NO. 17-16783

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

HIQ LABS, INC.,

PLAINTIFF-APPELLEE,

V.

LINKEDIN CORPORATION,

DEFENDANT-APPELLANT.

On Remand from The United States Supreme Court
No. 19-1116

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION AND INTERNET ARCHIVE IN SUPPORT OF PLAINTIFF-APPELLEE AND AFFIRMANCE

Aaron Mackey
Mukund Rathi
Kurt Opsahl
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: amackey@eff.org
Telephone: (415) 436-9333

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, Amici Curiae Electronic Frontier Foundation and Internet Archive each individually state that they do not have a parent corporation and that no publicly held corporation owns 10 percent or more of their stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the digital world. With more than 30,000 active donors and dues-paying members, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age. EFF's interest in this case is in the principled and fair application of computer crime laws generally, and the Computer Fraud and Abuse Act ("CFAA") specifically, 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 engaged in cutting-edge exploration of technology whose work in the public interest may be unjustly chilled by laws including the CFAA. EFF has also served as counsel or amicus curiae in key cases addressing the CFAA and/or state computer crime statutes, including *Van Buren v. United States*, 141 S.Ct. 1648 (2021) (amicus); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) ("*Nosal I*") (en banc) (amicus); *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016) ("*Nosal II*") (amicus); *Facebook, Inc. v. Power*

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), no one except for Amici or their counsel authored this brief in whole or in part, or contributed money towards its preparation. Both parties consent to this brief's filing.

Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016) (amicus); *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015) (amicus); and *United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (co-counsel).

The Internet Archive is a public nonprofit organization founded in 1996 to build an "Internet library," with the purpose of offering researchers, historians, scholars, artists, and the general public permanent access to historical collections in digital format. Located in San Francisco, California, the Internet Archive receives data donations and collects, records, and digitizes material from a multitude of sources, including libraries, educational institutions, government agencies, and private companies. The Internet Archive then provides free public access to its data—which include text, audio, video, software, and archived Web pages. The Internet Archive's Wayback Machine uses automated tools to capture, index, and make public historic versions of websites for the benefit of researchers, historians, and all internet users.

INTRODUCTION

Van Buren v. United States, 141 S.Ct. 1648 (2021) confirms that this Court correctly held that scraping a publicly accessible website does not violate the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §1030. The Supreme Court's interpretation of the CFAA's text, structure, and purpose, forecloses LinkedIn's effort to "turn a criminal hacking statute into a 'sweeping Internet-policing mandate.'" *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003 (9th Cir. 2019) (quoting *Nosal I*, 676 F.3d at 858), *cert. granted, judgment vacated*, No. 19-1116, 2021 WL 2405144 (June 14, 2021).

EFF and fellow amici previously filed a brief with this Court because they were concerned that a broad interpretation of the CFAA would chill a wide range of valuable tools, services, and research online. *See* Br. of Amici Curiae Electronic Frontier Foundation, DuckDuckGo, and the Internet Archive (Dkt. 42) ("EFF Br."). The legitimate activities threatened by a broad interpretation include the use of "good Internet bots" that collect, aggregate, and index publicly available information, as well as the work of journalists, researchers, and watchdog organizations, who use automated tools to find stories and investigate discrimination online. *Id*. at 19-24.

This Court was right to avoid an outcome that would have curtailed those legitimate activities and to hold that where "access is open to the general public,

the CFAA 'without authorization' concept is inapplicable." *hiQ*, 938 F.3d at 1000. EFF and the Internet Archive (collectively, "Amici") file this brief to explain why *Van Buren* supports this Court's conclusion and to ensure that the CFAA is not misused to jeopardize those valuable activities online.

