No. 26-1444

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

AMAZON.COM SERVICES, LLC,

PLAINTIFF -APPELLEE,

V.

PERPLEXITY AI, INC.,

DEFENDANT- APPELLANT.

On Appeal from the United States District Court
for the Northern District of California, San Francisco
3:25-cv-09514-MMC
The Honorable Maxine M. Chesney

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, ALLIANCE FOR RESPONSIBLE DATA COLLECTION, MOZILLA CORPORATION, DIGITAL MEDUSA, AND ELEUTHERAI IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Corynne McSherry
Victoria Noble
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: corynne@eff.org
Telephone: (415) 436-9333
Fax: (415) 436-9993
Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amici curiae Electronic Frontier Foundation, Alliance for Responsible Data Collection, Digital Medusa, and EleutherAI state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock. Amicus curiae Mozilla Corporation is wholly owned by the Mozilla Foundation which does not have a parent corporation and no publicly held corporation owns 10% or more of its stock.

Dated: April 8, 2026

By: /s/ *Corynne McSherry*
Corynne McSherry

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Legislative Materials

Other Authorities

STATEMENT OF INTEREST OF AMICI[1]

The Electronic Frontier Foundation ("EFF") is a non-profit public interest organization that has worked for more than thirty-five years to ensure new technology enhances, rather than erodes, civil liberties. EFF and its members support the principled and fair application of computer crime laws to online activities and systems—especially as it impacts internet users, innovators, and security researchers. Additionally, as part of its Coders' Rights Project, EFF offers pro bono legal services to researchers whose work in the public interest may be unjustly chilled by such laws. EFF has served as counsel or amicus curiae in many of the key cases addressing federal and state computer crime statutes.

The Alliance for Responsible Data Collection ("ARDC") is an unincorporated association of businesses, non-profit organizations, and individuals whose mission is to preserve access to public internet data by providing a trusted framework for responsible data collection. ARDC has published guidance on industry best practices for public web data collection, organized workshops, and frequently presents on the importance of access to publicly available web data to the global economy, businesses, non-profits, journalists, researchers, and government watchdogs.

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), amici curiae certify that no person or entity, other than amici curiae, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. All parties have consented to the filing of this brief.

Mozilla Corporation is a global, mission-driven organization that creates open source products like the Firefox browser and Gecko browser engine. Today, over 200 million people worldwide use the Firefox browser. Mozilla's mission is guided by the Manifesto, a set of principles recognizing that, among other things, the Internet must remain open and accessible to all and that privacy and security online are fundamental.

Digital Medusa is a boutique advisory firm that engages in research and advocacy at the intersection of internet infrastructure governance, platform accountability, and human rights — consistently centering the perspectives of those most vulnerable to exclusion from technical governance processes, including individual creators, users in under-resourced regions, and communities whose rights are often subordinated to commercial or security interests.

The EleutherAI Institute ("EleutherAI") is a non-profit research organization that builds artificial intelligence models and software, and releases these artifacts openly on the Internet. This open source release enables EleutherAI to advance public-interest research in AI security and evaluation, and to further support thousands of independent researchers and innovators.

INTRODUCTION

The stakes of this dispute go far beyond a skirmish between two commercial services. This case concerns whether the Computer Fraud and Abuse Act

("CFAA")—a 1986 criminal "anti-hacking" statute intended to target malicious computer breaks-ins—gives private companies like Amazon veto power over how the public accesses and engages with publicly available information on their websites.

Open access is a hallmark of today's internet, and is one of the main reasons it has become our "modern public square." *See Packingham v. North Carolina*, 582 U.S. 98, 107 (2017). Developers like Perplexity facilitate that access by creating tools that enable users to meaningfully engage with the web. As new, increasingly powerful artificial intelligence tools rapidly shift user behavior, companies have responded by attempting to limit tools that may not serve their business interests.[2] Carefully balancing the competing policy interests presented by AI is particularly important, given that poor policy choices could derail the development of this nascent technology and impede users' ability to meaningfully benefit from it.

Expansive applications of general-purpose anti-hacking laws like the CFAA are a particularly poor substitute for that careful balancing. That is why binding precedent forecloses overly broad applications of the CFAA that "turn a criminal hacking statute into a 'sweeping Internet-policing mandate.'" *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1200–01 (9th Cir. 2022) (quoting *United States v.*

[2] Will Knight, *AI Bots Are Now a Significant Source of Web Traffic*, WIRED (Feb. 4, 2026), https://www.wired.com/story/ai-bots-are-now-a-signifigant-source-of-web-traffic/.

