FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

AMAZON.COM SERVICES, LLC, *Plaintiff - Appellee*, v. PERPLEXITY AI, INC., *Defendant - Appellant*.	No. 26-1444 D.C. No. 3:25-cv-09514-MMC OPINION

Appeal from the United States District Court
for the Northern District of California
Maxine M. Chesney, District Judge, Presiding

Argued and Submitted June 11, 2026
Seattle, Washington

August 4, 2026

Before: MILAN D. SMITH, JR. AND ERIC C. TUNG, Circuit Judges, and JOHN CHARLES HINDERAKER, District Judge.[*]

[*] The Honorable John Charles Hinderaker, United States District Judge for the District of Arizona, sitting by designation.

Opinion by Judge Milan D. Smith, Jr.

SUMMARY**

Computer Fraud and Abuse Act

The panel (1) vacated the district court's preliminary injunction requested by Amazon.com Services, LLC, against Perplexity AI, Inc., an artificial intelligence company, to prevent the use of Perplexity's agentic web browser AI tool on Amazon.com in violation of the federal Computer Fraud and Abuse Act (CFAA) and its California state law analogue, the Comprehensive Computer Data Access and Fraud Act (CDAFA); and (2) remanded for further proceedings.

To succeed on a claim under the CFAA, a plaintiff must show that the defendant (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that the defendant (3) thereby obtained information (4) from any protected computer, and that (5) there was loss to one or more persons during any one-year period aggregating at least $5,000 in value.

The panel concluded that Amazon was not entitled to a preliminary injunction because it was unlikely to succeed on the merits of its CFAA claims by showing that Perplexity "accessed" Amazon computers for CFAA purposes. On the facts before the panel, it concluded that Perplexity did not

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

use a tool to "access" Amazon's computers. Rather, it was the user who "accessed" Amazon's computers, with the help of Perplexity's AI agent, the "Assistant," to carry out specific acts on Amazon.com. The panel concluded that Amazon was unlikely to succeed on the merits of its CDAFA claim for the same reason that Amazon was unlikely to succeed on the merits of its CFAA claim: the user (not Perplexity) accessed Amazon using the Assistant as an AI tool.

The panel held that the district court erred in concluding that the remaining equitable factors favored Amazon. The remaining equitable factors favored Perplexity because (1) the potential harms Amazon faces do not weigh in favor of an injunction, (2) the balance of the equities favors Perplexity and weighs against an injunction, and (3) an injunction against conduct that likely does not violate the CFAA or the CDAFA would not serve the public interest. The panel therefore vacated the preliminary injunction and remanded for further proceedings.

COUNSEL

Hagan Scotten (argued), Hueston Hennigan LLP, New York, New York; Christine M. Woodin, Moez M. Kaba, and Billy J. McLain, Hueston Hennigan LLP, Los Angeles, California; for Plaintiff-Appellee.

Christopher G. Michel (argued), Quinn Emanuel Urquhart & Sullivan LLP, Washington, D.C.; Lucas A. Hammill and Renita N. Sharma, Quinn Emanuel Urquhart & Sullivan LLP, New York, New York; Daniel C. Posner, Jonathan H. Kim, and John B. Quinn, Quinn Emanuel Urquhart &

Sullivan LLP, Los Angeles, California; Andrew H. Schapiro, Quinn Emanuel Urquhart & Sullivan LLP, Chicago, Illinois; for Defendant-Appellant.

Esha Bhandari and Lauren Yu, American Civil Liberties Union Foundation, New York, New York; Jake Karr, Ramya Krishnan, and Alex Abdo, Knight First Amendment Institute, Columbia University, New York, New York; for Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Northern California, and Knight First Amendment Institute at Columbia University.

Corynne McSherry, Victoria Noble, and Andrew Crocker, Electronic Frontier Foundation, San Francisco, California, for Amici Curiae Electronic Frontier Foundation, Alliance for Responsible Data Collection, Mozilla Corporation, Digital Medusa, and Eleutherai.