ARGUMENT

I. *VAN BUREN* SUPPORTS THIS COURT'S HOLDING THAT THE CFAA DOES NOT APPLY TO PUBLICLY ACCESSIBLE INFORMATION ONLINE

Van Buren reinforces this Court's holding that the CFAA does not proscribe accessing publicly available information on a website that anyone with an Internet connection can view. This Court held that the CFAA "contemplates three kinds of computer information:" (1) generally accessible public information for which permission is not required; (2) information requiring authorization to access, when such authorization has been given; and (3) information requiring authorization to access, when authorization has not been given, either generally or specifically to a part of a system. *hiQ*, 938 F.3d at 1001-02. *Van Buren* dealt with a subset of the third kind—"information for which authorization is required but has not been given … for the part of the system accessed." *See id*. Thus, *Van Buren*'s interpretation of the CFAA's text supports this Court's earlier conclusion that the statute's prohibitions do not apply when websites do not impose access controls (i.e., an "authorization" system) that prevent the public from viewing information

contained on those sites.

Van Buren's holding rested on the Supreme Court's interpretation of the statute's definition of "exceeds authorized access" and the specific phrase, "entitled so to obtain." *Van Buren*, 141 S.Ct. at 1654-58 ("[W]e start where we always do: with the text of the statute."). 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 1657, 1658 n.7 (internal citation omitted). Thus, for the CFAA, the technical meaning *is* the plain meaning. *Id*. at 1657 ("That reading, moreover, is perfectly consistent with the way that an 'appropriately informed' speaker of the language would understand the meaning.") (internal citation omitted).

In light of the CFAA's technical terms, the Supreme Court held that *Van Buren* did not violate the statute because he was "entitled so to obtain" information from the law enforcement database he searched. This was because the "narrowed scope of 'entitled'" encompassed only the use of "a computer one is authorized to access." *Id*. at 1657. Van Buren had that authorization, and thus the entitlement to obtain information from the database. 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*.

This case concerns a separate provision of the CFAA that prohibits access "without authorization." Unlike "exceeds authorized access," "without authorization" has no statutory definition. *Van Buren*'s instruction that the CFAA should be interpreted in light of its "technical meaning" should thus apply. *See id*. at 1657. This Court has interpreted the CFAA this way before. *Nosal I* anticipated *Van Buren*'s "reading of 'entitled' as a synonym for 'authorized'" and its recognition of the CFAA's focus on hacking, or "the circumvention of technological access barriers." *See* 676 F.3d at 857, 863.

Turning to technical meaning, "authorization" is not a catch-all term for "permission," but refers to "[a] process by which users, having completed an authentication stage, gain or are denied access to particular resources based on their entitlement." *A Dictionary of Computer Science* 32 (7th ed. 2016). Only by circumventing an authentication stage, 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*, 983 F.3d at 1002.

II. *VAN BUREN* FORECLOSES CFAA INTERPRETATIONS THAT RELY ON NON-TECHNICAL DEFINITIONS OR PROPERTY LAW

The Supreme Court's use of technical meanings and its rejection of other

interpretive tools when construing the CFAA foreclose LinkedIn's reliance on them here to claim hiQ accessed its website without authorization.

Van Buren undermines LinkedIn's reliance on previous decisions by this Court that have interpreted the CFAA's terms in a non-technical manner which stretches the meaning of "without authorization" to include accessing a computer without permission. LinkedIn Supp. Br. at 7; *Nosal II*, 844 F.3d at 1028.

This Court previously distinguished *Nosal II*, which dealt with access requiring user accounts and passwords, rather than a publicly available website in which prior authorization is not required. *hiQ*, 983 F.3d at 1000. That distinction remains correct. But *Van Buren* goes further, instructing courts not to interpret the plain meaning of the CFAA's terms in a non-technical manner.

Using technical definitions to interpret the "without authorization" clause leads to the same result of this Court's previous decision, albeit with a more direct route that focuses on the statute's text. And because that interpretation aligns with the CFAA's purpose as an anti-hacking statute, it avoids chilling beneficial internet activity. *See* EFF Br. 19-24.

Van Buren also counsels against relying on property law concepts, including analogies to physical trespass, rather than defining authorization according to its technical meaning. The *Van Buren* majority found the dissent's broader interpretation of "entitled," which included circumstance-specific conditions and

rested on "basic principles of property law" and "common-law," to be "ill advised," given the CFAA's focus on "computer crime." *Id*. at 1655 n.4. LinkedIn's argument regarding the CFAA's "without authorization" prohibition similarly relies on circumstance-specific conditions it placed on hiQ's access, and its revocation argument echoes the *Van Buren* dissent's reliance on property law. LinkedIn Supp. Br. 20-23.