Nosal, 676 F.3d 854, 858 (9th Cir. 2012) ("*Nosal I*")).

Unfortunately, the district court applied the wrong precedent and compounded the error with an improperly cursory analysis of the remaining preliminary injunction factors. This Court should reverse the decision below and apply the "narrow interpretation" of the CFAA that the law requires. *Id.*

BACKGROUND

The district court's order appears to rest on a fundamental misunderstanding of how the technology at issue, Perplexity's "agentic" browser, Comet, actually works.

Though Comet may look like a single AI "agent" that operates on Perplexity's servers, it is actually a collection of multiple systems, which run on different computers and are controlled by different parties. 3-ER-521–22; *see also* 2-ER-269–70. Comet is comprised of three different components: (1) a traditional web browser, which operates on the user's computer; (2) an AI "Assistant" feature that operates exclusively within the browser on the user's computer and automates certain browsing activities, at the user's request; and (3) Perplexity's AI systems, running on the company's servers, which process the user's instructions to the Assistant, contextual data, and limited information about the page displayed on the user's device, and determines appropriate actions to effectuate the user's request. *See* 3-ER-521–525.

When a user visits a website, only one of these three components—the browser—communicates with the website's server. *See* 3-ER-524–525. 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. 3-ER-522–524. 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. 3-ER-523–524. The Assistant does not access Amazon's servers. 3-ER-524–525. 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. 3-ER-524–525; *see also* 2-ER-284. Perplexity's servers never directly access Amazon's servers. 3-ER-525.

Amazon alleges that elements of Comet that run on the user's machine within the Comet browser obtain information from Amazon, then transmits at least some of that information to Perplexity's servers. 2-ER-269–270; 2-ER-277. But the vast majority of Amazon webpages are public. Anyone can browse pages for products offered for sale on Amazon whether or not they are logged into an Amazon account.[3]

[3] Amazon's privacy policy specifically informs users that they may browse Amazon's website while logged out of their Amazon account (and even recommends "signing out of your account" before browsing the site as a privacy-protection measure). AMAZON, *Amazon.com Privacy Notice*, (last updated Dec. 31, 2025),

In other words, Amazon's web servers deliver these pages to any browser—including the Comet browser—that requests them, even if a user never logged in.

To be sure, users have legitimate privacy interests in their "browsing history." However, a user's browsing history—a record of the sites and pages visited from a browser—is collected and stored locally by the user's browser, not Amazon's secured servers.[4] Additionally, if a Comet user logs into their Amazon account, only the browser, operating on the user's computer, handles their login credentials. 3-ER-525. The user's password is stored only on the user's device and is never transmitted to Perplexity's servers. 3-ER-525. When a user logs into Amazon, Amazon generates an HTTP "cookie"—a unique string of alphanumeric characters associated with a user—and sends the cookie to the browser, which stores it on the user's device. 2-ER-270–272.[5] The next time a user visits an Amazon.com webpage, the browser sends the cookie back to the site's server, allowing Amazon to recognize the user without requiring them to re-enter their login credentials. 2-ER-270–272.[6]

---

https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ.

[4] *See* WIKIPEDIA, *Web Browsing History*, https://en.wikipedia.org/wiki/Web_browsing_history; PCMAG ENCYCLOPEDIA, *Browser History*, https://www.pcmag.com/encyclopedia/term/browser-history.

[5] Mozilla, *Using HTTP Cookies*, MOZILLA DEVELOPER NETWORK (Oct. 8, 2025), https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/Cookies; CLOUDFLARE, *What Are Cookies*, https://www.cloudflare.com/learning/privacy/what-are-cookies/.

[6] *Id.*

This is entirely standard: most major web browsers, including Google Chrome and Mozilla Firefox, store and transmit authentication "cookies" in the same way that Comet does. 2-ER-270–72 (explaining that browsers "typically" store authentication cookies).[7]

Private user information stored on protected areas of Amazon's servers, such as full credit card numbers or past purchases, are never accessed by any component of the Comet system, unless displayed on a webpage accessed by the user through the browser, either by navigating to the page themselves or instructing the Assistant to do so. 3-ER-525; *see also* 2-ER-274–275.