Tod Cohen and Annie Nguyen, Manatt Phelps & Phillips LLP, San Francisco, California, for Amicus Curiae Software & Information Industry Association.

David M. Gossett, Davis Wright Tremaine LLP, Washington, D.C.; Alexandra Perloff-Giles, Davis Wright Tremaine LLP, New York, New York; for Amicus Curiae National Retail Federation.

Karl Huth, Matthew Reynolds, J. Lee Hill, and Jack Mitchell, Huth Reynolds LLP, Huntington, New York, for Amicus Curiae Digital Context Next.

Michael S. Elkin and Sean R. Anderson, Winston and Strawn LLP, New York, New York; Jennifer A. Golinveaux and Thomas J. Kearney, Winston and Strawn LLP, San Francisco, California; for Amicus Curiae News/Media Alliance.

A. Jeff Ifrah and Robert W. Ward, Ifrah PLLC, Washington, D.C., for Amicus Curiae Air Transport Association of America Inc. d/b/a Airlines for America.

OPINION

M. SMITH, Circuit Judge:

This case concerns a preliminary injunction requested by Amazon.com Services, LLC (Amazon) against Perplexity AI, Inc. (Perplexity), an artificial intelligence (AI) company, to prevent the use of Perplexity's agentic web browser AI tool on Amazon.com in violation of the federal Computer Fraud and Abuse Act (CFAA) and its California state law analogue. Because Amazon is unlikely to succeed in showing that Perplexity "accessed" Amazon computers for CFAA purposes, we vacate the district court's preliminary injunction and remand for further proceedings.

BACKGROUND

I. Statutory Background

Congress originally enacted the CFAA as part of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. Pub. L. No. 98-473, tit. II, ch. XXI, 98 Stat. 1837, 2190–92 (codified as amended at 18 U.S.C. § 1030). In enacting the CFAA, Congress aimed "to prevent intentional intrusion onto someone else's computer—specifically, computer hacking." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1196 (9th Cir. 2022). This initial version of the CFAA was limited to computers "containing national security information or financial data and those operated by or on behalf of the government." *Id.* at 1197. In

1996, Congress expanded the CFAA's scope to any "protected computer." *Id.* Now, § 1030 defines "protected computer" to include a computer (A) exclusively used by the federal government or a financial institution , (B) "used in or affecting interstate or foreign commerce or communication," or (C) used in a voting system either (I) to support a federal election, or (II) that "has moved in or otherwise affects interstate or foreign commerce." *See* 18 U.S.C. § 1030(e)(2). The CFAA also includes a private cause of action for anyone who "suffers damage or loss" aggregating at least $5,000 per year "by reason of a violation" of the statute's criminal provisions. *See id.* §§ 1030(c)(4)(A)(i)(I), (e)(11), (g).

California enacted the Comprehensive Computer Data Access and Fraud Act (CDAFA), a similar computer access law, in 1987. *See* Cal. Penal Code § 502. The state legislature's goal in passing the CDAFA was "to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." *Id.* § 502(a). The CDAFA criminalizes "[k]nowingly and without permission access[ing] or caus[ing] to be accessed any computer, computer system, or computer network," and also provides a private cause of action. *Id.* §§ 502(c)(7), (e)(1).

II. Factual Background

a. Perplexity and the Comet Browser

Perplexity is an AI startup and the creator of an AI-enabled web browser, Comet. After acquiring another browser company, Sidekick, Perplexity developed Comet and publicly released it in 2025. Comet is a web browser that operates like Google Chrome, running locally on a

user's machine and enabling the user to navigate the Internet. According to Perplexity, Comet's differentiating feature is an optional AI "agent" (the Assistant) that "can perform tasks at the user's direction, such as browsing websites like Amazon.com to shop for requested goods."