III. *VAN BUREN*'S "GATES-UP-OR-DOWN" METAPHOR COMPLEMENTS THIS COURT'S EARLIER CONCLUSION THAT THE CFAA DOES NOT APPLY TO ACCESSING A PUBLIC WEBSITE

Although the Supreme Court's holding in *Van Buren* centered on technical definitions under the CFAA, the majority also used a "gates-up-or-down" analogy to describe the statute's prohibitions. The analogy is consistent with the Court's prior holding that hiQ did not access LinkedIn's website without authorization. LinkedIn and hiQ devote much time to analyzing the "gates-up-or-down" language, so Amici will not belabor those points.

Instead, we offer these observations.

First, *Van Buren*'s gate analogy is not a textual interpretation of the CFAA, as LinkedIn argues. LinkedIn Supp. Br. 11-20. The majority's holding centered on the technical meaning of the CFAA's text. *Van Buren*, 141 S.Ct. at 1654-58. Only after the textual analysis did the majority consider the gates analogy. *Van Buren*, 141 S.Ct. at 1658; *compare id*. (describing the gates analogy as "Van Buren's

reading"), *with* LinkedIn Supp. Br. 12 (stating that "The Supreme Court held" that the analogy controlled the CFAA's interpretation). The gates analogy was useful insofar as it "align[ed] with the computer-context understanding of access as entry." *Van Buren*, 141 S.Ct. at 1659.

For the reasons explained above, that textual reading supports this Court's holding that one cannot access a publicly available website "without authorization" because those websites do not employ authentication or other systems that privilege such access. IP address blocking, as explained below, is insufficiently secure or reliable to be considered an authorization system.

Second, *Van Buren*'s gates analogy is properly understood to address the latter two categories of computer information that this Court described in its earlier holding: (a) information for which authorization is required and has been given and (b) information for which authorization is required but has not been given. *hiQ*, 938 F.3d at 1001-02. *Van Buren*'s gates analogy stemmed from the CFAA's prohibitions involving "access" and "authorization," which, when interpreted technically, presume an authentication or other system that grants or denies entry. Thus the "gate" is an analogy to that system—so under *Van Buren*, the lack of an authorization system means no gate at all.

LinkedIn incorrectly argues that the gates analogy expands the CFAA's reach, creating a binary internet in which users either do or do not have

authorization to access publicly available websites open to anyone. LinkedIn Supp. Br. 11-23. In doing so, LinkedIn misreads *Van Buren*'s statement that the CFAA's prohibitions apply "to all information from all computers that connect to the Internet." 141 S. Ct. at 1652. What the *Van Buren* majority meant is that any computer *can* use technological access barriers and authentication systems to provide "authorization" under the CFAA. As explained above, "authorization" under the CFAA is not a catch-all term for permission but requires technical systems that control entry. Moreover, if the CFAA's prohibition reaches publicly available information that anyone with internet access can view, then the statute would in fact "attach criminal penalties to a breathtaking amount of commonplace computer activity," including web scraping, rather than being "aimed at preventing the typical consequences of hacking." *Van Buren*, 141 S.Ct. at 1660-61 (internal citation omitted). This is precisely the outcome this Court and *Van Buren* sought to avoid. *See hiQ*, 983 F.3d at 1003 (the CFAA is a "criminal hacking statute," not a "sweeping Internet-policing mandate") (quoting *Nosal I*, 676 F.3d at 858).

Third, although the gates-up-or-down approach is inapt here because LinkedIn has not installed a gate, if this Court believes it must apply the analogy under *Van Buren*, the Court should hold that publicly available websites' gates are plainly up and the steps taken by LinkedIn did not lower them. The Court should clarify that closing a generally accessible public website's gates requires

technological access barriers, like "an authentication requirement, such as a password gate, [that] create[s] the necessary barrier that divides open spaces from closed spaces on the Web." *hiQ*, 983 F.3d at 1001 (quoting Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1161 (2016)).

