2026 WL 2568346
Only the Westlaw citation is currently available.
United States District Court, D. Colorado.

Colin DUNN, Plaintiff,

v.

LEXISNEXIS RISK SOLUTIONS, INC., and Farmers Insurance Exchange, Defendants.

Civil Action No. 26–cv–01249–GPG–MDB
|
Signed August 31, 2026

Attorneys and Law Firms

McKenzie R. Czabaj, Consumer Justice Law Firm PLC, Scottsdale, AZ, for Plaintiff.

Stephen J. Sovinsky, Troutman Pepper Locke LLP, Richmond, VA, for Defendant LexisNexis Risk Solutions, Inc.

Melissa Ann Wiese, Gordon Rees Scully Mansukhani LLP, Denver, CO, Candice S. Nam, Gordon Rees Scully Mansukhani LLP, Los Angeles, CA, for Defendant Farmers Insurance Exchange.

ORDER

Maritza Dominguez Braswell, United States Magistrate Judge

***1** Before the Court is the Second Joint Motion for Entry of Protective Order ([“Motion”], Doc. No. 29). The parties attach a proposed protective order (Doc. No. 29-1) and agree on all provisions except one: the “Additional Disputed Language.” (*See* Doc. No. 29-1 at 12.) After carefully considering the issues, the Court **GRANTS** the Motion but will enter the proposed protective order without the Additional Disputed Language.

BACKGROUND

The parties are engaged in discovery and agree that many of the at-issue documents contain confidential information. (*See* Doc. No. 29 at 1.) They initially filed a motion for a protective order with competing AI provisions. (*See* Doc. No. 24.) The Court set a hearing, and the parties explained their respective positions. (*See* Doc. No. 28.) Seeing that the parties were quite close to agreement and had overlapping goals, the Court offered limited guidance but ordered them to confer once more. (*Id*.) They did, and the process was productive. Through a videoconference and several email exchanges, the parties reached agreement on almost every aspect of their AI provision. (*See generally* Doc. No. 29; *see also* Doc. No. 29-1 at 11.)

The AI provision prohibits the uploading of confidential information to certain AI platforms but permits the use of secure platforms, so long as they limit training and disclosure, and allow deletion. (Doc. No. 29-1 at 11.) The agreed-upon AI provision also identifies the tools the parties intend to use. (*Id*.) Still, the parties could not reach agreement on the Additional Disputed Language: one sentence at the end of the proposed protective order that would require disclosure, consent, and amendment each time a party seeks to use a new AI tool with confidential information. Defendants support this requirement. Plaintiff objects.

ANALYSIS

The Court begins by addressing certain characterizations in the Motion. First, Plaintiff characterizes the remaining dispute as motivated by “the perverse incentive of fighting for the sake of making the other litigant suffer.” (Doc. No. 29 at 3–4.) The Court does not share this view. Knowing how confidential information is handled is a legitimate interest. That the parties disagree on the right mechanism for addressing that interest does not make the concern illegitimate or the incentives perverse.

Second, Plaintiff contends that AI risks “are *identical* to those inherent in using any cloud storage service.” (Doc. No. 29 at 3 (emphasis added).) The Court rejects the notion that the risks are *identical*. There are certainly some similarities across systems, and indeed, in *Morgan v. V2X, Inc.*, this Court highlighted those similarities and concluded that routing information through a modern AI tool is, in some respects, like routing information through email, and a user does not automatically forfeit privacy in either scenario. 2026 WL 864223, at *4 –5 (D. Colo. Mar. 30, 2026). But these similarities do not make the *risks identical*. Cloud storage, email infrastructure, and traditional data management systems operate under more mature frameworks than modern AI. Indeed, modern AI systems are relatively nascent, and

inputs are processed in ways that are not fully transparent. *See generally* International AI Safety Report 2026, *available at* https://internationalaisafetyreport.org. Thus, when it comes to uploading confidential information, AI systems present greater risk due to their opacity and continued evolution. That increased risk changes the calculus when someone else's data is at stake.[1]