When a Comet user directs the Assistant to locate an item on Amazon.com, the Assistant takes screenshots of the browser view, sends those screenshots from the user's computer to Perplexity's servers, and receives instructions from Perplexity's servers on how to navigate Amazon.com. In other words, the Assistant cannot operate wholly independently; it relies on direction from the user and instructions from Perplexity's servers.

b. Amazon and the Amazon Store

Amazon owns and operates Amazon.com, also known as the Amazon Store. Customers may create Amazon.com accounts, which, according to Amazon, allow them to "manage orders, store payment information and delivery addresses, receive personalized recommendations, track purchases, and process returns within their password-protected accounts." Amazon also operates in the AI space and launched agentic AI products in 2025.

c. The Comet Agent and the Amazon Store

Before Comet's release, Amazon told Perplexity's CEO that Perplexity's AI products would not be permitted to access the Amazon Store. After Perplexity launched Comet and the Assistant accessed the Amazon Store, Amazon again informed Perplexity that it did not have authorization to do so. At the core of the dispute was Perplexity's decision not to use a "user-agent string," a mechanism "that would communicate that the user has activated an AI agent." That

user-agent string would allow Amazon to block the Assistant's access to the Amazon store.[1]

d. Procedural History

Amazon filed its Complaint in November 2025, alleging violations of the CFAA and the CDAFA. Amazon also moved simultaneously for a preliminary injunction. In March 2026, the district court held a hearing on the motion and issued a tentative ruling in Amazon's favor, indicating that it was a close call. The district court soon after issued a written order granting Amazon's requested preliminary injunction on the grounds that Amazon had shown a likelihood of success on its CFAA claims under § 1030(a)(2) and its CDAFA claims.[2] The district court also held that Amazon had shown it would suffer irreparable harm absent an injunction and that the balance of the hardships and public interest favored Amazon.

The district court denied Perplexity's request that the court require Amazon to post a bond and Perplexity's request for a broader stay pending appeal, although it issued a seven-day administrative stay to allow Perplexity to seek a stay pending appeal with our court. Perplexity filed its Notice of Appeal the next day and simultaneously moved for an injunction pending appeal. A motions panel of this court initially entered an administrative stay and then

[1] The parties dispute whether Perplexity knowingly altered the Assistant's user-agent string once Amazon initially succeed in identifying and blocking the Assistant from the Amazon Store.

[2] The district court's written order did not address Amazon's § 1030(a)(4) claim, and Amazon does not raise any arguments regarding that provision on appeal.

subsequently issued a stay pending appeal, ordering expedited briefing and calendaring.

ANALYSIS

I. Standard of Review

We review the grant of a preliminary injunction for abuse of discretion. *See Sierra Forest Legacy v. Rey*, 577 F.3d 1015, 1021 (9th Cir. 2009). In determining whether a district court has abused its discretion, we must first determine if the district court identified the correct legal rule and then determine whether the district court's "application of the correct legal standard was (1) illogical, (2) implausible, or (3) without support in inferences that may be drawn from the facts in the record." *United States v. Hinkson*, 585 F.3d 1247, 1261–62 (9th Cir. 2009) (en banc) (internal quotation marks omitted) (emphasis omitted).

II. The district court abused its discretion in granting the preliminary injunction.

The party requesting a preliminary injunction must show that "(1) they are likely to succeed on the merits; (2) they are likely to suffer irreparable harm in the absence of preliminary relief; (3) the balance of equities tips in their favor; and (4) a preliminary injunction is in the public interest." *Sierra Forest Legacy*, 577 F.3d at 1021 (citing *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)). We have "adopted a sliding-scale approach to the *Winter* factors," where "serious questions going to the merits and a hardship balance that tips sharply toward the plaintiff can support issuance of an injunction, assuming the other two elements of the *Winter* test are also met." *Bennett v. Isagenix Int'l LLC*, 118 F.4th 1120, 1126 (9th Cir. 2024) (internal quotation marks omitted).

a. Amazon is unlikely to succeed on the merits of its CFAA and CDAFA claims.

i. Amazon's CFAA Claim

To bring a successful § 1030(a)(2) claim pursuant to the CFAA private right of action, Amazon must show that Perplexity "(1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that [Perplexity] (3) thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was loss to one or more persons during any one-year period aggregating at least $5,000 in value." *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir. 2009). We have cautioned against interpretations that "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *United States v. Nosal* (*Nosal I*), 676 F.3d 854, 857 (9th Cir. 2012) (en banc).