In short, Comet never causes Perplexity's servers to directly access Amazon computers, let alone protected areas of those systems. Only the Comet user's computer communicates with Amazon servers, and in most cases, will receive only public page content when it does so.

ARGUMENT

I. SIMPLY PROVIDING A TOOL TO "ACCESS" A WEBSITE CANNOT GIVE RISE TO CFAA LIABILITY.

A. The CFAA Was Meant to Target Computer Break-Ins.

Congress intended the Computer Fraud and Abuse Act ("CFAA") to "prevent intentional intrusion onto someone else's computer." *hiQ Labs*, 31 F.4th at 1196.

[7] *Id.*

Congress sought "to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data." *United States v. Valle,* 807 F.3d 508, 525 (2d Cir. 2015) (citing H.R. Rep. No. 98–894, 1984 U.S.C.C.A.N. 3689, 3691–92, 3695–97 (1984); S. Rep. No. 99–432, 1986 U.S.C.C.A.N. 2479, 2480 (1986)). After a "flurry of electronic trespassing incidents," lawmakers were concerned about nightmare scenarios such as the one depicted in the film War Games, where a teenaged hacker played by Matthew Broderick breaks into a U.S. military supercomputer and unwittingly nearly starts a nuclear war. The 1984 House Committee Report (incorrectly) stated that the film was a "realistic representation of the automatic dialing and access capabilities of the personal computer." H.R. Rep. No. 98–894, U.S.C.C.A.N. 3689, 3696 (1984).

In response, in 1984 Congress passed the precursor to the CFAA to address serious and malicious computer break-ins. The law was "designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives[.]'" *LVRC Holdings LLC v. Brekka,* 581 F.3d 1127, 1130–31 (9th Cir. 2009). The 1984 House Committee Report explained, "the conduct prohibited is analogous to that of 'breaking and entering'"—not "using a computer (similar to the use of a gun) in committing the offense." H.R. Rep. No. 98–894, U.S.C.C.A.N. 3689, 3706 (1984). As an example of the conduct

Congress intended to prohibit, the Report identified an incident involving an individual who had "stole[n] confidential software" from a previous employer "by tapping into the computer system of [the] previous employer from [a] remote terminal." *Id.* at 3691–92. The individual would have escaped federal prosecution—despite a clear computer break-in—had he not made two of his fifty access calls from across state lines. *Id.* The Report called for a statutory solution to ensure that such computer intrusions would not evade prosecution.

Two years later, Congress extended the prohibition on unauthorized access to any "protected computer" under section 1030(a)(2)(C). And again, Congress characterized its intent as prohibiting computer break-ins. *Valle*, 807 F.3d at 525. As another example of the conduct targeted by this broadened language, the 1986 Senate Committee Report cited an adolescent gang that "broke into the computer system at [a cancer center] in New York." The group "gained access to the radiation treatment records of 6,000 past and present cancer patients" and thus "had at their fingertips the ability to alter the radiation treatment levels that each patient received." S. Rep. No. 99-432, 1986 U.S.C.C.A.N. 2479, 2480. It was this sort of technical, exploitative behavior—breaking into a computer system for the purpose of accessing or altering non-public information—that Congress sought to outlaw.

B. The CFAA Must Be Interpreted Narrowly and in Accordance with the Technical Meaning of its Terms.

By enacting the CFAA, Congress sought to address a narrow problem, not

create "a sweeping Internet-policing mandate." *See Nosal I*, 676 F.3d at 858. But Congress passed the CFAA when the internet was in its infancy, and its attempt to take on computer breaks-ins so early in the internet's lifecycle resulted in a vague and ill-defined statute. To avoid converting the CFAA into an overly broad policing tool, courts must interpret the statute in light of its core purpose.

Courts should take particular care in interpreting the meaning of "authorized access." While the CFAA defines "exceeds authorized access," it does not define its most critical term: access "without authorization." At the start of 1986, the total number of networks connected via the internet was a mere 2,000. Accessing another person's computer was relatively rare.[8] Today, more than 95 percent of U.S. adults use the internet.[9] It's possible to check your email—and thus access information on a distant server, *i.e.*, someone else's computer—from a remote campsite, at 30,000 feet above sea level or deep underwater, and even from low Earth orbit.[10] In a world where it is difficult to go a single day, or even sometimes a single waking hour, without "accessing" someone else's computer system, the precise meaning of "without authorization . . . has proven to be elusive.'" *See EF Cultural Travel BV v.*

---

[8] COMPUTER HISTORY MUSEUM, *Internet History 1962 to 1992*, http://www.computerhistory.org/internethistory/1980s/.

