No. 19-1116

IN THE

Supreme Court of the United States

LINKEDIN CORPORATION,

Petitioner,

v.

HIQ LABS, INC.,

Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

PETITIONER'S SUPPLEMENTAL BRIEF

E. JOSHUA ROSENKRANZ
ORRICK HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000

ERIC A. SHUMSKY
ORRICK HERRINGTON & SUTCLIFFE LLP
1152 15th Street, NW
Washington, DC 20005
(202) 339-8400

DONALD B. VERRILLI, JR.
Counsel of Record
JONATHAN S. MELTZER
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Avenue, NW
Suite 500E
Washington, DC 20001
(202) 220-1100
donald.verrilli@mto.com

JONATHAN H. BLAVIN
ROSEMARY T. RING
NICHOLAS D. FRAM
MARIANNA Y. MAO
MUNGER, TOLLES & OLSON LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105
(415) 512-4000

Counsel for Petitioner

ARGUMENT

Like *Van Buren v. United States*, 593 U.S. ___ (2021), this case addresses the proper interpretation of Section 1030(a)(2) of the Computer Fraud and Abuse Act of 1986 (CFAA). *Van Buren* definitively construed "exceeds authorized access" in Section 1030(a)(2), but the Court did not address the "without authorization" clause of that provision, which it characterized as "distinct." *See Van Buren*, slip op. at 12-13 & n.8. As the Petition in this case explains, there is widespread uncertainty in the lower courts regarding the meaning of "without authorization" in Section 1030(a)(2), *see* Pet. 15-20, and its proper application is an issue of manifest and increasing importance, *see* Pet. 27-32. The Court should grant the Petition now to provide complementary and equally needed guidance as to the meaning of "without authorization."

1. Section 1030(a)(2) subjects to civil or criminal liability anyone who "intentionally accesses a computer without authorization or exceeds authorized access" and thereby obtains information from the computer, so long as that computer is used in or affects interstate commerce. *See* 18 U.S.C. § 1030(a)(2), (e)(2), (e)(6); *Van Buren*, slip op. at 2. As Van Buren explained, Section 1030(a)(2)

> specif[ies] two distinct ways of obtaining information unlawfully. *First*, an individual violates the provision when he "accesses a computer without authorization." §1030(a)(2). *Second*, an individual violates the provision when he "exceeds authorized access" by accessing a computer "with authorization" and then obtaining information he is "not entitled so to obtain." §§1030(a)(2), (e)(6).

Van Buren, slip op. at 12-13. *Van Buren* construed the "exceeds authorized access" prong of the provision, and in doing so, it relied principally on the definition of that term in Section 1030(e)(6). *See* slip op. at 5-12.

This Court had no cause to address the "without authorization" clause in the statute, as both "parties agree[d] that Van Buren 'access[ed] a computer with authorization.'" *Van Buren*, slip op. at 5. And unlike "exceeds authorized access," the term "without authorization" is not defined in the statute, thereby limiting the applicability of *Van Buren*'s textual analysis to the question of what constitutes "authorization" under the statute. The Court did note, however, that its approach means that liability under both the "without authorization" and "exceeds authorized access" clauses "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.* at 13. The Court then explicitly declined to say what qualifies as a gate. Instead, it stated: "For present purposes, we need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies." *Id.* at 13 n.8.

2. This Petition addresses the precise question left open by the Court in *Van Buren*. LinkedIn put gates around its servers by employing technical "code-based" measures to prevent hiQ from scraping data (which hiQ circumvented via bots) and sending a cease-and-desist letter to hiQ, thereby expressly revoking any "authorization" hiQ had to access LinkedIn's computers. *See* Pet 10. *Van Buren* expressly left open whether these methods of denying and revoking authorization, or any other methods of doing so, qualify

as "gates-down" under Section 1030(a)(2), thus rendering hiQ's massive scraping of data "without authorization."