In its short written order, the district court stated: "Amazon has provided strong evidence that Perplexity, through its Comet browser, accesses with the Amazon user's permission but without authorization by Amazon, the user's password-protected account, thereby obtaining information as to the user's private Amazon account information, and that such information is transmitted to Perplexity's servers for the purpose of conducting said user's requested tasks," and "Amazon has submitted essentially undisputed evidence that it has expended significantly more than $5,000 in responding to such circumstances, including, for example, costs attributable to numerous hours spent by Amazon employees in developing tools to block Comet's access to its private customer accounts and detecting future unauthorized

access by Comet." The district court erred, however, in its "access" analysis.

Perplexity argues that "access" for CFAA purposes requires the defendant to have "gain[ed] entry" to the computer "system itself." *See Van Buren v. United States*, 593 U.S. 374, 388 & n.6 (2021). In Perplexity's view, it never "gain[ed] entry" to an Amazon computer because no Perplexity computer ever accessed Amazon's servers. Instead, Perplexity explains that any Amazon data was first transmitted to the user's computer and then to Perplexity's servers via browser screenshots.

This is most akin, Perplexity argues, to an Apple user accessing Amazon.com via the Safari web browser, even if "the Safari software automatically fills in the user's address and payment information at checkout on the user's behalf." Any arguable intent that the Assistant possesses should, Perplexity asserts, be ascribed to the user, not to Perplexity itself, because "the Assistant is mere computer software that has no 'intent' apart from what the user directs it to do on the user's behalf." Perplexity also points to *Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218 (N.D. Cal. 2022), for the proposition that access to data on a user's computer sent to that user by a company is not the same as access to that company's computer. *See id.* at 1232, 1260–61.

In Amazon's view, it suffices for CFAA purposes that the Assistant communicates with Perplexity's servers to, as Perplexity states, "determine appropriate actions" regarding the Amazon Store. Amazon argues that Perplexity itself admits that the Assistant proceeds autonomously and "behaves like an efficient human shopper," and that autonomous action should be ascribed to Perplexity because

it is the Perplexity servers that direct the Assistant. According to Amazon, this argument tracks our conclusion in *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), and what Amazon describes as a "relatively ministerial, user-directed task" can be ascribed to Perplexity. *See id.* at 1066–68. This is different, Amazon argues, from Safari because the Assistant's agentic capabilities—i.e., its autonomous action—go beyond the passive displays of a traditional web browser. Amazon further argues that *BrandTotal* is distinguishable because the data there was collected passively through users' normal use of Facebook, as opposed to the Assistant actively navigating Amazon.com.

Agentic AI is an emerging technology. There is thus little to no existing caselaw directly dealing with how to ascribe responsibility for AI agents like the Assistant, let alone caselaw specifically dealing with agentic AI in the CFAA context. And CFAA cases dealing with more established technologies do not provide a perfect analogue to the case at hand. Take the parties' two main cited cases as examples.

In *Power Ventures*, Facebook sued Power Ventures under the CFAA for alleged violations of the same subsection at issue in this case. *See* 844 F.3d at 1066. Power Ventures operated a social media aggregation platform that allowed users to "see all contacts from many social networking sites on a single page." *Id.* at 1062. As part of a promotional campaign in which Power awarded users who invited others to the Power platform, "Power caused a message to be transmitted to the user's friends within the Facebook system." *Id.* at 1063. We held that Power was liable pursuant to the CFAA for continuing to cause such

messages to be sent on Facebook even after receiving a cease-and-desist letter. *See id.* at 1065–69.