[9] PEW RESEARCH CENTER, *Internet, Broadband Fact Sheet* (November 20, 2025), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.

[10] Adrienne LaFrance, *The Internet in Space? Slow as Dial-Up*, THE ATLANTIC (June 11, 2015), https://www.theatlantic.com/technology/archive/2015/06/the-internet-in-space-slow-dial-up-lasers-satellites/395618/.

Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001).

Fortunately, the U.S. Supreme Court and this Court have provided guidance, instructing courts to apply the "narrow," "technical meaning" of important undefined terms like "access." In *Van Buren v. United States*, the Supreme Court interpreted the CFAA—specifically the terms "exceeds authorized access" and "entitled to obtain"—in light of terms' technical meanings. *Van Buren*, 593 U.S. at 381–89. The Supreme Court used the "technical meaning[s]" of these terms and rejected broader interpretations, because "when a statute, like this one, is 'addressing a…technical subject, a specialized meaning is to be expected.'" *Id.* at 387 & n.7 (quoting A. Scalia & B. Garner, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 73 (2012)). Thus, for the CFAA, the technical meaning *is* the plain meaning. *Id*. at 388 ("That reading, moreover, is perfectly consistent with the way that an 'appropriately informed' speaker of the language would understand the meaning.") (citation omitted).

Accordingly, the Supreme Court explained that the phrase "entitled so to obtain" should be construed in the context of computer use, and that this "narrowed scope of 'entitled'" referred to "a computer one is authorized to access." *Id*. at 386–87. Van Buren had technical authorization to access the computer, and thus the "entitlement" to obtain information from the database for purposes of the CFAA, regardless of non-technical policies and prohibitions against obtaining the

information at issue. *Id.* at 387–88, 395–96. In further support of its holding, the majority also relied on the "well established" meaning of "access" in the computing context: "'access' references the act of entering a computer 'system itself' or a 'particular part of computer system,' such as files, folders, or databases." *Id*. at 388.

This case concerns a separate provision of the CFAA that prohibits access "without authorization." Unlike "exceeds authorized access," the term "without authorization" has no statutory definition. Courts thus interpret this provision of the CFAA in light of the "specialized," technical meaning of "access." *hiQ*, 31 F.4th at 1195 n.13 (citing *Van Buren*, 593 U.S. at 388).

As this Court explained in *hiQ Labs*, *Van Buren* held that the "without authorization clause ... protects computers themselves by targeting so-called outside hackers—those who acces[s] a computer without any permission at all." *hiQ Labs*, 31 F.4th at 1198 (quoting *Van Buren*, 593 U.S. at 389) (alterations original). Liability under the "without authorization" clause thus "'stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.'" *Id.* (quoting *Van Buren*, 593 U.S. at 390).

Only by circumventing an authentication gate, then, can someone access a computer "without authorization" in the technical sense. Using this interpretation, this Court correctly held that since hiQ accessed "[p]ublic LinkedIn profiles,

available to anyone with an Internet connection…the concept of 'without authorization' is inapt." *hiQ Labs*, 31 F.4th at 1198. As the Court explained in *hiQ Labs*,

> Van Buren's distinction between computer users who "can or cannot access a computer system," suggests a baseline in which there are "limitations on access" that prevent some users from accessing the system (i.e., a "gate" exists, and can be either up or down). The Court's "gates-up-or-down inquiry" thus applies to…two categories of computers we have identified: if authorization is required and has been given, the gates are up; if authorization is required and has *not* been given, the gates are down. As we have noted, however, a defining feature of public websites is that their publicly available sections lack limitations on access; instead, those sections are open to anyone with a web browser. In other words, applying the "gates" analogy to a computer hosting publicly available webpages, that computer has erected no gates to lift or lower in the first place. *Van Buren* therefore reinforces our conclusion that the concept of "without authorization" does not apply to public websites.

