Always focus on the use case first – the legal work
- Legal AI vendor selection is a risk assessment decision
- Due diligence in vendor selection must be deeper for AI
- Data security, confidentiality, and validation controls are paramount – these are non-negotiable
- Governance ensures safe scaling—and keeps lawyers accountable



Thank You!

**Questions &
Answers**



Potential Complex Liability Issues

- “Supervision” of legal work may be harder to define in an AI-driven system
- Accountability when an AI tool operates beyond its intended boundaries
- Terms of service in vendor contracts need to be updated
- Insurance and risk mitigation will need to evolve . . . quickly



ARCHIE MORGAN, Plaintiff,

v.

V2X, Inc., Defendant

Civil Action No. 25–cv–01991–SKC–MDB

United States District Court, D. Colorado

March 30, 2026

Maritza Dominguez Braswell, United States Magistrate Judge

ORDER

*1 Before the Court is Defendant's Motion to Amend the Stipulated Protective Order, seeking to add language that specifically addresses the use of modern artificial intelligence tools (“AI”), and asking the Court to compel disclosure of Plaintiff's AI. ([“Motion”], Doc. No. 52). Plaintiff opposes, in part. (Doc. Nos. 58, 59.) Defendant has replied. (Doc. No. 60.) After considering the Motion, applicable law, and facts and circumstances of this case, **the Motion is GRANTED, in part.**

SUMMARY FOR PRO SE PLAINTIFF

The Court is granting Defendant's Motion, in part. Federal Rule of Civil Procedure 26(b)(3) can protect your mental impressions and litigation preparation materials, but you must disclose the name of any AI tool you used in connection with Confidential Information. This is because you have not demonstrated that identifying the tool itself will reveal your mental impressions or legal strategy, and Defendant needs that information to assess whether Confidential Information was compromised. The Court is also amending the Protective Order to address AI use. The practical effect is that you may not upload, input, or submit Confidential Information into any mainstream AI tool like standard ChatGPT, Claude, Gemini, or similar platforms.

BACKGROUND

This is an employment discrimination case where Plaintiff, a self-described “qualified Black American manager,” claims he was subjected to a hostile work environment and eventually “terminated based on his race and national origin and in retaliation for protected activities, including opposing sexual harassment and engaging in protected whistleblowing activity.” (Doc. No. 35 at 2-3.)

Defendant says Plaintiff was discharged for “legitimate and non-discriminatory, non-retaliatory reasons,” after “a workplace complaint was lodged against [Plaintiff],” and Defendant “conducted a thorough investigation, including interviewing and/or taking the statements of more than 30 witnesses.” (Id. at 3-4.)

The Dispute

Defendant brought the instant Motion shortly after Plaintiff moved to compel an insurance policy. ([“Plaintiff's MTC”], Doc. No. 48.) Plaintiff's MTC claimed that Defendant was refusing to produce a copy of the insurance policy, as “leverage to force Plaintiff's consent to a modified Protective Order.” (Doc. No.

48 at 2.) Specifically, Plaintiff claimed that Defendant sought disclosure of Plaintiff's AI tool, and restrictions on Plaintiff's AI use, before it would provide the insurance policy to Plaintiff. (Id.) Plaintiff characterized this as "holding a four-month overdue disclosure 'hostage' to force an amendment to a Protective Order," in a way that "creates an unfair 'technological gap' by barring a pro se litigant from using modern analytical aids while Defendant's firm maintains its own proprietary AI and cloud-based systems." (Id. at 3.)

The Court struck Plaintiff's MTC for failure to follow the Court's discovery dispute procedures but set a discovery hearing to address Plaintiff's concerns. (Doc. No. 51.) However, the morning of the discovery hearing, Defendant's counsel emailed Chambers saying:

**2 I am writing on behalf of Defendant, V2X, Inc. ("V2X"), with regarding to the discovery conference set in the above-referenced case for 12:00 p.m. MT today, March 3, 2026, in connection with Plaintiff Archie Morgan's motion to compel. See ECF Nos. 48, 51. Mr. Morgan is cc'ed on this correspondence and agrees to the relief requested herein.*

Per the Court's direction, the parties meaningfully conferred via videoconference on February 26, 2026. Following that conferral, the parties resolved their discovery dispute regarding Mr. Morgan's motion to compel discovery, and V2X has produced to Plaintiff the requested document underlying his motion. Accordingly, the parties jointly request that the Court vacate the discovery conference set for later today.

Accordingly, the Court vacated the hearing.

Upon careful review of the instant Motion and related materials, the Court finds it is based on some of the same disputes underlying Plaintiff's now stricken MTC. Both parties appear to be using AI in connection with their litigation work, but they disagree on how AI should or should not be used in connection with Confidential Information as defined in the current Protective Order. (Doc. No. 30.)

The Current Protective Order

The current Protective Order allows the parties to designate information "Confidential" when it "is confidential and implicates the privacy or business interests of the parties, including but not limited to: medical and personal financial information, private personnel information, trade secrets, and other proprietary business information." (Doc. No. 30 at 1.) The Protective Order provides that all Confidential Information "shall not, without the consent of the designating party or further Order of the Court, be disclosed," except under limited, specifically enumerated, circumstances. (Id. at 2.)

Defendant's Motion & Plaintiff's Response

Although Defendant's Motion is styled as one to amend the current Protective Order, it requests two forms of relief. First, Defendant asks the Court to enter an amended protective order with new language that specifically addresses its AI-related concerns. Second, Defendant asks the Court compel Plaintiff to "disclose the identity of the AI tool [Plaintiff] is utilizing in this case so that [Defendant] can determine

whether it does, in fact, have appropriate safeguards in place regarding [Defendant's] confidential information.” (Doc. No. 52 at 5.)

For his part, Plaintiff does not oppose amending the current Protective Order, but he offers competing language. Plaintiff does however oppose disclosure of his AI, saying “[t]he specific software, research platforms, and analytical tools chosen by a litigant to review discovery, synthesize information, and prepare for trial fall squarely under the Work-Product Doctrine, codified in Federal Rule of Civil Procedure 26(b)(3).” (Doc. No. 58 at 2.)

ANALYSIS

AI is forcing litigants and courts to confront difficult questions about how and to what extent longstanding protections will apply when parties use AI to assist them in the litigation process. In particular, courts are beginning to wrestle with practical questions surrounding confidentiality, work product, and privilege. This dispute raises two such questions: (1) to what extent will work product protections apply to a *pro se* litigant's use of AI, and (2) to what extent should a protective order expressly restrict the use of AI? The Court addresses each question in turn.

I. Do work product protections apply to *pro se* Plaintiff's use of AI, and in particular, to his tool selection?

*3 Defendant seeks disclosure of Plaintiff's AI so it can “verify it has appropriate confidentiality restrictions.” (Doc. No. 60 at 3; see also Doc. No. 52 at 5.) Plaintiff resists, citing Federal Rule of Civil Procedure 26(b)(3). (Doc. No. 58 at 2.) The Court begins by considering the applicability of the Rule, then it moves on to consider the scope of its protections under these facts and circumstances.

A. Applicability of Rule 26(b)(3)

Federal Rule of Civil Procedure 26(b)(3)(A) protects “documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative.” Mental impressions, conclusions, opinions, and legal theories, are contents that may be embedded in such documents and tangible materials. See Rule 26(b)(3)(B) (referencing Rule 26(b)(3)(A) and recognizing that “those materials” may include mental impressions, conclusions, opinions, and legal theories). Rule 26(b)(3)(B) adds another layer of protection to mental impressions and opinions when they come from “a party's attorney or other representative...” This heightened protection is consistent with the doctrine's origins in *Hickman v. Taylor*, 329 U.S. 495 (1947).

The Tenth Circuit has not weighed in on the applicability of Rule 26(b)(3) to *pro se* litigants, but the plain language broadly refers to things prepared in anticipation of litigation by any *party*, language that would “seem to include material created by a party before retaining a lawyer as well as a party who never actually hires an attorney.” Jennifer A. Gundlach & Zeus Smith, *Expanding the Federal Work Product Doctrine to Unrepresented Litigants*, 30 GEO. J. ON POVERTY L. & POL'Y 53, 62 (2022) (hereinafter “Gundlach & Smith”). This reading is reinforced by the Rule's history. See *generally id.* Prior to the 1970 amendments, some courts had declined to protect work product prepared by anyone other than an attorney, but the Advisory Committee's amendments were specifically designed to extend protection

beyond attorneys' work product to materials prepared by or for a *party*. *Id.* at 61–62. Since then, courts routinely interpret the Rule to apply not just to attorney work product, but to a *pro se* litigant's work product as well. *See Carbajal v. St. Anthony Cent. Hosp.*, 2014 WL 2459713, at *2 (D. Colo. June 2, 2014) (assuming without deciding that the work product protection in Rule 26(b)(3) applies to a *pro se* litigant); *Anderson v. Furst*, 2019 WL 2284731, at *4 (E.D. Mich. May 29, 2019) (stating, “a *pro se* litigant[] has a right to assert work product protection” under Rule 26(b)(3)); *Yates v. Cobb Cnty. Sch. Dist.*, 2016 WL 9444452, at *2 (N.D. Ga. Aug. 4, 2016) (finding persuasive authority indicating *pro se* plaintiffs can assert work product protections under Rule 26(b)(3)).