But this case differs from *Power Ventures* in several respects. First, in *Power Ventures*, we assumed without discussion that Power "accessed" Facebook for CFAA purposes. *See id.* at 1066–69. The bulk of the analysis was devoted to authorization, not access, and we simply stated that "Power caused a message" to be sent on Facebook, indicating this was the result of "Power users t[aking] action akin to allowing a friend to use a computer or to log on to an e-mail account." *See id.* at 1063, 1067. Nevertheless, our description implied that Power accessed Facebook's servers. *See, e.g.*, *id.* at 1067 ("Power reasonably could have thought that consent from *Facebook users* to share the promotion was permission for Power to access *Facebook's* computers.").

Nor does *BrandTotal* provide a perfect analogue. In that case, Meta sued BrandTotal pursuant to the CFAA for its UpVoice 2021 browser extension, which passively logged and sent to BrandTotal "data that users receive from Facebook through their normal use of the website." *BrandTotal*, 605 F. Supp. 3d at 1260. The district court explained that UpVoice accessed only the "data that Meta has sent to the individual users," and that the program was "not proactively 'accessing' or 'communicating with' Meta's servers." *Id.* Relying on the rule of lenity then,[3] the

[3] We have previously explained that because the CFAA is "primarily a criminal statute" and interpretations of its provisions are "equally applicable" in the civil and criminal contexts, the rule of lenity should guide any interpretation of the statute, meaning that "any ambiguity" should be construed "against the government." *Brekka*, 581 F.3d at 1134–35 (internal quotation marks omitted).

district court declined to extend CFAA liability to such conduct. *See id.* at 1261. But here, the Assistant appears to do more than passive data collection.

The Amicus Brief of Electronic Frontier Foundation, Alliance for Responsible Data Collection, Mozilla Corporation, Digital Medusa, and EleutherAI articulates the nature of the system most clearly:

> When a user visits a website, only . . . the browser . . . communicates with the website's server. Specifically, when a user visits an Amazon.com webpage, the browser requests the contents of the page from Amazon's server and displays the page to the user. If the user activates the Assistant, the Assistant will analyze the contents of the page that has been displayed by the browser on the user's computer. . . . If necessary to carry out the task requested by the user, the Assistant may communicate the user's instructions, along with information received from the browser pertaining to the page accessed by the user and any potentially relevant browsing history, to Perplexity's AI servers. Perplexity's servers never directly access Amazon's servers.

What is clear from this description—and how the parties themselves describe the systems at issue—is that Perplexity itself does not directly communicate with Amazon's servers.

We must nevertheless determine whether Perplexity accesses Amazon.com through the Assistant. The CFAA's plain language suggests the Assistant itself cannot "access"

Amazon's servers. The relevant provision of the CFAA punishes "*[w]hoever* . . . intentionally accesses" a "protected computer." 18 U.S.C. § 1030(a)(2) (emphasis added). In other words, the CFAA contemplates access by a person. However advanced the Assistant currently is, it is a tool, not a person for statutory purposes. *See* 18 U.S.C. § 921(a)(1) ("The term . . . 'whoever' include[s] any individual, corporation, company, association, firm, partnership, society, or joint stock company."); *see also Whoever*, Cambridge English Dictionary, [https://perma.cc/YY3T-VTJF] (last visited July 16, 2026) ("[T]he *person* who" (emphasis added)).

The Supreme Court has instructed that, "in the computing context, 'access' references the act of entering a computer system itself or a particular part of a computer system, such as files, folders, or databases." *Van Buren*, 593 U.S. at 388 (internal quotation marks omitted). Our focus is thus to ask whether Perplexity uses a tool (the Assistant) to "access" Amazon's computers. On the facts before us, we answer no. It is the user who "accesses" Amazon's computers, with the help of the Assistant to carry out specific acts on Amazon.com. To be sure, Perplexity may receive screenshots of the user's browser and may communicate instructions to the Assistant. But those activities, by themselves, do not mean that Perplexity has "accessed" (gained entry) to Amazon's servers. We do not address whether, on a different record or new facts, Perplexity may exercise control over the Assistant in such a way as to gain entry to Amazon's servers. On the current record, Amazon

is not likely to succeed in proving the "access" prong of its CFAA claim.[4]