Id. at 1198–99 (citation and footnote omitted).[11]

II. DEVELOPERS CANNOT BE HELD LIABLE FOR USERS' ACCESS TO A WEBSITE.

Perplexity cannot be liable under the CFAA, because it never "accessed" Amazon's servers. "In the computing context, 'access' references the act of entering

[11] Similarly, Section 502 of the California Penal Code defines "access" as "to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with" a computer. *See* Cal. Penal Code § 502(b)(1). Section 502 "is 'different' than the CFAA," and its definition of "access" does not control the meaning of this term under the CFAA. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016). However, it does define the term as it applies to Amazon's Section 502 claim.

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. As explained above, use of the Comet browser never causes *Perplexity* to access or "enter" Amazon's computers. Instead, when a user accesses an Amazon webpage using Comet, the browser—running on the user's computer—obtains the content of the page from Amazon. Perplexity's servers do not receive any information about the page unless the user asks the Assistant to take an action on the page. Even then, Perplexity's servers only receive information from the user's computer. Thus, only the user can be reasonably understood to have accessed or "entered" an Amazon computer to obtain information. In other words, Perplexity does not "access" Amazon; Amazon users do.

This alone requires reversal.

III. ENABLING ACCESS TO AND ENGAGEMENT WITH PUBLICLY AVAILABLE INFORMATION ON THE INTERNET CANNOT GIVE RISE TO CFAA LIABILITY.

There is another fatal problem with the district court's analysis contains: most Amazon webpages are publicly available online. "[T]he concept of 'without authorization' does not apply to public websites." *hiQ Labs*, 31 F.4th at 1199. A user can only access a computer "without authorization" by breaching "'limitations on access' that prevent some users from accessing the system." *Id.* In other words, a "gate" must exist, and it must be down. *Id.* "A defining feature of public websites is

that their publicly available sections lack limitations on access; instead, those sections are open to anyone with a web browser. In other words, applying the 'gates' analogy to a computer hosting publicly available webpages, that computer has erected no gates to lift or lower in the first place." *Id.* Thus, in *hiQ Labs*, this Court correctly held that accessing publicly available LinkedIn profiles after receiving a cease-and-desist letter from LinkedIn did not violate the CFAA's prohibition on accessing a computer "without authorization," because no access permissions, such as username and password requirements, were necessary to access the information. *Id.* at 1195, 1201.

Here, like the plaintiff in *hiQ Labs*, Perplexity cannot have circumvented a "gate" preventing access, because there is no gate at all. To be clear, a public webpage does not become "password-protected" simply because a user happened to be logged into their account when browsing it. If this were true, the public LinkedIn profiles would have been considered "secured" had a user been logged into LinkedIn when they accessed them, but the logic of the case does not permit such a result. Instead, it is simply irrelevant whether someone had entered login credentials that were not required.

Accordingly, the district court's reliance on *Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058 (9th Cir. 2016), rather than *hiQ Labs*, was incorrect. As the Court explained in *hiQ Labs*, the decision in *Power Venures* applies only to

data that a company protects by requiring users to log in to access, not data "available to anyone with a web browser." *hiQ Labs*, 31 F.4th at 1199. The defendant in *Power Ventures* was a platform that, with the user's permission, aggregated a user's social networking information, allowing them to view on one page updates from their "friends" on multiple social media platforms. *Power Ventures*, 844 F.3d at 1062. The platform then used users' private Facebook data to send promotional emails advertising its site, with the user's consent, despite receiving a cease-and-desist letter form Facebook. *Id.* at 1063. That "access to password-protected Facebook member profiles" distinguishes this case from those "in which information is 'presumptively open to all comers.'" *hiQ Labs*, 31 F.4th at 1199 (quoting *Facebook Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1028 (N.D. Cal. 2012)). Thus, *hiQ Labs*, not *Power Ventures*, controls where the user has accessed publicly available portions of Amazon's site.

IV. THE DISTRICT COURT'S EXPANSIVE INTERPRETATION OF THE CFAA WOULD THREATEN THE OPEN INTERNET, CHILL THE CREATION OF VALUABLE TOOLS AND SERVICES, AND IMPEDE COMPETITION.

Congress enacted the CFAA to deter harmful attacks on computers and systems. Broadly interpreted, however, it can be a weapon against scrutiny and accountability when well-resourced companies, governments, and other powerful actors wish to prevent criticism, competition, and follow-on innovation. The district court's expansive interpretation of the CFAA creates such a weapon.

A. The District Court's Overbroad Application of the CFAA Is Antithetical to Foundational Principles of the Open Internet.