***2** When a party uploads their *own* documents and information, they accept the risk (however small) that their own confidential information could become compromised.[2] By contrast, when a party turns over confidential information to another, the producing party cannot manage their risk absent agreement or court order. Given the pace of change in consumer-grade AI, and the limited visibility into how these tools process data, it is reasonable for a party to request that confidential information be kept out of consumer-grade AI tools that do not offer the same assurances and configurations found in certain enterprise offerings. *See generally* T. Christakis, *You Trust Your Chatbot With Everything. Should You? Part 1: How The Controller Uses Your Chat Data, AI Regulation Papers*, 26-03-2, AI-Regulation.com, March 2026, *available at* https://ai-regulation.com/you-trust-your-chatbot-with-everything-should-you/ (noting that "sector-specific deployments (for example, in healthcare, legal services, or other regulated professional environments)," allow confidentiality to be shaped by contract, and "[e]nterprise offerings…typically involve materially different commitments, technical configurations, and governance assumptions than consumer chatbots.").[3]

None of this, however, requires the Additional Disputed Language. Defendants say the Additional Disputed Language does "nothing more than carry [transparency] into any future AI tools that the parties intend to use." (Doc. No. 29 at 4.) Not so. The Additional Disputed Language requires a party to disclose new AI, but also to "obtain[ ] consent to amend this paragraph of the Protective Order" each time a new tool is used. (Doc. No. 29-1 at 12.) That is more than a transparency requirement. It is a consent-and-amend process that will require motion practice every time a party adopts a new tool. The Court favors transparency in conferrals. Indeed, it previously encouraged the parties to disclose their specific AI tools to each other. (*See* Doc. No. 28.) But the purpose for that transparency has been served. By exchanging information about their respective tools, the parties were able to understand each other's concerns and agree on an AI provision that sets clear, tool-agnostic requirements: no model training on inputs, no third-party disclosure beyond what is essential for service delivery, and the ability to delete information. (Doc. No. 29-1 at 11–12.) Now that the parties have specific parameters, they do not need to return to this Court every time they adopt a new tool. Both parties are represented by competent counsel, and they are each capable of evaluating whether a new tool satisfies the standing requirements. (*See* Doc. No. 29-1 ¶ 14.) Thus, while the agreed-upon AI provision is reasonable, the Additional Disputed Language is unnecessary, and the Court will strike it.

CONCLUSION

***3** For the reasons set forth herein, the Court **GRANTS** the parties' Second Joint Motion for Entry of Protective Order (Doc. No. 29) and will enter the proposed protective order (Doc. No. 29-1) without the Additional Disputed Language.

All Citations

Slip Copy, 2026 WL 2568346

Footnotes

1 This distinction is reflected in *Morgan*, where this Court engaged in two separate inquiries. The first was whether a litigant's *own* use of AI compromised work product protections. The second was a separate inquiry into the terms of a protective order that would govern the use of the *opposing party's* information.

2 In the Court's view, accepting this risk still does not forfeit the user's own expectations of privacy. Because many AI chats are of a private nature, reasonable protections should be afforded to them where appropriate. *See generally* *Morgan*, 2026 WL 864223.

3 Recent commentary suggests that courts are drawing too sharp a line between consumer-grade and enterprise-grade AI, and that distinction risks creating barriers for those who cannot afford enterprise-tier access. *See, e.g.*, Craig Ball, *The AI Protective Order Double Standard, Ball in Your Court* (July 27, 2026) *available at*, https://craigball.net/2026/07/27/the-

ai-protective-order-double-standard/. The Court takes that concern seriously and has itself warned of that problem. *See* *Morgan*, 2026 WL 864223, at *7, fn. 5. But when parties raise these disputes for resolution, the Court must balance all competing interests and ultimately determine which protections are reasonable under the specific facts and circumstances of the case and the current state of technology. That is precisely what the Court is doing here. And contrary to Plaintiff's statement that this is simply "the direction that winds are currently blowing," (Doc. No. 29 at 3), the Court is deliberate in its analysis and approach.

End of Document