Moreover, courts have broadly interpreted the rule to protect not just litigation preparation materials, but also the mental impressions, opinions, and theories of *parties*. *See, e.g., Moore v. Tri-City Hosp. Auth.*, 118 F.R.D. 646, 649–50 (N.D. Ga. 1988) (finding work product protection applied to plaintiff's diary); *Ortega v. New Mexico Legal Aid, Inc.*, 2019 WL 5864784, at *3 (D.N.M. Nov. 8, 2019) (finding *pro se* plaintiff's mental impressions, opinions and legal theories set forth in diaries, agendas, notebooks, and more, to be protected work product); *Carrier-Tal v. McHugh*, 2016 WL 9185306 (E.D. Va. Feb. 3, 2016) (overruling objections to a magistrate judge's order that found work product protections applied to a *pro se* plaintiff's mental thoughts, impressions, and litigation strategy); *Moore v. Kingsbrook Jewish Med. Ctr.*, 2012 WL 1078000, at *8 (E.D.N.Y. Mar. 30, 2012) (overruling objections to magistrate judge order that found a *pro se* litigant's personal notes reflected her mental impressions of the deposition and the litigation and were therefore protected work product). Thus, while only attorneys and “other representatives” receive additional heightened protection under Rule 26(b)(3)(B), a party's own mental impressions are nevertheless protected under Rule 26(b)(3), generally.

*4 The importance of applying these protections to *pro se* litigants is magnified in the context of AI—one of the most powerful knowledge tools ever to become available to the masses. This is because *pro se* litigants are forced to act as both party and advocate, simultaneously. *See* Gundlach & Smith, at 70 (quoting *Boegh v. Harless*, 2021 WL 1923365, at *6 n.5 (W.D. Ky. May 13, 2021)). And for the first time in history, widespread access to powerful technology may make that dual role surmountable. A reading of Rule 26(b)(3) that conditions 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. *Pro se* litigants are held to the same standard as represented litigants. *See Requena v. Roberts*, 893 F.3d 1195, 1205 (10th Cir. 2018). They should be afforded the same protections. *See Nielsen v. Soc'y of New York Hosp.*, 1988 WL 100197, at *2 (S.D.N.Y. Sep. 22, 1988) (saying, “[i]f plaintiff were represented by counsel, his attorney's notes in similar circumstances would not be subject to production. A plaintiff appearing *pro se* is entitled to no less protection.”).

The Court is mindful of a recent decision that at first blush may appear contrary. *See United States v. Heppner*, 2026 WL 436479 (S.D.N.Y. Feb. 17, 2026). In *Heppner*, the court observed that work product protections have historically been rooted in shielding the mental impressions and legal theories of attorneys. *Id.* at *3. It concluded that a represented criminal defendant who used an AI tool on his own initiative, without any direction or involvement from their attorney, could not claim work product protection over the resulting materials. *Id.* at *3-4. The *Heppner* decision is of course not binding on this Court, but even if it were, the case is distinguishable for at least two reasons. First, *Heppner* was a

criminal matter; this is a civil case governed by the Federal Rules of Civil Procedure, and the text of Rule 26(b)(3) broadly protects the work product of a party, not merely counsel. Second, in *Heppner*, there was a gap between the party and the attorney because the defendant acted entirely apart from his lawyer. No such gap exists in the *pro se* context. A *pro se* litigant is simultaneously the party and the advocate.

Here, like in *Warner v. Gilbarco, Inc.*, 2026 WL 373043 (E.D. Mich. Feb. 10, 2026), Plaintiff can assert work product protections in connection with his AI use. It is true that AI systems like ChatGPT, Claude, Gemini, and others widely available to the public, collect user data for training and other purposes. But in this Court's estimation, that does not eliminate all expectations of privacy or automatically waive protections.

Today, nearly all electronic interaction passes through third-party systems. Google, for example, hosts millions of accounts, and by extension, has access to millions of messages, emails, documents, videos, and more. Moreover, we now know that our phones, computers, in-home smart devices, and other electronics, collect information about us to offer more bespoke services. Does that mean that anyone with a Gmail account has forfeited all rights to confidentiality and privacy? In *United States v. Warshak*, the Sixth Circuit held—albeit in the context of a Fourth Amendment seizure analysis—that email subscribers have a reasonable expectation of privacy in the contents of emails stored with commercial internet service providers. 631 F.3d 266, 268 (6th Cir. 2010). The court rejected the idea that intermediary access alone extinguishes privacy expectations. *Id.* at 285-86. And though the Tenth Circuit did not fully weigh in on this issue in *United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016), the Supreme Court has since held that the mere fact that information is held by a third-party intermediary, does not automatically extinguish a reasonable expectation of privacy in that information. *Carpenter v. United States*, 585 U.S. 296, 310-16 (2018).

*5 The Fourth Amendment governs searches and seizures and offers a wholly different legal framework from the work product doctrine, but the principle reflected in those cases is informative: routing information through a third-party system does not forfeit all privacy. Moreover, the case for privacy is arguably stronger in the context of modern AI use (as contrasted with email use or cell site location). Unlike a general-purpose search engine, which passively returns results, many modern AI platforms are specifically designed and trained to engage. They invite candid and significant disclosure of information, including sensitive information. They simulate empathy, foster trust, and interact in a way that feels genuine and intimate.^[1] Research confirms that people share personal and sensitive information with AI chatbots, often without appreciating what happens to that information once shared. See Jennifer King et al., *User Privacy and Large Language Models: An Analysis of Frontier Developers' Privacy Policies*, 8 PROCEEDINGS OF THE AAAI/ACM CONFERENCE ON AI, ETHICS, AND SOCIETY 1465 (2025) (noting that the conversational nature of AI chatbots encourages greater disclosure of personal information than traditional search interfaces); see also Molly G. Smith, Thomas N. Bradbury & Benjamin R. Karney, *Can Generative AI Chatbots Emulate Human Connection? A Relationship Science Perspective*, 20 PERSPECTIVES ON PSYCHOLOGICAL SCIENCE 1081 (2025).

Moreover, and in the context of a *pro se* litigant's use of AI to assist with their litigation preparation, the use of AI closely resembles the kind of confidential, strategy-laden iterative work product that Rule

26(b)(3) was designed to protect. In other words, given how AI tools function, it is entirely reasonable for a person to expect some privacy and confidentiality when interacting with these tools, even though they understand a third party is behind the tool collecting and storing their information.

In any event, work product protections are typically waived by disclosure to an adversary, or in circumstances that substantially increase the likelihood that an adversary will obtain the materials. *United States v. Am. Tel. & Tel. Co.*, 642 F.2d 1285, 1297-1301 (D.C. Cir. 1980); see also Warner, 2026 WL 373043; *In re Qwest Commc'ns Int'l Inc.*, 450 F.3d 1179, 1186 (10th Cir. 2006) (citing *Foster v. Hill*, 188 F.3d 1259, 1272 (10th Cir. 1999) for the proposition that “the work-product doctrine is affected when a disclosure is to an adversary”). In other words, even though AI use technically “discloses” information to a third party, it is highly unlikely the information will fall into the hands of an adversary absent some legal process to compel it. Thus, AI interactions do not automatically compromise work product protections. See *Warner*, 2026 WL 373043, at *4 (finding that even if *pro se* plaintiff's AI-generated information is discoverable, it is subject to work product protection and the protections were not waived because 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.)

In sum, Rule 26(b)(3) applies and offers Plaintiff some level of work product protection in connection with his use of AI. The question is, how far will that protection extend?

B. Scope of Rule 26(b)(3) Protections

Plaintiff seeks to shield from disclosure, not only the outputs from the AI system, but the name of the AI tool he is using.