Ensuring that the CFAA remains limited to its original purpose is not merely important as a matter of principle; it is necessary to ensuring that the statute cannot be used to undermine a hallmark of today's internet—open access to publicly available information.[12]

The web is the largest, ever-growing data source on the planet. It's a critical resource for journalists, academics, businesses, and everyday people alike. It offers "the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge." *Packingham*, 582 U.S. at 107.

Tools like web browsers serve as portals to those sources, including browsers that automate and expedite the process of accessing, collecting and analyzing public information. Threatening the development and use of these tools undermines free and unrestricted access to data published on the open web.

B. The Threat of Expanded Criminal Liability Would Deter the Development of Myriad Beneficial Tools and Services.

The district court's interpretation of the CFAA threatens potential *criminal* liability for developers who make these valuable tools available to users. This would

[12] *See* Orin S. Kerr, *Norms of Computer Trespass,* 116 COLUM. L. REV. 1143, 1161–63 (2016).

make the risks of providing these tools to the public would be untenable for all by the well-resourced, the reckless, and the ignorant.

Companies have already threatened small companies that offer alternative browsers that allow users to customize their own user experience to better meet their needs. For example, in 2020, Facebook sent a cease-and-desist letter to the developers of the Friendly Social Browser, threatening liability under state and federal anti-hacking laws, simply for providing a tool that modifies the experience of visiting Facebook.[13] Facebook's position, much like Amazon's here, would create the risk of near-universal liability for the developers of any tool that allows users to browse the web or alters the look or function of a website in any way. Such a rule would give websites the power to forbid commonly used tools like password managers, screen readers, and accessibility features for users with visual impairments and other disabilities.

Imposing CFAA liability for accessing publicly available information via automated scripts would potentially criminalize all automated "scraping" tools—including societally valuable tools on which internet users, researchers, and journalists around the world rely every day. Automated scraping is the process of using internet "bots" to extract content and data from a website. These bots are an

[13] Letter from attorneys Andrew Crocker and Mitch Stoltz regarding Facebook Cease and Desist Letter to Friendly App Studios LLC (Nov. 20, 2020), available at https://www.eff.org/files/2020/11/20/eff_letter_to_facebook_re_friendly.pdf.

essential component of the internet. Amazon's position will potentially criminalize—and therefore undoubtedly chill[14]—many of these automated tools, and make it even more difficult for smaller companies to create new automated tools for accessing publicly available information.

Web crawlers power tools we all rely on every day, such as Google Search. News aggregation tools, including Google's Crisis Map, which aggregates critical emergency information, are Internet bots.[15] Archival tools like the Internet Archive's Wayback Machine also require bots that scrape public online content.[16]

Journalists, researchers, and watchdog organizations, also (increasingly) rely on automated tools including scrapers to support their work, much of which is protected First Amendment activity. For investigative journalists, scraping is "one of the most powerful techniques for data-savvy journalists who want to get to the story first, or find exclusives that no one else has spotted."[17] ProPublica journalists,

---

[14] *See* Letter from Computer Security Experts to Congress and Members of the Senate and House Committees on the Judiciary (Aug. 1, 2013), https://www.eff.org/document/letter-def-con-cfaa-reform ("Many of our colleagues, and many of us, have directly experienced the chilling effects of the CFAA….[T]he mere risk of litigation or a federal prosecution is frequently sufficient to induce a researcher (or their educational or other institution) to abandon or change a useful project. Some of us have jettisoned work due to legal threats or fears.").

[15] *See* GOOGLE, *Crisis Map Help: About Google Crisis Map* (2017), https://support.google.com/crisismaps.

[16] *See* INTERNET ARCHIVE, *User Agent: archive.org_bot*, https://archive.org/details/archive.org_bot?tab=about.

[17] LEANPUB, *Scraping for Journalists (2nd edition)* https://leanpub.com/scrapingforjournalists.

for example, investigated Amazon's algorithm for ranking products by price via a "software program that simulated a non-Prime Amazon member" and "scraped…product listing page[s]"; their research uncovered that Amazon's pricing algorithm was hiding the best deals from many of its customers.[18]

Online discrimination researchers also rely on automated access tools for audit testing. One recent study of racial discrimination on Airbnb—which found that distinctively African American names were 16 percent less likely to be accepted relative to identical guests with distinctively white names—"sent inquiries to Airbnb hosts using web browser automation tools" and "collected all data using scrapers[.]"[19] Discrimination research has historically proven necessary for ensuring compliance with federal and state anti-discrimination laws,[20] and testing websites is no different—it just requires different tools, like scraping, to accomplish.