This conclusion is further reinforced by the rule of lenity. As previously discussed, the CFAA is "primarily a criminal statute" and courts' interpretation of its provisions are "equally applicable" in the civil and criminal contexts. *Brekka*, 581 F.3d at 1134. Thus, the rule of lenity guides our interpretation, meaning we construe "any ambiguity" as to statutory meaning against liability. *Id.* at 1135 (internal quotation marks omitted). To be sure, the rule of lenity applies only where the statute at issue "is truly ambiguous." *United States v. LeCoe*, 936 F.2d 398, 402 (9th Cir. 1991); *see also Shular v. United States*, 589 U.S. 154, 165 (2020). Even accepting Amazon's approach as reasonable, imposing liability here would require a novel interpretation far afield from the statute's purpose "to prevent intentional intrusion onto someone else's computer—specifically, computer hacking." *hiQ*, 31 F.4th at 1196. Another note of caution: Amazon's approach, if accepted, could expose users themselves to criminal liability (under a conspiracy or aiding-and-abetting theory) for facilitating Perplexity's purported unauthorized access to Amazon's servers. We are conscious of precedent cautioning against "transform[ing] whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved" or "criminaliz[ing] a broad range of day-to-day activity." *Nosal I*, 676 F.3d at 860, 862 (internal quotation marks omitted). In our view, it is unlikely that Congress would

[4] We do not address the remainder of the CFAA factors, including the scope of the CFAA's loss provision, because they are "unnecessary to resolve this case." *Safari Club Int'l v. Haaland*, 31 F.4th 1157, 1178 n.1 (9th Cir. 2022).

have exposed individual users to criminal liability under the CFAA by using the Assistant and Comet browser to access Amazon.com under these facts. On these narrow facts and given the care with which we must interpret the CFAA to ensure defendants are on notice, we decline to adopt Amazon's interpretation of § 1030(a)(2).

Because we recognize that agentic AI is an emerging technology, we reiterate what this opinion is not. We do not establish a new legal regime governing agentic AI. We do not address whether in other contexts, including tort claims, Perplexity can avoid liability for the Assistant's actions. Our holding here is limited to "access" as contemplated by the CFAA and as applied to the Assistant's interactions with Amazon.com on the record before us, not the broader legal landscape surrounding agentic AI. The legal understanding of agentic AI will doubtless change as AI technology grows increasingly sophisticated. For now, this opinion reflects and applies to the state of technology only as presented in the filings in this case.

ii. Amazon's CDAFA Claim

The CDAFA, the California state law analogue to the CFAA, similarly focuses on "conduct such as hacking into and tampering with computer systems and data, and the disruptions and costs of such conduct to the business of public and private entities." *Teran v. Superior Ct.*, 334 Cal. Rptr. 3d 299, 308 (Cal. Ct. App. 2025). However, the "statutes are different" in certain ways. *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2016). Amazon argues that the CDAFA has a broader definition of "access," simpler permission requirements, and no requirement that information is "obtained."

Ultimately, Amazon's CFAA and CDAFA claims rise and fall together. The CDAFA defines "access" to mean, among other things, "caus[ing] input to [or] data processing with . . . the logical, arithmetical, or memory functions of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(1). And the relevant prohibition applies only to "any person" who causes unauthorized access. *Id.* § 502(c)(7). While Amazon might be correct that "access" under the CDAFA is broader than the CFAA's definition, the focus of the inquiry is still on the person accessing or causing the access. Accordingly, we arrive at the same conclusion: the user (not Perplexity) accesses Amazon using the Assistant as an AI tool, and thus Amazon is unlikely to succeed on the merits of its CDAFA claim.

b. The district court erred in concluding that the remaining injunction factors favored Amazon.