Some courts have applied the work product doctrine broadly to cover, for example, processes not just outputs. See, e.g., *Sporck v. Peil*, 759 F.2d 312, 315 (3d Cir. 1985) (finding that counsel's selection process and grouping certain documents together out of the thousands produced in litigation was work product entitled to protection under Rule 26(b)(3)). But the Court does not need to delve into that issue here. Even if it is possible that in some contexts disclosing an AI tool can reveal mental impressions or strategy, Plaintiff has not carried his burden to demonstrate that here. See *Martin v. Monfort, Inc.*, 150 F.R.D. 172, 172-73 (D. Colo. 1993) (describing the sequential step approach to resolving work product issues, and noting that once the party seeking discovery establishes relevance, the burden shifts to the resisting party to show the materials are protected work product); *Pouncil v. Branch L. Firm*, 277 F.R.D. 642, 653 (D. Kan. 2011) (noting that the proponent of a work product protection had the burden of establishing that certain calendars, appointment books, and event logs contain information that constitutes protected mental impressions). At best, Plaintiff states, in conclusory fashion and without any legal or factual support, that “[t]he selection and use of specific litigation support tools reveal a party's mental impressions, case strategy, and legal resource allocation.” (Doc. No. 58 at 2; see also Doc. No. 58-1 (offering similar conclusory statements).) But the Court cannot discern from that, or any other information Plaintiff provides, how disclosing the name of an AI tool would reveal Plaintiff's mental impressions or case strategy. Moreover, Defendant's request for the name of the tool is legitimate and reasonable. If Plaintiff already submitted Confidential Information to some AI system—and it appears he has—Defendant is entitled to know which system.

II. To what extent should a protective order restrict AI use?

*6 The current Protective Order arguably covers the use of AI already,^[2] but the parties appear to agree that a clarifying amendment is necessary.

Defendant asks the Court to add the following language to the Protective Order:

*Restrictions on Use of AI to process Confidential or Highly Confidential Information:
Absent notice to and written permission from the producing party, any person or entity
authorized to have access to Confidential Information under the terms of this Order:*

*a. shall not use or employ any application, service, or analytical software that will
transfer, transmit, send or allow access to Confidential Information, in whole or in part –
including metadata, unless such application, service or analytical software:*

*i. does not further transfer the Confidential Information to another provider,
unless the receiving party has confirmed through due diligence that the security
and privacy controls of and contractual obligations for such provider allow that
party to comply with its obligations under this Protective Order; and*

*ii. provides the receiving party the ability to remove or delete from the system all
Confidential information.*

*b. shall not permit any Confidential Information to be used to train any artificial
intelligence tool. These restrictions apply to the use of advanced or generative AI tools
from OpenAI's GPT or ChatGPT, Harvey.AI, Google's Bard, Anthropic's Claude, and similar
tools or applications.*

(Doc. No. 52 at 2-3.) Plaintiff says Defendant's proposed language is “overly broad, technologically vague, and improperly attempt[s] to dictate the specific litigation strategies and work-product tools utilized by a pro se litigant.” (Doc. No. 58 at 1-2.) Plaintiff also argues that “Defendant's language fails to account for the capabilities of professional-grade, closed-circuit platforms that already ensure strict data isolation and prohibit machine learning training on user data.” (*Id.*) Plaintiff proposes the following language instead:

*Any party utilizing third-party software, cloud-based platforms, or artificial intelligence
tools for the storage, processing, review, or analysis of Confidential Information must
ensure that such tools operate within a secure, closed-circuit environment. No
Confidential Information may be uploaded to any platform or service whose Terms of
Service permit the provider to utilize the uploaded data for the training of Large
Language Models (LLMs), machine learning algorithms, or for any internal human-in-
the-loop review.*

(Doc. No. 58 at 5.) Defendant says Plaintiff's proposed language does not offer sufficient safeguards.

(Doc. No. 60 at 3.) Defendant also advocates for its own proposal because it is “narrowly-tailored.” (*Id.*)

Upon careful consideration of the issues and close review of the competing provisions, the Court finds it appropriate to amend the Protective Order with a provision similar to Defendant's proposed provision, but tailored to the practical realities of this litigation and the current dispute.

*7 Defendant is correct that Plaintiff's proposal does not offer sufficient guardrails. It allows Confidential Information to be uploaded into an AI system so long as it operates in "a secure, closed-circuit environment," which seems to address cybersecurity concerns about unauthorized access rather than the distinct risks associated with today's widely available AI platforms. (See *generally* Doc. No. 58-1.) Moreover, to the extent Plaintiff's proposal *does* address the unique risks associated with AI, it does so in a very limited and vague way, prohibiting the uploading of Confidential Information only when the provider's terms of service "permit the provider to utilize the uploaded data for the training of Large Language Models (LLMs), machine learning algorithms, or for any internal human-in-the-loop review." (Doc. No. 58 at 5.)

Defendant's proposed language is better, but not without its shortcomings. It is, as Defendant says, narrowly-tailored, but not in the way Defendant touts. Defendant's proposed language appears crafted to fit the precise bounds of Defendant's contractual engagement with AI providers, resulting in an over-engineered provision that feels vague to Plaintiff. (See Doc. No. 58 at 1 (saying the provision is broad, vague, and an attempt to dictate his strategies and tools).)[3]

Thus, instead of adopting the parties' proposals, the Court will amend the Protective Order to include the following AI-specific language:

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 recognizes that practically speaking, and in light of the current state of AI, this provision will (at least for now) bar the parties from using most, if not all, mainstream low-to-no-cost AI to process Confidential Information. This type of restriction disadvantages *pro se* litigants.[4] Enterprise-tier AI accounts that satisfy these requirements may be available only through organizational procurement processes, or at costs that a *pro se* litigant is unlikely to bear.[5] But the Court cannot ignore the real risks associated with mainstream tools that persistently collect and store data and could compromise confidentiality.

To be clear, the Court does not intend to leave *pro se* Plaintiff without the benefits of AI. Modern AI tools may be used in many ways that do not involve uploading Confidential Information, and nothing in this particular Order restricts those uses.^[6] What this Order requires is that Confidential Information not be entrusted to platforms that lack the contractual safeguards described above, regardless of the sophistication or apparent trustworthiness of the tool.

CONCLUSION

*8 For these reasons, the Court **GRANTS Defendant's Motion in part, and DENIES it in part** as follows:

- (1) The Court will enter an amended protective order reflecting the AI-specific provision set forth in this Order; and
- (2) Plaintiff is **ORDERED** to, within ten (10) days of this Order, disclose the name of any AI platform he used to upload, submit, process, review, analyze, organize, or store any information designated by Defendant as "CONFIDENTIAL" under the Protective Order.
- (3) Defendant is **ORDERED** to, within ten (10) days of Plaintiff's disclosure, file a Notice with this Court indicating whether it intends to seek relief from this Court (and if so, what relief), or whether it has mitigated any potential harm or reached agreement with Plaintiff, such that no relief will be necessary.

Dated this 30th day of March, 2026.

Footnotes

- (1) The Court does not endorse these practices but simply notes them to describe the environment in which AI users operate.
- (2) The current Protective Order broadly prohibits disclosure, not just to a person or entity, but generally and in any fashion, except under specifically enumerated circumstances. (Doc. No. 30.) Thus, "disclosure" in the form of transmission to an AI system with a provider that stores the Confidential Information in their own databases, and/or for their own purposes, may violate the current Protective Order.
- (3) Defendant's proposed provision also references "Google's Bard," which has since been rebranded as Gemini.
- (4) In light of this restriction, the parties are strongly cautioned against the over-designation of Confidential Information.
- (5) This highlights 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?
- (6) Still, the parties must still comply with all applicable rules, litigation obligations, and the presiding judge's practice standards and orders when using AI.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-v-

BRADLEY HEPPNER,

Defendant.

25 Cr. 503 (JSR)

MEMORANDUM

JED S. RAKOFF, U.S.D.J.:

At a pretrial conference in this matter held on February 10, 2026, the Court, after hearing the arguments of counsel, granted from the bench the Government's motion for a ruling that certain written exchanges that defendant Bradley Heppner had with a generative artificial intelligence ("AI") platform were not protected from Government inspection by either the attorney-client privilege or the work product doctrine. See ECF No. 22 ("Gov't Mot."). This Memorandum sets forth the reasons for the Court's ruling.