Finally, open access to academic research and scholarship—which includes "non-restrictively allowing researchers to use automated tools to mine the scholarly

---

[18] Julia Angwin and Surya Mattu, *How We Analyzed Amazon's Shopping Algorithm*, PROPUBLICA (Sep. 20, 2016), https://www.propublica.org/article/how-we-analyzed-amazons-shopping-algorithm.

[19] Benjamin Edelman, Michael Luca, & Dan Svirsky, *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, 9 AMERICAN ECONOMIC JOURNAL: APPLIED ECONOMICS 1, at 1, 7 (Apr. 2017), available at https://www.aeaweb.org/articles?id=10.1257/app.20160213.

[20] Offline, audit testing has long been recognized as a crucial way to uncover racial discrimination in housing and employment and to vindicate civil rights laws, particularly the Fair Housing Act and Title VII's prohibition on employment discrimination. *Cf. Havens Realty Corp v. Coleman*, 455 U.S. 363, 373 (1982).

literature"—has "ensur[ed] rapid and widespread access to research findings such that all communities have the opportunity to build upon them and participate in scholarly conversations."[21] And because open access to academic scholarship leads to more media coverage, including via social media, open access allows for broader societal impact.[22]

Imposing potential CFAA liability for automated access will chill the development and availability of these societally valuable research tools. To avoid the threat of criminal prosecution, companies may stop building or making available the tools that necessary for constitutionally protected research, reporting, archiving, and other socially important activities.

C. Granting Website Owners the Power to Police Internet Access Tools Would Undermine Competition.

The CFAA is an anti-hacking statute—not a tool for the world's largest company to thwart competition and consumer choice. But if unauthorized access can be predicated simply on a violation of a website owner's stated preferences, rather than hacking technological barriers, companies will inevitably use the CFAA to fend off competition.

For example, comparison shopping tools help customers more easily compare

---

[21] Jonathan P. Tennant, et al., *The Academic, Economic and Societal Impacts of Open Access: An Evidence-Based Review,* F1000RESEARCH (2016), https://f1000research.com/articles/5-632/v3.
[22] *Id.*

prices for a product sold by multiple online retailers, allowing them to find the best deal, often from retailers they may not have otherwise considered.[23] And AI agents can be particularly powerful tools in this regard, because they can process vast amounts of information from numerous sites quickly, on demand.[24] As a result, consumer may become less reliant on familiar sites like Amazon, and purchase from competitors instead.

For decades, companies have tried to use the CFAA to shut down comparison shopping tools. *See, e.g., Southwest Airlines v. Farechase*, 318 F. Supp. 2d 435, 437 (N.D. Tex. 2004); *Ryanair DAC v. Booking.com B.V.*, 2025 WL 266631, at *1 (D. Del. Jan. 22, 2025); *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 966 (N.D. Cal. 2013). And consumers quite literally pay the price. For example, undermining airfare comparison services allowed airlines like Southwest to significantly increase prices—sometimes by more than 20 percent—costing consumers an estimated $7.3 billion per year.[25] Companies thus have powerful incentives to capitalize on

---

[23] Michael Adu Kwarteng, et al., *The Influence of Price Comparison Websites on Online Switching Behavior: A Consumer Empowerment Perspective*, *in* 12066 LECTURE NOTES IN COMP. SCI. 216, 217, 219 (2020), accessible at https://pmc.ncbi.nlm.nih.gov/articles/PMC7134266/.

[24] Beth Stackpole, *Agentic AI, Explained,* MIT SLOAN SCHOOL OF MANAGEMENT (Feb. 18, 2026), https://mitsloan.mit.edu/ideas-made-to-matter/agentic-ai-explained.

[25] Charles Duan, *Hacking Antitrust: Competition Policy and the Computer Fraud and Abuse Act*, 19 COLO. TECH. L. J. 313, 328–30 (2021). Accessible at https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=3181&context=facsch_lawrev.

ambiguities in the CFAA to impede competition, at consumers' expense.

Amazon itself offers an AI shopping agent, "Rufus."[26] But Rufus only provides information about products sold on Amazon and does not allow users to compare prices or products across sites. Comet's similar shopping tool naturally threatens Amazon's ability to control what its users see, and Amazon can make Comet much less useful by forcing it to exclude Amazon—the world's largest seller[27]—from its results.