At the outset, the parties dispute whether the district court impermissibly substituted its likelihood of success finding for the remaining equitable factors. It is true that even if a plaintiff is likely to succeed on the merits, the district court must nonetheless consider irreparable injury, the balance of the equities, and the public interest—that is, likelihood of success is not sufficient on its own to warrant a preliminary injunction. *See Klein v. City of San Clemente*, 584 F.3d 1196, 1207 (9th Cir. 2009). However, this is not a case where the district court entirely ignored the equitable factors after determining a likelihood of success on the merits. While much of the district court's equitable analysis was premised on the existence of a CFAA violation, it discussed each of the equitable factors.

i. Irreparable Harm

The district court reasoned that Amazon would suffer irreparable harm absent an injunction because Perplexity "will continue to engage in the above-referenced challenged conduct." While the district court might be correct that a showing of likelihood of success on the merits is sufficient to establish a likelihood of irreparable harm, *see Facebook, Inc. v. Power Ventures, Inc.*, 252 F. Supp. 3d 765, 782 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019), Amazon failed to make that showing here. Irreparable harm is thus a closer question.

As a general matter, "[e]vidence of threatened loss of prospective customers or goodwill certainly supports a finding of the possibility of irreparable harm." *Stuhlbarg Int'l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001). But Amazon puts forth only weak evidence as to the actual threat of such harm. It cites declarations claiming that the Assistant "may not select the best price, delivery method, or product recommendations for a customer when shopping in the Amazon Store," which suggest that the Assistant leads to a degraded shopping experience. These types of harms, though, are more attenuated than the harms recognized in other "threat of harm" cases. In *Stuhlbarg*, for example, the risk of harm arose from the United States Customs Service's detention of goods already promised to new customers with large orders. *Id.* at 840–41. The harm to goodwill was obvious because those customers would not receive the specific product they ordered. By comparison, the degradation of the overall Amazon.com shopping experience is more abstract, as is the degree to which users would hold the Assistant responsible for any such degradation given their choice to employ it.

Amazon's cyber-risk harm argument is also weak. Amazon asserts that "multiple security researchers corroborated the security risks posed by Perplexity," but Perplexity argues that Amazon's own expert stated that he was unable to fully replicate those risks and that Perplexity has addressed any such risks. Only one of the cyber risks Amazon points to in its expert's declaration involved a shopping website, and even that example did not involve Amazon.com specifically. While the expert's declaration thus provides some support for the idea that use of the Assistant may introduce cyber security risks to Amazon.com, Amazon's proffered evidence is limited and counteracted, at least in part, by Perplexity's asserted cyber improvements. Accordingly, the potential harms Amazon faces do not weigh in favor of an injunction.

ii. Balance of the Equities and the Public Interest

Because Amazon has failed to show a likelihood of success on the merits of its claims, its arguments regarding the harm to Perplexity from an injunction fall flat. An injunction here, where it is unlikely that Amazon will be able to establish statutory violations, needlessly imposes a burden on Perplexity by preventing it from fully operating a product that it spent large sums developing. As a result, the balance of the equities favors Perplexity and weighs against an injunction.

Similarly, an injunction against conduct that likely does not violate the CFAA or the CDAFA would not serve the public interest. Instead, such an injunction would impair consumer choice and needlessly limit development of a

nascent technology.[5] The public interest thus favors Perplexity.

CONCLUSION

Because Amazon is unlikely to succeed on the merits of the "access" prong of the CFAA and CDAFA analysis and the equitable factors do not otherwise strongly favor an injunction, we **VACATE** the preliminary injunction granted by the district court and **REMAND** for further proceedings consistent with this opinion.[6]

[5] This outcome does not impair Amazon's ability to regulate access to Amazon.com via private terms of service for its users. On the facts before us, Amazon is simply unlikely to succeed in its attempt to regulate access by invoking the CFAA and the CDAFA.

[6] Perplexity's motion to file documents under seal, Dkt. 28, is **GRANTED.**