Indeed, the *Van Buren* majority noted that its "gates-up-or-down" analogy aligned with the "CFAA's prohibition on password-trafficking," 18 U.S.C. § 1030 (a)(6), which "contemplates a 'specific type of authorization—that is, authentication,' which turns on whether a user's credentials allow him to proceed past a computer's access gate." *Id*. at 1659 n.9 (quoting Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 Geo. Wash. L. Rev. 1442, 1470 (2016)).

Although *Van Buren* left open whether "technological (or 'code-based') limitations" are necessary to lower the gate, 141 S.Ct. at 1659 n.8, this Court should require an authentication system to impose the CFAA's prohibitions in the internet context, in which billions of users access hundreds of millions of public websites. These technological access barriers are the only way to provide notice to internet users that they either have or lack authorization. Otherwise, this Court risks creating a vague statute that criminalizes average internet users. *See* EFF Br. at 19-29.

At minimum, this Court should reaffirm that LinkedIn's cease-and-desist

letter combined with its internet protocol ("IP") address blocking efforts did not amount to LinkedIn closing the gate on hiQ to create a CFAA violation. LinkedIn incorrectly asserts that IP blocking automatically qualifies as a code-based limitation. LinkedIn Supp. Br. 22. This Court previously recognized that a user blocked this way "does not receive notice" and "may never realize that the block was imposed," and so is not "without authorization." *Power Ventures*, 844 F.3d at 1068 n.5.

In any event, technologists have recognized that IP address blocks—in which one computer blocks traffic from others based on the IP addresses they use—are "a fundamentally unsecure way to control access" to a computer system or server. Simson Garfunkel and Gene Spafford, *Practical Unix and Internet Security* 484 (2d ed. 1996). Users encountering IP blocks may interpret them as errors because the blocks do not communicate anything beyond the fact that a website or service is inaccessible. Those users may then simply use a different IP address to connect to the service.

Additionally, millions of internet users change or otherwise obscure their IP addresses for a variety of legitimate and beneficial reasons. For example, many people switch their IP addresses due to online retailers' practice of using visitors' IP addresses to charge people different prices depending on their location. *See* Jennifer Valentino-Devries, Jeremy Singer-Vine and Ashkan Soltani, *Websites*

Vary Prices, Deals Based on Users' Information, Wall Street Journal (Dec. 24, 2012).[2] Internet users also rely on IP-address-changing tools, such as Virtual Private Networks and Tor, to avoid state-based censorship online, such as China's Great Firewall. *See* Paolo Zialcita, *BBC Launches Tor Mirror Site to Thwart Media Censorship*, NPR (Oct. 24, 2019).[3] Indeed, Apple recently announced a Private Relay feature that will change users' IP addresses automatically. Dan Patterson, *Apple unveils new privacy features in iOS 15 and other products*, CBS News (June 10, 2021);[4] Chaim Gartenberg, *How to use Apple's Private Relay feature with iCloud Plus*, The Verge (July 12, 2021).[5]

Switching IP addresses thus does not require much, if any technical expertise, and internet users frequently rely on them for a variety of reasons that are neither improper nor unlawful. LinkedIn is thus wrong to elevate IP address blocking into an access restriction that rendered hiQ's scraping without authorization under the CFAA.

---

[2] https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[3] https://www.npr.org/2019/10/24/773060596/bbc-launches-tor-mirror-site-to-thwart-media-censorship.

[4] https://www.cbsnews.com/news/apple-privacy-iphone-ios15/.

[5] https://www.theverge.com/22573519/apple-private-relay-icloud-plus-ios-15-ipados-macos-monterey-how-to.

IV. CONGRESS MUST ADDRESS LEGITIMATE CONCERNS ABOUT MISUSING PERSONAL DATA VIA PRIVACY LAWS, RATHER THAN COURTS STRETCHING THE CFAA IN WAYS THAT WILL CRIMINALIZE INTERNET USERS

LinkedIn is right to recognize the threat to individual privacy posed by actors who obtain personally identifying information and misuse it to harm people, but it is wrong to ask this Court to remedy those harms by expanding the CFAA, an anti-hacking statute. *See* LinkedIn Supp. Br. 18-19, 23-26. Although computer intrusions can result in bad actors accessing sensitive personal information, the CFAA's prohibitions turn on accessing computer systems without or in excess of authorization, not on the content of the information beyond those access controls.