I. Background and Procedural History

Generative artificial intelligence tools have become increasingly prevalent across various domains of human activity. It has reliably been estimated, for instance, that more than half of United States households have adopted AI in some form. See Bond, Trends - Artificial Intelligence (2025), https://www.bondcap.com/report/pdf/Trends_Artificial_Intelligence.pdf at 59 (accessed February 12, 2026). Only three years after its release, one prominent AI platform is being used by more than 800 million people worldwide every week. Id. at 55. Yet the implications of AI for the law are only beginning to be explored.

Thus, the Court's ruling in this case appears to answer a question of first impression nationwide: whether, when a user communicates with a publicly available AI platform in connection with a pending criminal investigation, are the AI user's communications protected by attorney-client privilege or the work product doctrine?¹ For the reasons that follow, the answer is no.

On October 28, 2025, a grand jury in this District returned an indictment charging Heppner with securities fraud, wire fraud, conspiracy to commit securities fraud and wire fraud, making false statements to auditors, and falsifying corporate records. ECF No. 3. The indictment was unsealed on November 4, 2025, see ECF No. 4, and Heppner was arrested the following day in the Northern District of Texas. On November 10, 2025, Heppner pleaded not guilty before this Court to all the charges against him and was released on bond. See ECF Nos. 16, 18. Trial is set to commence April 6, 2026. See ECF No. 16.

The charges against Heppner arise from his alleged misconduct as an executive of several corporate entities, including the publicly traded company GWG Holdings, Inc. ("GWG"). See generally ECF No. 3. At a high level, the indictment charges that Heppner defrauded GWG's investors out of more than \$150 million by making false representations about, and causing GWG to enter into undisclosed self-serving

¹ The Court is unaware of, and the parties have not identified, any case to date that has presented this issue. Most published decisions involving generative artificial intelligence have had to do with attorneys' misuse of that technology. That set of concerns is plainly not present here.

transactions concerning, two privately held companies that Heppner controlled, Beneficient Company Group, L.P. and Highland Consolidated L.P. See id. ¶¶ 1-3.

In connection with Heppner's arrest on November 4, 2025, agents with the Federal Bureau of Investigation executed a search warrant at Heppner's home and seized numerous documents and electronic devices. See Gov't Mot. at 3; ECF No. 23-1 at 1. Heppner's counsel later represented to the Government that among the seized materials were approximately thirty-one documents that memorialize communications that Heppner had with the generative AI platform "Claude," which is operated by the private company Anthropic. See Gov't Mot. at 3; ECF Nos. 23-1 23-2. According to Heppner's counsel, the documents represent communications between Heppner and Claude that took place "in 2025, after Mr. Heppner had received a grand jury subpoena [and] after it was clear with discussions with the government that Mr. Heppner was the target of this investigation." Transcript, February 10, 2026 ("Tr.") at 4. Without any suggestion from counsel that he do so, Heppner "prepared reports that outlined defense strategy, that outlined what he might argue with respect to the facts and the law that we anticipated that the government might be charging." Id. Thus, counsel asserted, Heppner "was preparing these reports in anticipation of a potential indictment." Id.

In exchanges with the Government, Heppner, through his counsel, asserted privilege over these documents (the "AI Documents"), arguing that (1) Heppner had inputted into Claude, among other things,

information that Heppner had learned from counsel; (2) Heppner had created the AI Documents for the purpose of speaking with counsel to obtain legal advice; and (3) Heppner had subsequently shared the contents of the AI Documents with counsel. See Gov't Mot. at 3-4, 11; ECF Nos. 23-2, 23-4, 23-5. Heppner's counsel conceded, however, that counsel "did not direct [Heppner] to run Claude searches." ECF No. 23-5. Pursuant to a "Privilege Protocol Stipulation," the Government and Heppner's counsel agreed that the Government would segregate the AI Documents and not inspect them pending the resolution of Heppner's claims of privilege, and Heppner's counsel listed the AI Documents in Heppner's privilege log. See Gov't Mot. at 3-4 & n.1; ECF Nos. 23-1, 23-2.

On February 6, 2026, the Government moved, in writing, for a ruling that the AI Documents are protected by neither the attorney-client privilege nor the work product doctrine. Gov't Mot. The Court heard oral argument on the Government's motion at the pretrial conference held on February 10, 2026, and, as noted, orally granted the motion.

II. Attorney-Client Privilege

It is well established that the attorney-client privilege attaches to, and protects from disclosure, "communications (1) between a client and his or her attorney (2) that are intended to be, and in fact were, kept confidential (3) for the purpose of obtaining or providing legal advice." United States v. Mejia, 655 F.3d 126, 132 (2d

Cir. 2011).² Courts construe the attorney-client privilege narrowly because it operates as an exception to the rule that “all relevant proof is essential” for a complete record and for “confidence in the fair administration of justice.” In re Six Grand Jury Witnesses, 979 F.2d 939, 943 (2d Cir. 1992). See also, e.g., Calvin Klein Trademark Tr. v. Wachner, 198 F.R.D. 53, 55 (S.D.N.Y. 2000).

Applying these principles here, the AI Documents lack at least two, if not all three, elements of the attorney-client privilege. First, the AI Documents are not communications between Heppner and his counsel. Heppner does not, and indeed could not, maintain that Claude is an attorney. “In the absence of an attorney-client relationship, the discussion of legal issues between two non-attorneys is not protected by attorney-client privilege.” E.g., In re OpenAI, Inc., Copyright Infringement Litig., 802 F. Supp. 3d 688, 699 (S.D.N.Y. 2025). Because Claude is not an attorney, see ECF No. 23-6, that alone disposes of Heppner’s claim of privilege.

The Court is aware that some commentators have argued that whether Claude is an attorney is irrelevant because a user’s AI inputs, rather than being communications, are more akin to the use of other Internet-based software, such as cloud-based word processing applications. But the use of such applications is not intrinsically privileged in any case, and the argument that Claude is like any other form of software

² Except where otherwise indicated, all quotations in this Memorandum omit citations, quotation marks, footnotes, brackets, ellipses, and other alterations in source material.

only cuts against the invocation of privilege because all “[r]ecognized privileges” require, among other things, “a trusting human relationship,” such as, in the attorney-client context, a relationship “with a licensed professional who owes fiduciary duties and is subject to discipline.” See Ira P. Robbins, Against an AI Privilege, JOLT Dig., Harvard L. Sch. (Nov. 7, 2025), <https://jolt.law.harvard.edu/digest/against-an-ai-privilege>. No such relationship exists, or could exist, between an AI user and a platform such as Claude.

Second, the communications memorialized in the AI Documents were not confidential. This is not merely because Heppner communicated with a third-party AI platform but also because the written privacy policy to which users of Claude consent provides that Anthropic collects data on both users’ “inputs” and Claude’s “outputs,” that it uses such data to “train” Claude, and that Anthropic reserves the right to disclose such data to a host of “third parties,” including “governmental regulatory authorities.” See Anthropic, Privacy Policy (as of February 19, 2025), <https://www.anthropic.com/legal/archive/a2eecf43-807a-4a53-89dd-04c44c351138>. The policy clearly puts Claude’s users on notice that Anthropic, even in the absence of a subpoena compelling it to do so, may “disclose personal data to third parties in connection with claims, disputes[,] or litigation.” Id. More generally, as another court in this District recently observed, AI users do not have substantial privacy interests in their “conversations with [another publicly accessible AI platform] which users voluntarily disclosed” to the platform and which the platform “retains in the normal course

of its business.” In re OpenAI, Inc., Copyright Infringement Litig., No. 25 MD 3143, ECF No. 1021 at 3 (Jan. 5, 2026). For these reasons, Heppner could have had no “reasonable expectation of confidentiality in his communications” with Claude. See Mejia, 655 F.3d at 132-34. And the AI Documents are not like confidential notes that a client prepares with the intent of sharing them with an attorney because Heppner first shared the equivalent of his notes with a third-party, Claude. Cf. United States v. DeFonte, 441 F.3d 92, 95-96 (2d Cir. 2006) (per curiam).

Third, Heppner did not communicate with Claude for the purpose of obtaining legal advice. This issue perhaps presents a closer call because Heppner’s counsel asserts that Heppner communicated with Claude for the “express purpose of talking to counsel.” ECF No. 23-5. But, as Heppner’s counsel also conceded, Heppner did not do so at the suggestion or direction of counsel. See id. (noting that counsel “did not direct [Heppner] to run Claude searches”). Had counsel directed Heppner to use Claude, Claude might arguably be said to have functioned in a manner akin to a highly trained professional who may act as a lawyer’s agent within the protection of the attorney-client privilege. Cf. United States v. Adlman, 68 F.3d 1495, 1498-99 (2d Cir. 1995) (citing United States v. Kovel, 296 F.2d 918 (2d Cir. 1961)). But because Heppner communicated with Claude of his own volition, what matters for the attorney-client privilege is whether Heppner intended to obtain legal advice from Claude, not whether he later shared Claude’s outputs with counsel. And Claude disclaims providing legal

advice. Indeed, when the Government asked Claude whether it could give legal advice, it responded that "I'm not a lawyer and can't provide formal legal advice or recommendations" and went on to recommend that a user "should consult with a qualified attorney who can properly assess your specific circumstances." ECF No. 23-6 at 1-2.