There is a pressing need for an answer to that question. Websites employ myriad strategies that might or might not qualify as "gates," from code-based measures such as password requirements and LinkedIn's technical blocking measures, to express communications such as cease-and-desist letters, to the contracts and policies mentioned in *Van Buren*. Even in the time during which this Petition has been pending, lower courts have continued to take divergent approaches in determining whether circumvention of these potential "gates" qualifies as accessing a website "without authorization. *See, e.g.*, *Sandvig v. Barr*, 451 F. Supp. 3d 73, 85 n.2 (D.D.C. 2020) (noting that because individualized cease-and-desist letters were not sent in that case, "the Court need not decide whether they would constitute a revocation of authorization and thereby make any further visits by the recipients to the otherwise public portions of LinkedIn a CFAA violation"); *SMH Enterprises, LLC v. Krispy Krunchy Foods, LLC*, No. 20-cv-2970, 2021 WL 1226411, at *3 (E.D. La. Apr. 1, 2021) (termination of business relationship "ended any authorization to access its servers that would have arisen by virtue of the former relationship between the companies" which "adequately alleged that [plaintiff] accessed its servers 'without authorization.'"); *Motogolf.com, LLC v. Top Shelf Golf, LLC*, No. 20-cv-00674, 2021 WL 1147149, at *5 (D. Nev. Mar. 25, 2021) (Plaintiff's argument that it revoked access to its website through the cease-and-desist letters fails because the letters do not affect the "public" website analysis); *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 129 (N.D. Cal. 2020) ("In situations where a plaintiff clearly revokes access to a party and

not simply the means, manner, or method for such access, that party may be liable under the CFAA.").

Clarifying the meaning of "without authorization," just as *Van Buren* construed "exceeds authorized access," has thus become even more necessary since the Petition was filed 15 months ago. As the Petition explains, the ability of Internet users to control their data and protect their privacy has never been more at risk, and the consequences of mass scraping of public-facing websites are extraordinarily harmful for the hundreds of millions of users of such websites. *See* Pet. 27-28 (describing Cambridge Analytica's harvesting of Facebook user information and Clearview AI's largescale scraping of user information from public-facing websites to create a facial recognition database sold to private companies and law enforcement); Pet. Reply 9; *see also*, *e.g.,* Jonathan Vanian, *Data From Half a Billion LinkedIn Users Has Been Scraped and Put Online*, Fortune Magazine (April 8, 2021), https://fortune.com/2021/04/08/linkedin-user-data-breach-leak-hackers/ (noting that data scraped from 500 million LinkedIn users was being sold online to hackers, who could use it for phishing attempts and other bad acts); *200 million Facebook, Instagram, and LinkedIn Users' Scraped Data Exposed*, Security Magazine (Jan. 12, 2021), https://www.securitymagazine.com/articles/94327-million-facebook-instagram-and-linkedin-users-scraped-data-exposed (describing a data breach at a Chinese start-up that contained scraped personal identifiable information from 214 million social media users).

In view of the metastasizing threats to the privacy of individual information stored on website servers and the paucity of legal options other than the CFAA to combat those threats, any benefit to be gained by further percolation of the question presented is more

than outweighed by the pressing need for a clear and universally applicable rule. Indeed, the consequence of uncertainty in the lower courts is particularly troubling. Because the Internet is ubiquitous, the same conduct involving the same website could be a violation of the CFAA in some parts of the country but not others. *See* Pet. 4. Companies like LinkedIn require the clarity and stability that only this Court can provide as to how they can safeguard their users' data and privacy. Just as the Court in *Van Buren* resolved an important circuit conflict regarding the meaning of Section 1030(a)(2), the Court should do the same in this case, providing a clear, nationwide rule as to what conduct qualifies as accessing information from the Internet "without authorization." 18 U.S.C. 1030(a)(2).

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

E. JOSHUA ROSENKRANZ
ORRICK HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000

ERIC A. SHUMSKY
ORRICK HERRINGTON & SUTCLIFFE LLP
1152 15th Street, NW
Washington, DC 20005
(202) 339-8400

DONALD B. VERRILLI, JR.
Counsel of Record
JONATHAN S. MELTZER
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Avenue, NW
Suite 500E
Washington, DC 20001
(202) 220-1100
donald.verrilli@mto.com

JONATHAN H. BLAVIN
ROSEMARY T. RING
NICHOLAS D. FRAM
MARIANNA Y. MAO
MUNGER, TOLLES & OLSON LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105
(415) 512-4000

Counsel for Petitioner

June 7, 2021