

August 10, 2026

Tool or Intruder? What *Amazon v. Perplexity* Means for Agentic AI and the CFAA

Authors: Regina Sam Penti, Sabrina Kim, Chloe Meyers

Introduction

On August 4, 2026, the United States Court of Appeals for the Ninth Circuit issued its decision in *Amazon.com Services, LLC v. Perplexity AI, Inc.*, vacating a preliminary injunction that had barred Perplexity’s AI-enabled web browser from interacting with Amazon’s website.¹ The decision addresses a question of first impression: whether an AI “agent” that assists a user in navigating a website constitutes unauthorized “access” under the federal Computer Fraud and Abuse Act (CFAA).² The court held that, on the facts presented, it does not, concluding that it is the user, not the AI tool, who “accesses” the website for purposes of the statute.³ This alert summarizes the decision and its practical implications for AI developers and deployers, as well as for businesses whose platforms or data may be implicated by AI-driven interactions.

Background

The CFAA is the principal federal anti-hacking statute. It prohibits, among other things, intentionally accessing a “protected computer” without authorization or in excess of authorized access, and provides both criminal penalties and a civil right of action for those who suffer qualifying damages.⁴ In recent years, courts have interpreted the CFAA narrowly, confining it to its core purpose of preventing unauthorized intrusion into computer systems. For example, in *Van Buren v. United States*, the Supreme Court held that a person “exceeds authorized access” when they access a computer with authorization but then obtain information from off-limits areas of that computer, such as restricted files, folders, or databases, but not when

they access permitted information for an improper purpose.⁵ Further, in *hiQ Labs, Inc. v. LinkedIn Corp.*, the Ninth Circuit held that scraping publicly available data does not constitute access “without authorization.”⁶ *Amazon v. Perplexity* now confronts a new dimension: whether an AI agent’s actions can be attributed to its developer as “access” under the CFAA.

In this case, Perplexity developed an AI-enabled web browser called “Comet” with an optional agentic AI feature, which the court refers to as the “Assistant.” The Assistant can perform tasks autonomously within the browser at the user’s direction. When a user directs the Assistant to perform a task on Amazon.com, such as finding a product, the Assistant takes screenshots of the user’s browser view, sends those screenshots to Perplexity’s servers for analysis, and receives navigation instructions in return.⁷ Critically, the user’s browser (not Perplexity’s servers) communicates directly with Amazon’s servers at all times. The Assistant cannot operate independently, but instead relies on both user direction and server-side instructions to function.

Before Comet’s release, Amazon informed Perplexity that its AI products would not be authorized to interact with the Amazon Store.⁸ Perplexity declined to use a “user-agent string” that would have allowed Amazon to identify and block the Assistant. In response, Amazon filed suit in November 2025, alleging violations of the CFAA and its California state analog, the Comprehensive Computer Data Access and Fraud Act (CDAFA).⁹ In March 2026, the district court granted Amazon a preliminary injunction.¹⁰ Perplexity appealed.¹¹

The Court’s Analysis

The Ninth Circuit vacated the injunction, holding that Amazon was unlikely to succeed on the merits of its CFAA claim.¹² The court’s reasoning rested on a textual point: the CFAA punishes “whoever . . . intentionally accesses” a protected computer, and “whoever” means a person.¹³ In the court’s view, the Assistant, “however advanced,” is a tool, not a person for statutory purposes.¹⁴ Because Perplexity’s servers never communicated directly with Amazon’s servers, and because it was the

user's browser that transmitted requests to Amazon.com, the court concluded that the user, not Perplexity, was the one who "accessed" Amazon's computers, with the Assistant serving as a navigational aid.¹⁵

In coming to this holding, the court distinguished prior Ninth Circuit precedents. In *Facebook, Inc. v. Power Ventures, Inc.*, the court held a third-party platform liable under the CFAA for directly causing messages to be sent on Facebook's website, focusing mainly on the question of authorization, rather than access, and assumed, without extended analysis, that the platform itself had accessed Facebook's servers.¹⁶ In *Meta Platforms, Inc. v. BrandTotal Ltd.*, the court declined to extend CFAA liability to a browser extension that passively collected data already sent to a user's computer, finding it was not "accessing" or "communicating with Meta's servers."¹⁷ Here, the Assistant was more active than *BrandTotal's* extension but, like in *BrandTotal*, did not involve Perplexity's servers directly communicating with Amazon's systems. The court found this factual distinction dispositive.