Thus, the communications between Heppner and Claude were not privileged at the time they took place.³ Moreover, even assuming that Heppner intended to share these communications with his counsel and eventually did so, it is black-letter law that non-privileged communications are not somehow alchemically changed into privileged ones upon being shared with counsel. Thus, because the AI Documents "would not be privileged if they remained in [Heppner's] hands," they did not "acquire protection merely because they were transferred" to counsel. See Gould, Inc. v. Mitsui Min. & Smelting Co., Ltd., 825 F.2d 676, 679-80 (2d Cir. 1987).

III. Work Product Doctrine

Related to but distinct from the attorney-client privilege, the work product doctrine, "[a]t its core[,] . . . shelters the mental processes of the attorney, providing a privileged area within which

³ At oral argument, Heppner's counsel suggested in passing that the AI Documents may be privileged because they "incorporated information that we had conveyed to Mr. Heppner over the course of our representation." Tr. at 3. But even if certain information that Heppner input into Claude was privileged, he waived the privilege by sharing that information with Claude and Anthropic, just as if he had shared it with any other third party. Further, in light of Anthropic's privacy policy discussed above, Heppner had no reasonable expectation that the inputs would not be shared with other third parties.

he can analyze and prepare his client's case." United States v. Nobles, 422 U.S. 225, 238 (1975). The doctrine "provides qualified protection for materials prepared by or at the behest of counsel in anticipation of litigation or for trial." In re Grand Jury Subpoenas Dated March 19, 2002, and August 2, 2002, 318 F.3d 379, 383 (2d Cir. 2003). As with the attorney-client privilege, the work product doctrine is not "lightly created nor expansively construed," id. (quoting United States v. Nixon, 418 U.S. 683, 710 (1974)), and the Second Circuit has repeatedly held that the doctrine's purpose "is not generally promoted by shielding from discovery materials in an attorney's possession that were prepared neither by the attorney nor his agents," id. (citing Matter of Grand Jury Subpoenas Dated Oct. 22, 1991, and Nov. 1, 1991, 959 F.2d 1158 (2d Cir. 1992)). The doctrine's availability in reference to materials in the possession of a client "depends upon the existence of a real, rather than speculative, concern that the thought processes of [the client's] counsel in relation to pending or anticipated litigation would be exposed." Matter of Grand Jury Subpoenas, 959 F.2d at 1167 (quoting Gould, 825 F.2d at 680).

The AI Documents do not merit protection under the work product doctrine because, even assuming, arguendo, that they were prepared "in anticipation of litigation," In re Grand Jury Subpoenas, 318 F.3d at 383, they were nevertheless not "prepared by or at the behest of counsel," id., nor did they reflect defense counsel's strategy, see Matter of Grand Jury Subpoenas, 959 F.2d at 1167. As to the former, Heppner's counsel confirmed that the AI Documents "were prepared by

the defendant on his own volition.” Tr. at 5. That means that Heppner was not acting as his counsel’s agent when he communicated with Claude. As to the latter, counsel conceded that while the AI Documents did “affect” counsel’s strategy going forward, they did not “reflect” counsel’s strategy at the time that Heppner created them. See id.

At oral argument, Heppner resisted these conclusions by relying on two authorities. The first, Federal Rule of Criminal Procedure 16(b)(2)(A), is inapplicable on its face. That rule provides that, where the Government provides a defendant with pretrial discovery and the defendant thereby becomes obligated to satisfy the Government’s pretrial discovery requests, the defendant’s obligation does not extend to “discovery or inspection of reports, memoranda, or other documents made by the defendant, or the defendant’s attorney or agent, during the case’s investigation or defense.” Id. Here, however, the AI Documents were seized from Heppner, at the time of his arrest, pursuant to a search warrant the validity of which Heppner’s counsel does not challenge. See Gov’t Mot. at 3. The Government did not request them, and Heppner did not produce them, in pretrial discovery.

Heppner’s second authority is Shih v. Petal Card, Inc., 565 F. Supp. 3d 557 (S.D.N.Y. 2021). In that case, a Magistrate Judge in this District authorized the plaintiff to withhold certain communications that she had with an individual who was then her lawyer, and later became her husband, that the plaintiff prepared in anticipation of litigation or for trial. The court held that the work product doctrine protected such communications, “regardless of whether [the

lawyer/husband] was acting as her counsel at the time, and without showing that another attorney 'directed the work.'" Id. at 574.

Shih, of course, is not binding on this Court, and this Court respectfully disagrees with its holding. As relevant here, the court in Shih principally concluded that the work product doctrine is not limited to materials prepared by or at the direction of an attorney. Id. But that conclusion undermines the policy animating the work product doctrine, which, as one of the cases cited in Shih explains, is "to preserve a zone of privacy in which a lawyer can prepare and develop legal theories and strategy 'with an eye toward litigation.'" Parneros v. Barnes & Noble, Inc., 332 F.R.D. 482, 492 (S.D.N.Y. 2019) (quoting United States v. Adlman, 134 F.3d 1194, 1996 (2d Cir. 1998) (quoting, in turn, Hickman v. Taylor, 329 U.S. 495, 510-11 (1947))); see Shih, 565 F. Supp. 3d at 574 (citing Parneros). While it is true that the work product doctrine may apply to materials generated by non-lawyers, the Second Circuit has repeatedly stressed that the purpose of the doctrine is to protect lawyers' mental processes. See, e.g., In re Grand Jury Subpoenas, 318 F.3d at 383-85 (extensively describing doctrine's rationale and applying it to material "prepared by or for counsel"); Adlman, 134 F.3d at 1197 (similar); Adlman, 68 F.3d at 1500-02 (similar); Matter of Grand Jury Subpoenas, 959 F.2d at 1166 (doctrine "generally does not shield from discovery documents that were not prepared by the attorneys themselves, or their agents"); see also Bice v. Robb, 511 F. App'x 108, 110 (2d Cir. 2013) (summary

order) (declining to extend protection to documents “not the work product of an individual acting as [plaintiffs’] attorney”).

Here, there is no dispute that Heppner acted on his own when he created the AI Documents. See ECF No. 23-5 (noting that defense counsel “did not direct [Heppner] to run Claude searches”); Tr. at 5 (confirming same). Because the AI Documents were not prepared at the behest of counsel and did not disclose counsel’s strategy, they do not merit protection as work product.

IV. Conclusion

Generative artificial intelligence presents a new frontier in the ongoing dialogue between technology and the law. Time will tell whether, as in the case of other technological advances, generative artificial intelligence will fulfill its promise to revolutionize the way we process information. But AI’s novelty does not mean that its use is not subject to longstanding legal principles, such as those governing the attorney-client privilege and the work product doctrine. Because Heppner’s use of Claude fails to satisfy either of these rules, the AI Documents do not merit the protections Heppner has claimed.

New York, NY
February 17, 2026


JED S. RAKOFF, U.S.D.J.

AI Vendor Risk Assessment Checklist for Law Firms

1. Vendor Profile

- ☐ Legal industry experience
- ☐ Law firm references
- ☐ Financial stability
- ☐ Clear product roadmap

2. AI Technology

- ☐ Type of AI clearly explained
- ☐ Training data sources disclosed
- ☐ Accuracy tested and validated
- ☐ Human-in-the-loop controls available

3. Data Security & Privacy

- ☐ No client data used for training by default
- ☐ Encryption at rest and in transit
- ☐ Data residency disclosed
- ☐ Clear breach notification process

4. Ethical & Professional Responsibility

- ☐ Supports lawyer supervision
- ☐ No unauthorized practice of law risk

- ☐ Bias mitigation addressed
- ☐ Transparency options available

5. Regulatory & Compliance

- ☐ Compliance with applicable data laws
- ☐ Audit logs and traceability
- ☐ Regulatory readiness demonstrated

6. Contractual Protections

- ☐ Firm retains data ownership
- ☐ IP rights in outputs clarified
- ☐ Adequate indemnification
- ☐ Reasonable liability caps
- ☐ Exit and data return provisions

7. Governance & Oversight

- ☐ Internal approval process defined
- ☐ Usage policies documented
- ☐ Training provided
- ☐ Ongoing review scheduled

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

SOHYON WARNER,

Plaintiff,

Case No. 2:24-cv-12333

v.