Thus, this Court and others have described the CFAA "as an anti-intrusion statute and not as 'a misappropriation statute.'" *See hiQ*, 938 F.3d 1000 (quoting *Nosal I*, 676 F.3d at 857-858); *Valle*, 807 F.3d at 525.

Indeed, *Van Buren* rejected an effort by the government to turn the CFAA into a data privacy statute. There, Van Buren abused his authority as a law enforcement officer and obtained a woman's private information through a law enforcement database. 141 S.Ct. 1653. Van Buren undoubtedly violated the woman's privacy, but the Supreme Court reversed his CFAA conviction to ensure that the CFAA would not police downstream uses of information.[6] *Id*. at 1662. The

[6] EFF is deeply concerned with law enforcement personnel's misuse of sensitive information contained in police databases. EFF has demanded that the California

purpose-based restrictions that Van Buren violated "can be expressed as either access or use restrictions," and would allow private parties and the government to create fine distinctions and leverage the CFAA by categorizing downstream misuse as an access restriction. *Id*.

LinkedIn seeks to use the CFAA to police how certain parties use publicly available information posted by users on its website. As explained in detail in Amici's prior brief, there are many legitimate and beneficial reasons for third parties to scrape public websites. EFF Br. at 19-24. LinkedIn's interpretation threatens to ensnare those legitimate activities in the CFAA while also running counter to the textual and structural analysis provided by the Supreme Court in *Van Buren*. The Court should once more reject LinkedIn's incorrect interpretation of the CFAA.

Rather than push for an expansive interpretation of the CFAA, a statute that is ill-suited to comprehensively protect personal privacy, LinkedIn should join EFF and other advocates pushing Congress and state legislatures to adopt consumer and biometric privacy laws that would prohibit services from collecting people's

---

Department of Justice proactively police reports of misuse, including by disciplining and terminating personnel who abuse their access. *See* Dave Maass, *EFF Pressure Results in Increased Disclosure of Abuse of California's Law Enforcement Databases*, EFF Deeplinks (March 31, 2016), https://www.eff.org/deeplinks/2016/03/eff-pressure-results-increased-disclosure-abuse-californias-law-enforcement.

sensitive information without their consent. *See* Gennie Gebhart, *EFF's Recommendations for Consumer Data Privacy Laws*, EFF Deeplinks (June 17, 2019);[7] Adam Schwartz, *Sen. Merkley Leads on Biometric Privacy*, EFF Deeplinks (Aug. 4, 2020).[8] These proposed laws directly address the privacy violations LinkedIn describes in its supplemental brief without criminalizing legitimate activity online.

CONCLUSION

For the foregoing reasons, Amici respectfully requests that this Court affirm its previous decision that hiQ did not access LinkedIn's public website without authorization.

Dated: July 16, 2021

Respectfully submitted,

By: /s/ Aaron Mackey

Aaron Mackey
Mukund Rathi
Kurt Opsahl
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
amackey@eff.org

Counsel for Amici Curiae
Electronic Frontier Foundation
and the Internet Archive

[7] https://www.eff.org/deeplinks/2019/06/effs-recommendations-consumer-data-privacy-laws.
[8] https://www.eff.org/deeplinks/2020/08/sen-merkley-leads-biometric-privacy.

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 17-16783

I am the attorney or self-represented party.

This brief contains 3,328 **words**, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one):*
  - ○ it is a joint brief submitted by separately represented parties;
  - ○ a party or parties are filing a single brief in response to multiple briefs; or
  - ○ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated _____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Aaron Mackey **Date** July 16, 2021

*(use "*s/[typed name]*" to sign electronically-filed documents)*

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

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 CM/ECF system on July 16, 2021.

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

Dated: July 16, 2021

/s/ Aaron Mackey
Aaron Mackey