The risk is not confined to shopping tools. Companies commonly use automated web browsing products to gather web data for a wide variety of uses. Some examples from industry include manufacturers tracking the performance ranking of products in the search results of retailer websites, companies monitoring information posted publicly on social media to keep tabs on issues that require customer support, and businesses staying up to date on news stories relevant to their industry across multiple sources. E-commerce businesses use automated web browsing to monitor competitors' pricing and inventory, and to aggregate information to help manage supply chains. Businesses also use automated web

[26] AMAZON, *Meet Rufus*, https://www.amazon.com/Rufus/b?ie=UTF8&node=1212 14013011.

[27] Amazon is now the world's largest company, measured by sales. Alina Selyukh, *Amazon Dethrones Walmart as the World's Biggest Company by Sales*, NPR (Feb. 19, 2026), https://www.npr.org/2026/02/19/nx-s1-5719173/amazon-walmart-biggest-company-by-sales.

browsers to monitor websites for fraud, perform due diligence checks on their customers and suppliers, and to collect market data to help plan for the future. Narrowly interpreting the CFAA, in accordance with the technical meaning of its terms, is essential to help reduce anticompetitive uses.

V. THE DISTRICT COURT ERRED IN CONFLATING ITS MERITS DETERMINATION WITH THE PUBLIC INTEREST.

The district court compounded its erroneous determination on the merits by allowing that determination to swallow the rest of the preliminary injunction analysis, particularly competing public interests.

A preliminary injunction is an extraordinary remedy never awarded as of right. *Munaf v. Geren*, 553 U.S. 674, 689–690 (2008). Instead, courts must apply "traditional equitable considerations," and may not presume "that an injunction automatically follows" from a finding of liability. *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 392–93 (2006). And, "in exercising their sound discretion, courts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction." *Weinberger v. Romero–Barcelo*, 456 U.S. 305, 312 (1982); *see also Railroad Comm'n of Tex. v. Pullman Co.*, 312 U.S. 496, 500 (1941).

The district court did not heed that instruction. Instead, it did precisely what *eBay* forbids: assumed that its (incorrect) finding of likely liability necessarily meant an injunction would serve the public interest because "the public has an interest in

protecting computers from unauthorized access." Order at 5–6. If conflating factors one and four is impermissible with respect to a *permanent* injunction following a *final* determination of liability, it is even more inappropriate at this early stage in the case.

As discussed above, the CFAA is commonly deployed not to address hacking, but rather to inhibit competition, follow-on innovation, and consumer choice. As numerous courts have held, innovation and consumer choice are quintessential public interests. *See Int'l Jensen, Inc. v. Metrosound U.S.A., Inc.*, 4 F.3d 819, 827 (9th Cir. 1993) (affirming denial of preliminary injunction where injunction would have "depriv[ed] consumers of a choice of products"); *see also Epic Games, Inc. v. Apple Inc.*, 2021 WL 5205487, at *2 (N.D. Cal. Nov. 9, 2021) ("consumer choice is in the interest of the public"); *Wagner Aeronautical, Inc. v. Dotzenroth*, 2022 WL 6837701, at *10 (S.D. Cal. Oct. 7, 2022) ("Preserving and protecting innovation . . . is clearly in the public's interest."). Accordingly, courts weighing CFAA claims must be scrupulous in requiring plaintiffs to meet their burden of showing that an injunction will serve the public interest. The district court was not.

CONCLUSION

For the reasons stated above, we urge the Court to reverse the decision below.

Dated: April 8, 2026

By: /s/ *Corynne McSherry*
Corynne McSherry

Victoria Noble
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993
corynne@eff.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amici Curiae Electronic Frontier Foundation, Alliance for Responsible Data Collection, Mozilla Corporation, Digital Medusa, and EleutherAI in Support of Defendant-Appellant and Reversal with the type-volume limitation of Fed. R. App. P. 32(a)(5) because this brief contains 5,767 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: April 8, 2026

By: /s/ *Corynne McSherry*
Corynne McSherry

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate ACMS system on April 8, 2026.

I certify that all participants in the case are registered ACMS users and that service will be accomplished by the appellate ACMS system.

Dated: April 8, 2026

By: /s/ *Corynne McSherry*
Corynne McSherry

Counsel for Amici Curiae