District Judge Gershwin A. Drain
Magistrate Judge Anthony P. Patti

GILBARCO, INC., GILBARCO, INC.
(d/b/a GILBARCO VEEDER-ROOT), and
VONTIER CORPORATION,

Defendants.

_____/

**ORDER DENYING PLAINTIFF’S MOTION FOR SANCTIONS BASED ON
NON-COMPLIANCE WITH A COURT ORDER (ECF No. 68), GRANTING
IN PART, DENYING IN PART, AND DEEMING WITHDRAWN IN PART
DEFENDANTS’ MOTION TO COMPEL (ECF No. 80), and STRIKING
THE NON-JOINT STATEMENT (ECF No. 89)**

A. Pending Matters

On August 28, 2025, the Court entered an amended scheduling order, which set the fact discovery deadline for December 5, 2025. (ECF No. 41.) To date, the Undersigned has handled several discovery-related motions (*see, e.g.*, ECF No. 45, 47, 48, 49, 50) via orders dated September 26, 2025 (ECF No. 56) and October 30, 2025 (ECF No. 66).

Currently pending before the Court are: (1) Plaintiff’s November 10, 2025 notice of Defendants’ non-compliance with the Court’s October 30, 2025 order and request for sanctions under Fed. R. Civ. P. 37 (ECF No. 68), as to which

Defendants filed a response (ECF No. 73), and Plaintiff filed a reply (ECF No. 77); and, (2) Defendants' December 23, 2025 motion to compel and request for sanctions (ECF No. 80), as to which Plaintiff has filed a response (ECF No. 86) and Defendants have filed a reply (ECF No. 87). Additionally, the parties have filed statements of resolved and unresolved issues. (*See* ECF Nos. 89, 90.)¹

Judge Drain has referred each of these motions to me for hearing and determination (ECF No. 69, 81). The Undersigned conducted a video status conference on January 12, 2026. (ECF Nos. 85, 93.) Pursuant to the Court's January 13, 2026 notice, Plaintiff, on her own behalf, and defense counsel (Attorney Richard W. Warren) appeared on February 5, 2026 in person for a hearing on these motions. (ECF Nos. 82, 88.)

B. Order

1. Plaintiff's motion (ECF No. 68) is DENIED.

Upon consideration of the motion papers and the parties' arguments and representations at the hearing, and for all the reasons stated on the record by the

¹ Plaintiff's "notice" (ECF No. 68) has been treated as a motion. The usual path to gaining relief from the Court is to file a motion, and notices are generally not permitted unless previously requested by the Court (*e.g.*, ECF No. 51); more often than not, they are stricken. Plaintiff is cautioned about filing notices going forward, as she has, on more than one occasion, filed unauthorized "notices" on the docket. (*See, e.g.*, ECF No. 58, 68.) Also, Plaintiff's emergency supplement (ECF No. 72) was stricken pursuant to the Court's November 26, 2025 text-only order. Finally, at the February 5, 2026 motion hearing, the Court struck the non-joint statement (ECF No. 89) from the record.

Court, which are hereby incorporated by reference as though fully restated herein, Plaintiff's motion (ECF No. 68) is **DENIED** as set forth in the prayer for relief (*see* ECF No. 68, PageID.662-663 ¶¶ 1-6.):

- To the extent Plaintiff asked the Court to “[f]ind Defendants in non-compliance with ECF 66 and the Federal Rules of Civil Procedure[,]” the motion is **DENIED**. *Inter alia*, the Court agrees that Defendants complied with the direction regarding Bates ranges 162-462 (*see* ECF No. 66, PageID.630 ¶ 4), when it submitted its November 7, 2025 supplemental response (*see* ECF No. 73, PageID.735; ECF No. 73-1). To the extent that Defendants provided additional information after Court-ordered deadlines, the Court is satisfied that it did so in compliance with its duty to supplement under Fed. R. Civ. P. 26(e).

- To the extent Plaintiff asks Defendants to “[o]rder immediate, complete production of all comparator files, HR investigations, and ESI—requiring Defendants to re-run all searches using the expanded custodian and term list provided on October 27, 2025, and to re-produce the results in an organized, labeled format consistent with Rule 34(b)(2)(E)[,],” the motion is **DENIED**. Defense counsel, as an officer of the Court, provided answers to the Court’s extensive questioning on this subject, and the Court is satisfied that Defendants have produced the comparator files (*see* ECF No. 68, PageID.651-653) within their

“possession, custody, or control[,]” Fed. R. Civ. P. 34(a)(1); thus, there is nothing for the Court to order. The two investigation reports listed in the privilege log will be addressed below.

Although not spelled out in her prayer for relief, Plaintiff complains that Defendants’ production of Bates range 463-4427 on October 27, 2025 and November 7, 2025 did not comply with the Court’s October 30, 2025 order (ECF No. 66). (ECF No. 68, PageID.656-658). However, Defendants’ November 7, 2025 supplemental response reads: “Not long before Plaintiff’s counsel withdrew their representation, Defendants agreed to run an ESI search with specific search parameters—date range: December 1, 2021 to December 31, 2023—custodians: Ivan Ayma, Emily Heuser, Rosanna Hurst and Robert Steffler—and the search terms below[,]” below which appears a list of search terms. (ECF No. 73-1, PageID.754.) Immediately below the chart of search terms, Defendants state: “As a result of this search, see documents at Bates Nos. G000463-1378 and G001379-4427.” (ECF No. 73-1, PageID.754 [No. 16].) The Court finds that this suffices and complies with its prior order.

- To the extent Plaintiff asked the Court to “[r]equire Defendants to serve an updated, itemized privilege log identifying each withheld document with

sufficient detail to assess the claim of privilege, and to produce all non-privileged portions of the HR investigations[.]” the motion is **DENIED**. Instead, the Court performed Plaintiff’s suggested *in camera* review. Having considered the two investigation reports listed on Defendants’ November 21, 2025 privilege log (ECF No. 73-3), one by compliance counsel Kathy Martorell dated March 3, 2023 (*see* ECF No. 73-6) and the other by compliance investigator Kate S. Gibson dated December 14, 2022 (*see* ECF No. 73-4), along with the declarations filed in support of privileges with respect to those two documents, one by Kate Gibson, Esq. (ECF No. 73-5) and the other by Kathy Hunt, Esq. (ECF No. 73-7), the Court concludes these investigations and the reports they generated were done in anticipation of litigation, both subjectively and objectively, as opposed to the ordinary course of business. *See, e.g., Upjohn Co. v. United States*, 449 U.S. 383, 386 (1981); *Lee v. EUSA Pharma US LLC*, No. 2:22-CV-11145, 2024 WL 250064 (E.D. Mich. Jan. 23, 2024) (Patti, M.J.) (order after *in camera* review); *United States v. Nobles*, 422 U.S. 225, 238–39 (1975) (“the doctrine protect[s] material prepared by agents for the attorney as well as those prepared by the attorney himself.”). Because these documents are protected by both the attorney-client privilege and the work product doctrine, the Court will not order their production. Although Plaintiff argued that any factual accounts given in those reports should be produced, the Court extensively questioned defense counsel at the hearing and

is satisfied that no witnesses interviewed by in-house counsel gave written, recorded, sworn, or transcribed verbatim statements. As this Court has noted, “even attorney interview notes of fact witnesses (if any exist), which are inevitably funneled through the attorney-interviewers’ ears, minds, fingers and/or voices (if dictated), are also protected as work product and, thus, not discoverable.” *Lee*, 2024 WL 250064, at *4. *See In re General Motors LLC Ignition Switch Lit.*, 80 F.Supp.3d 521, 532 (S.D.N.Y. 2015) (“[i]nterview notes and memoranda produced in the course of ... internal investigations have long been considered classic attorney work product.”) As the Supreme Court has explained: “Forcing an attorney to disclose notes and memoranda of witnesses’ oral statements is particularly disfavored because it tends to reveal the attorney’s mental processes” *Upjohn*, 449 U.S. at 399 (citation omitted). *See also United States v. One Tract of Real Prop. Together With all Bldgs., Improvements, Appurtenances & Fixtures*, 95 F.3d 422, 427 (6th Cir. 1996); 6 *Moore’s Federal Practice* § 26.70[2][a] (Matthew Bender 3d ed.) (“Thus, while the facts themselves are not privileged, a chart or other compilation of facts may be protected as work product.”).² The Court confirmed that Plaintiff was provided with all of the names of the people

² This is in contrast with *government* documents protected by the *deliberative process privilege*, where factual summaries may be discoverable because they are not “deliberative.” *See EEOC v. Peoplemark, Inc.*, No. 1:08-cv-907, 2010 WL 748250, at *2 (W.D. Mich. Feb. 26, 2010).

interviewed by in-house counsel in the internal investigation, and, though she had the opportunity to depose them to obtain whatever factual information they had, she did not.