The court's reasoning aligns with the narrowing trajectory of recent CFAA jurisprudence. Just as *Van Buren* rejected the idea that accessing information for an improper purpose triggers CFAA liability, the court here rejected the idea that facilitating a user's access through an AI tool is the same as the developer itself gaining entry.¹⁸ The court invoked the rule of lenity, observing that extending the CFAA to cover this conduct would require a "novel interpretation far afield" from the statute's anti-hacking purpose and could "expose users themselves to criminal liability" simply for using an AI-assisted browser. That result, the court noted, would be inconsistent with congressional intent.¹⁹ This echoes both *Van Buren's* concern about attaching "criminal penalties to a ... commonplace computer activity" and *hiQ Labs's* caution against stretching the statute to cover conduct far removed from hacking.²⁰

The court reached the same result under the CDAFA, holding that all equitable factors weighed against the injunction.²¹ It was careful, however, to limit its holding. The court explicitly stated: "We do not establish a new legal regime governing agentic

AI.”²² The decision turns on the specific technical architecture at issue, particularly the fact that Perplexity’s servers never directly accessed Amazon’s systems, and leaves open whether a different architecture might yield a different result. In a footnote, the court also clarified that its ruling does not impair Amazon’s ability to enforce access restrictions through private terms of service; the CFAA simply is not the vehicle for doing so on these facts.²³

Practical Implications

For AI Developers and Deployers

- **Architecture Matters.** The outcome in this case turned on how Perplexity’s product was built. Because the user’s device, not Perplexity’s servers, communicated with Amazon, the court found that there was no “access” by Perplexity. AI companies should carefully consider how their products are architected. Based on this case, designs where the user’s device remains the point of contact with third-party systems are less likely to raise CFAA concerns. Conversely, system architectures where an AI agent directly queries or communicates with a third party’s servers without user mediation may yield a different result.
- **The Holding Is Narrow, Not a Safe Harbor.** The court went out of its way to limit its ruling. It did not bless agentic AI interactions broadly, and it expressly left open whether greater AI autonomy or different technical designs might constitute “access.” Developers should not treat this decision as blanket permission to circumvent access restrictions. As AI agents grow more sophisticated and potentially act with greater autonomy and less user direction, the legal analysis may shift. The CFAA’s limitations should not be confused with a broader legal safe harbor, as other legal theories remain available.
- **Terms of Service Still Create Exposure.** The court noted that website operators remain free to enforce access restrictions through private contract.²⁴ While a

terms-of-service violation may not rise to CFAA liability, it can still support breach of contract, trespass to chattels, or unfair competition claims. AI companies should remain attentive to the terms governing platforms their products interact with, particularly where those terms explicitly prohibit automated or AI-assisted access.

For Businesses Whose Data May Be Implicated

- **The CFAA Has Limits as a Protective Tool.** Businesses that have relied on the CFAA to deter unwanted automated access to their platforms should reassess. Where an AI tool operates through a user's browser rather than directly accessing the business's servers, the CFAA is unlikely to provide a remedy. Combined with *hiQ Labs* (which limited the CFAA for publicly available data), this decision further narrows the statute's utility as a defensive tool, particularly against the new generation of AI-assisted browsing products.²⁵
- **Strengthen Contractual and Technical Protections.** Because the court preserved the enforceability of private access restrictions, businesses should review and strengthen their terms of service to explicitly address AI-assisted or automated access. The *Van Buren* framework suggests the CFAA is most protective when data sits behind clear technological "gates," such as authentication barriers, access controls, and similar mechanisms. For data that is accessible once a user is logged in, contractual terms and robust technical measures (bot detection, rate limiting, user-agent requirements) are the primary line of defense.
- **Consider the Public/Private Data Distinction.** The Ninth Circuit's body of CFAA precedent now draws a meaningful line between data behind authentication barriers and data that is publicly accessible or available to any authenticated user. Businesses should evaluate where their most sensitive data sits on this spectrum and ensure that their access controls and contractual restrictions reflect the level of protection they need, rather than relying on the

CFAA to fill gaps.