- To the extent Plaintiff asked the Court to “[i]mpose sanctions under [Fed. R. Civ. P. 37(b) and Fed. R. Civ. P. 26(g)] . . . [,]” such as assessing expenses and fees, deeming facts established, imposing an adverse inference / spoliation, imposing an evidentiary preclusion, deeming a privilege waived, or providing a warning of further sanctions, the motion is **DENIED**;

- To the extent Plaintiff asked the Court to “[d]irect Defendants to certify, under oath, the preservation and completeness of all ESI and hard-copy materials associated with departed custodians (Schoultz, Hurst, Blaser, McClellan, Posada, Heuser, and Martorell) and to describe their data-retention measures in writing[,]” the motion is **DENIED**, as that certification was given on the record in open court; and,

- To the extent Plaintiff sought an extension of the discovery period “to ensure Plaintiff receives a meaningful opportunity to review all compelled productions, conduct follow-up discovery, and complete depositions after

compliance is achieved[,]” the motion is **DENIED**. For example, although Plaintiff claims to have requested depositions of Human Resources (HR) in September 2025, she never took a deposition, purportedly because she did not have related documents. She also never sought to compel that deposition at any time, let alone within the discovery period. Nonetheless, defense counsel confirmed that Plaintiff was given a list of those witnesses interviewed in the investigation, and, as the Court explained from the bench, although documents may be beneficial in deposing a witness, they are not absolutely necessary; indeed, a deposition may sometimes be used to *identify* documents to be sought in discovery, the revelation of which may occasionally become the basis for continuing a deposition. If Plaintiff was concerned about the completeness of personnel records produced to her, she was free to explore the contents that she had been given and whether other material exists or should have been included in document productions by deposing the HR director or some other appropriate custodian. She did not avail herself of this opportunity.

Given the Court’s denial of Plaintiff’s motion, the Court has considered whether to require Plaintiff to pay Defendants their “reasonable expenses incurred in opposing the motion, including attorney’s fees[,]” but the Court declines to do so, finding “the motion was substantially justified or other circumstances make an

award of expenses unjust[,]" Fed. R. Civ. P. 37(a)(5), particularly the need for the Court to engage in its *in camera* review. Plaintiff can hardly be faulted for making that request under these circumstances.

2. Defendants' motion (ECF No. 80) is GRANTED IN PART, DENIED IN PART, and DEEMED WITHDRAWN IN PART.

Upon consideration of the motion papers and the parties' arguments and representations at the hearing, and for all the reasons stated on the record by the Court, which are hereby incorporated by reference as though fully restated herein, Defendants' motion (ECF No. 80) is **GRANTED IN PART, DENIED IN PART, and DEEMED WITHDRAWN IN PART**. Preliminarily, the initial and amended scheduling orders provide: "Discovery shall be completed on or before the date set forth in the scheduling order. The court will not order discovery to take place subsequent to the discovery cutoff date." (ECF No. 14, PageID.81; ECF No. 41, PageID.257 (emphasis in original).) Judge Drain's and the Undersigned's Practice Guidelines contain similar provisions. (See www.mied.uscourts.gov.) Plaintiff served her responses to Defendants' second request to produce on October 23, 2025 (ECF No. 80-4), she was deposed on November 25, 2025, and the discovery deadline in this case was extended to December 5, 2025 (ECF No. 41, PageID.257.) Defendants have made no showing that it was impossible or impractical to have filed the December 23, 2025 motion before the close of discovery, nor did Defendants file a motion to extend discovery or otherwise

demonstrate good cause for filing their motion outside of the discovery period. Therefore, the motion is **DENIED AS UNTIMELY**, except as specified below. *See Santifer v. Inergy Auto Sys., LLC*, No. 5:15-cv-11486, 2016 WL 4011268, at *2 (E.D. Mich. Jul. 27, 2016) (E.D. Mich. July 27, 2016) (requiring good cause for bringing a motion to compel after the close of discovery). Alternatively, as set forth in the prayer for relief:

- To the extent Defendants seek production of “all documents and information concerning her use of third-party AI tools in connection with this lawsuit, as requested in Defendants’ discovery requests,” this request is **DENIED**, as the information sought is not discoverable. *See* Fed. R. Civ. P. 26(b)(3)(A) (“Ordinarily, a party may not *discover* documents and tangible things that are prepared in anticipation of litigation or for trial by another *party* or its representative”) (emphases added). Moreover, it is not relevant, or, even if marginally relevant, is not proportional. *See* Fed. R. Civ. P. 26(b)(1).³

³ Notably, the Court previously confirmed that Defendants have no evidence of Plaintiff having violated the protective order by uploading documents marked confidential onto an AI platform. (ECF No. 93, PageID.1002.) The Court also reviewed pertinent and highlighted portions of Plaintiff’s deposition transcript (ECF No. 80-2), which reveals an inordinate amount of questioning about Plaintiff’s use of AI, but again, no suggestion that she uploaded prohibited items. Defendants’ preoccupation with Plaintiff’s use of AI needs to abate.

- To the extent Defendants ask the Court to “[o]verrule[] Plaintiff’s attorney–client privilege and work-product objections to the AI materials,” or alternatively, “if the Court sustains any privilege or protection as to any item, require Plaintiff, within seven days, to serve a Rule 26(b)(5)(A)-compliant privilege log[,]” the request is **DENIED**. Even if this information were discoverable, it is subject to protection under the work-product doctrine, which Plaintiff is permitted to assert. *See, e.g., Systemes v. Childress*, No. 09-10534, 2013 WL 12181774 (E.D. Mich. Nov. 22, 2013) (Hluchaniuk, M.J.) (order granting in part and denying in part motion to quash subpoenas); *Anderson v. Furst*, No. 2:17-12676, 2019 WL 2284731, *4 (E.D. Mich. May 29, 2019) (Patti, M.J.) (“Plaintiff, as a *pro se* litigant, has a right to assert work product protection over such material.”); *see also* Fed. R. Civ. P. 26(b)(3). Moreover, to the extent Defendants argue that Plaintiff waived the work-product protection by using ChatGPT, the work-product waiver has to be a waiver *to an adversary* or in a way likely to get in an adversary’s hand. *In re Columbia/HCA Healthcare Corp. Billing Pracs. Litig.*, 293 F.3d 289, 306 n.28 (6th Cir. 2002) (explaining differences in waiver of attorney-client privilege and work product protection); *Schanfield v. Sojitz Corp. of Am.*, 258 F.R.D. 211, 214 (S.D.N.Y. 2009) (“It is well-established that voluntary disclosure of confidential material to a third party waives any applicable attorney-client privilege.”). *See also United States v. Am.*

Tel. & Tel. Co., 642 F.2d 1285, 1299 (D.C. Cir. 1980) (“while the mere showing of a voluntary disclosure to a third person will generally suffice to show waiver of the attorney-client privilege, it should not suffice in itself for waiver of the work product privilege.”). And ChatGPT (and other generative AI programs) are *tools*, *not persons*, even if they may have administrators somewhere in the background. As Plaintiff noted in her response, Defendants’ motion “asks the Court to compel Plaintiff’s internal analysis and mental impressions—*i.e.*, her thought process—rather than any existing document or evidence, which is not discoverable as a matter of law. The motion seeks intrusive post-discovery production based on speculation about what might exist in Plaintiff’s internal drafting process, untethered from Rule 26 relevance, disregarding the heightened protection afforded to opinion work product, and improperly attempting to manufacture a waiver where none exists. At its core, Defendants’ request is a fishing expedition. . . .” (ECF No. 86, PageID.917.) Additionally, the Court agrees with Plaintiff that the pursuit of this information is “a distraction from the merits of this case[,]” and that Defendants’ theory, which is supported by no case law but only a Law360 article posing rhetorical questions,⁴ “would nullify work-product protection in

⁴ See ECF No.80, PageID.825-826. But as Plaintiff points out, “no cited case orders the production of what Defendants seek here: a litigant’s internal mental impressions reformatted through software.” (ECF No. 86, PageID.933.)

nearly every modern drafting environment, a result no court has endorsed.” (*Id.*, PageID.920, 930.)