- **Monitor Legislative Developments.** Given the CFAA’s limitations as applied to AI-driven interactions, there is growing interest in legislative updates at both the federal and state level to address AI agents directly. New legislation could shift the legal landscape significantly, and businesses should monitor these developments closely.

Conclusion

The Ninth Circuit’s decision in *Amazon v. Perplexity* is the latest in a line of rulings, including *Van Buren*, *hiQ Labs*, and *Bartz v. Anthropic*,²⁶ in which courts have declined to stretch existing statutes to broadly regulate AI, opting instead for narrow, fact-specific holdings that aim to preserve the core purpose of each legal framework. The decision provides important early guidance on how the CFAA applies to agentic AI, but significant open questions remain. These include how courts will treat AI agents that directly access third-party systems rather than operating through a user’s device; whether the “tool vs. person” distinction will hold as AI agents become more autonomous; how the decision interacts with other legal theories available to platform operators; and whether Congress will update the CFAA or enact new legislation to address AI-assisted access directly. Companies developing or deploying AI tools, and companies whose platforms may be subject to AI-driven interactions, should evaluate their exposure in light of this evolving landscape.

1. *Amazon.com Servs., LLC v. Perplexity AI, Inc.*, No. 3:25-cv-09514, 2026 WL 2237587 (9th Cir. Aug. 4, 2026).

2. *Id.* at *8.

3. *Id.* at *15.

4. 18 U.S.C. § 1030(a)(2)(C), (c), (g).

5. *Van Buren v. United States*, 593 U.S. 374 (2021).

6. *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022). The Ninth Circuit’s CFAA holding in *hiQ* remains binding appellate authority. On remand, however, the district court found that *hiQ* breached LinkedIn’s User Agreement through its scraping and use of fake profiles, and the case resolved via consent judgment in LinkedIn’s favor, including \$500,000 in damages and a permanent injunction. See *hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-cv-03301-EMC, 2022 WL 16549042 (N.D. Cal. Nov. 4, 2022); Consent Judgment, No. 17-cv-03301-EMC (N.D. Cal. Dec. 8, 2022). The consent judgment stipulations illustrate viability of non-CFAA theories of liability.

7. *Amazon.com*, No. 3:25-cv-09514, at *7.

8. *Id.*, at *7; Amazon Staff, *Statement about Perplexity*, Amazon News (Nov. 4, 2025), <https://www.aboutamazon.com/news/company-news/amazon-perplexity-comet-statement>; *Bullying is Not Innovation*, Perplexity (Nov. 4, 2025), <https://www.perplexity.ai/hub/blog/bullying-is-not-innovation>.

9. *Amazon.com*, No. 3:25-cv-09514, at *7.

10. *Amazon.com Servs., LLC v. Perplexity AI, Inc.*, No. 3:25-cv-09514, 2026 WL 658407 (N.D. Cal. Nov. 4, 2025).

11. *Amazon.com Servs. LLC v. Perplexity AI, Inc.*, No. 3:25-cv-09514 (9th Cir. filed Mar. 2026).

12. *Amazon.com*, No. 3:25-cv-09514, at *18.

13. *Id.*, at *15.

14. *Id.*

15. *Id.*, at *14.

16. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016).

17. *Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218 (N.D. Cal. 2022).

18. *Amazon.com*, No. 3:25-cv-09514, at *15.

19. *Id.*, at *16-17.

20. *Van Buren*, 593 U.S. at 376; *hiQ Labs*, 31 F.4th at 1201.

21. *Amazon.com*, No. 3:25-cv-09514, at *18.

22. *Id.*, at *17.

23. *Id.*, at *21, fn 5.

24. *Id.*

25. *hiQ Labs*, 31 F.4th at 1197.

26. Regina Sam Penti, *From Books to Bots: Key Takeaways from the Anthropic Fair Use Decision for AI Developers and Copyright Holders*, Ropes & Gray LLP (Jun. 25, 2025), <https://www.ropesgray.com/en/insights/alerts/2025/06/from-books-to-bots-key-takeaways-from-the-anthropic-fair-use-decision-for-ai-developers>.