- To the extent Defendants ask the Court to compel Plaintiff “to execute HIPAA-compliant medical authorizations for the medical and mental-health providers Plaintiff identified in her deposition[,]” this request is **GRANTED**. Notwithstanding the untimeliness of this motion, pursuant to the Court’s broad authority under Fed. R. Civ. P. 1 and Fed. R. Civ. P. 16(a)(2) & (d), Plaintiff is required to produce signed HIPPA releases for Therapists Maria Yoo and Lemica Cox, and Dr. Shazia Kumar (*see* ECF No. 80, PageID.818; ECF No. 80-2, PageID.840 [pp. 23-24]) no later than **Thursday, February 12, 2026**. While Plaintiff claims that her prior attorney obtained these releases from her and would have given them to defense counsel, defense counsel represented that he did not receive them. Even a minimal amount of cooperation on Plaintiff’s part could have avoided this portion of Defendants’ motion to compel.

- To the extent Defendants seek an order requiring Plaintiff “to bear Defendants’ reasonable expenses, including attorneys’ fees, incurred in bringing this Motion, pursuant to Rule 37(a)(5),” the request was **WITHDRAWN** at the hearing.

(ECF No. 49, PageID.810-811.)

In the end, both sides of this dispute seek to obtain each other's thought processes, while shielding their opponent from discovery of their own. The Court will uphold the protections afforded the thought processes and litigation strategies of both sides and will order production of neither.

IT IS SO ORDERED.⁵

Dated: February 10, 2026



Anthony P. Patti
UNITED STATES MAGISTRATE JUDGE

⁵ The attention of the parties is drawn to Fed. R. Civ. P. 72(a), which provides a period of fourteen (14) days after being served with a copy of this order within which to file objections for consideration by the district judge under 28 U.S.C. § 636(b)(1).

CYNTHIA WHITE, Plaintiff,

v.

WALMART, INC., Defendant

No. 1:25-cv-01120-RLY-TAB

United States District Court, S.D. Indiana, Indianapolis Division

April 14, 2026

Counsel

John H. Haskin, John H. Haskin & Associates, LLC, Indianapolis, IN, Mark R. Waterfill, Mark Waterfill Attorney at Law P.C., Plainfield, IN, Matthew Smith, Employment Law Office of John H. Haskin & Assoc LLC, Indianapolis, IN, for Plaintiff.

Cheyne Galloway, Susan M. Zoeller, Ogletree Deakins Nash Smoak & Stewart PC, Indianapolis, IN, for Defendant.

Baker, Tim A., United States Magistrate Judge

DISCOVERY ORDER FOLLOWING APRIL 10, 2026, TELEPHONIC STATUS CONFERENCE

*1 Artificial intelligence can be a useful discovery tool. However, as discussed below, AI is not a substitute for attorneys and litigants exercising independent judgment and oversight in the discovery process. Relatedly, the Court once again reminds counsel of their obligation to meaningfully meet and confer with one another before seeking the Court's involvement in discovery disputes. Exclusive reliance on AI-generated discovery responses does not satisfy this obligation.

I. Background

Plaintiff Cynthia White alleges that Defendant Walmart wrongfully terminated her in retaliation for making a worker's compensation claim. Defendant served Plaintiff interrogatories and requests for production in July 2025. In August 2025, Plaintiff provided discovery responses. However, Defendant maintains that those responses are still incomplete. Plaintiff's original counsel was allowed to withdraw [Filing No. 30], but discovery problems have persisted despite the appearance of new counsel for Plaintiff. Eventually, Defendant proposed a March 23, 2026, conference call to discuss the ongoing discovery shortcomings with Plaintiff's new counsel. Plaintiff's counsel confirmed his availability for the call, but soon thereafter declined the calendar invitation without providing an explanation or proposing an alternative date. Accordingly, Defendant requested a Local Rule 37-1 conference with the Court. The Court conducted that

conference on April 10, 2026, at which time counsel appeared for the parties and the discovery issues were discussed.

Shortly before this conference, Plaintiff's counsel raised his own concerns regarding Defendant's discovery responses. However, a review of Plaintiff's concerns quickly revealed that they are based solely on an AI-generated list of supposed deficiencies. The Court questioned Plaintiff's counsel about this directly at the April 10 conference. Plaintiff's counsel admitted that he simply uploaded Defendant's discovery responses into an AI program, asked AI to identify insufficient responses, and copied and pasted the results to an email that he sent to Defendant's counsel and to the Court.

II. Discussion

Attorneys and litigants must exercise independent judgment and oversight in discovery-related matters, even when using AI tools. Plaintiff's exclusive reliance on AI is improper. "Though the use of AI platforms is not itself problematic, [parties must vet] any factual and legal references generated by AI." *Sheets v. Charlotte Cnty.*, No. 2:24-cv-958-JES-KCD, 2025 WL 1069271, at *2 (M.D. Fla. Apr. 9, 2025). Before an attorney raises a discovery dispute, that attorney must independently consider any discovery deficiencies identified by AI. See *Tijerina v. Spotify USA Inc.*, No. 24-2290, 2025 WL 1866057, at *7 (E.D. La. July 7, 2015) (finding it improper to "outsource [discovery] positions to artificial intelligence.").

Plaintiff's AI-generated list of discovery deficiencies claims that Defendant's answer to every interrogatory is deficient, without any consideration of whether the asserted deficiencies are material or otherwise warrant additional discussion or supplementation. The exercise of human discretion is needed to appropriately narrow the dispute and identify what discovery supplementation may be needed to move the case forward. Plaintiff's counsel has taken a perilous shortcut around his responsibilities as a trained legal professional.

*2 By relying exclusively on AI to identify and discuss potential deficiencies in Defendant's discovery responses, and then merely copying and pasting these results to an email he sent to Defendant's counsel and to the Court, Plaintiff's counsel also has failed to confer in good faith before bringing the alleged deficiencies to the Court's attention. *Tijerina*, 2025 WL 1866057, at *7 (finding Fed. R. Civ. P. 37(a)(1)'s meet and confer requirement unsatisfied where a party relied exclusively on AI-generated talking points during the meet and confer). As this Court has stated many times, before bringing a discovery dispute to the Court's attention, parties must meet and confer in good faith. *S.D. Ind. Local Rule 37-1(a)*; *Loparex, LLC v. MPI Release Techs., LLC*, No. 1:09-cv-1411-JMS-TAB, 2011 WL 1871167, at *2 (S.D. Ind. May 16, 2011) ("An electronic ultimatum is not a good faith attempt to resolve a

discovery dispute. Rather, the local rule contemplates an actual meeting with a date, time, and place—whether by telephonic, videoconference, or (if counsel's location permits) preferably face-to-face.").

Although Plaintiff did not satisfy the meet and confer requirement, Defendant did. Shockingly, Defendant is still awaiting proper responses to discovery served in July 2025. As noted above, after Plaintiff retained new counsel, Defendant proposed a March 23, 2026, conference call to discuss the problems in Plaintiff's discovery responses. Despite confirming his availability for the call, Plaintiff's counsel inexplicably declined Defendant's calendar invitation without providing an explanation or proposing an alternative date. That is when Defendant understandably sought the Court's intervention.

There are obvious deficiencies in Plaintiff's discovery responses. More than eight months have passed since Defendant served discovery on Plaintiff, yet Plaintiff has not even provided signed interrogatory responses. Nor has Plaintiff identified medical providers from whom she sought treatment in connection with her alleged injuries. These are two of the more glaring discovery deficiencies, but Plaintiff's responses raise numerous other concerns. At the April 10 conference, the Court ordered the parties to confer further in good faith regarding these issues and ordered Plaintiff to serve complete discovery responses to Defendant by April 27, 2026. If Defendant believes Plaintiff's responses remain incomplete, Defendant may request another discovery conference with the magistrate judge. If Plaintiff likewise has continued issues with Defendant's discovery responses—and if Plaintiff has fulfilled the meet and confer obligations set forth in this order and in *Loparaex*—Plaintiff may also seek the Court's intervention.

III. Conclusion

As this order reflects, AI is a useful tool, but not a substitute for good lawyering. Nor does exclusive reliance on AI satisfy counsel's obligation to meet and confer in good faith before asking the Court to wade into a discovery dispute. Plaintiff shall supplement her discovery responses by April 27, 2026.

Date: 4/14/2026