CASE NO. 17-16783

In the United States Court of Appeals
For the Ninth Circuit

HIQ LABS, INC.
Plaintiff-Appellee,

V.

LINKEDIN CORPORATION
Defendant-Appellant,

Appeal from the United States District Court
for the Northern District of California
The Honorable Edward M. Chen, Presiding

APPELLANT'S BRIEF ON REMAND FROM THE SUPREME COURT

MUNGER, TOLLES & OLSON LLP
JONATHAN H. BLAVIN
ROSEMARIE T. RING
NICHOLAS D. FRAM
MARIANNA MAO
560 Mission Street, 27th Floor
San Francisco, California 94105-3089
Telephone: (415) 512-4000
Facsimile: (415) 512-4077

MUNGER, TOLLES & OLSON LLP
DONALD B. VERRILLI, JR.
JONATHAN S. MELTZER
601 Massachusetts Ave. N.W., Suite 500E
Washington, DC 20001
Telephone: (202) 220-1100
Facsimile: (202) 220-2300

Attorneys for Defendant-Appellant *LinkedIn Corporation*

(additional counsel listed inside cover page)

(additional counsel continued from cover page)

ORRICK, HERRINGTON & SUTCLIFFE LLP

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

ERIC A. SHUMSKY
1152 15th Street, NW
Washington, DC 20005
(202) 339-8400

Attorneys for Defendant-Appellant *LinkedIn Corporation*

TABLE OF CONTENTS

Page

INTRODUCTION 1

THE SUPREME COURT'S *VAN BUREN* DECISION 4

ARGUMENT 6

I. *VAN BUREN* CONFIRMS THAT MAKING A WEBSITE PUBLICLY ACCESSIBLE IS A GRANT OF AUTHORIZATION UNDER THE CFAA 7

A. Under *Van Buren*'s Textual Analysis, Opening a Website to Public Access Is a Grant of Authorization 7

B. *Van Buren* Makes Clear that the Panel Erred by Disregarding Statutory Structure 13

C. Policy Considerations Counsel Against the Panel Decision's Prior Interpretation of "Without Authorization" 15

II. HIQ'S CONTINUED ACCESS TO LINKEDIN'S WEBSITE WOULD BE WITHOUT AUTHORIZATION 20

III. THE BALANCE OF THE EQUITIES AND THE PUBLIC INTEREST FAVOR LINKEDIN 23

CONCLUSION 26

TABLE OF AUTHORITIES

Page

FEDERAL CASES

Blankenhorn v. City of Orange,
485 F.3d 463 (9th Cir. 2007) 11

Craigslist Inc. v. 3Taps, Inc.,
964 F. Supp. 2d 1178 (N.D. Cal. 2013).....13, 14, 16, 17

EF Cultural Travel BV v. Zefer Corp.,
318 F.3d 58 (1st Cir. 2003).....9

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

hiQ Labs, Inc. v. LinkedIn Corp.,
938 F.3d 985 (9th Cir. 2019), ...passim

Lawrence ex rel. Lawrence v. Chater,
516 U.S. 163 (1996).....1

LinkedIn Corp. v. hiQ Labs, Inc.,
No. 19-1116, 2021 WL 2405144 (U.S. June 14, 2021).....1, 2

LVRC Holdings LLC v. Brekka,
581 F.3d 1127 (9th Cir. 2009) 6, 10, 12

Marx v. General Revenue Corp.,
568 U.S. 371 (2013).....15

Roberts v. Sea-Land Services, Inc.,
566 U.S. 93 (2012).....6

Sandvig v. Barr,
451 F. Supp. 3d 73 (D.D.C. 2020).....14

United States v. Nosal (*Nosal I*),
676 F.3d 854 (9th Cir. 2012) 16

United States v. Nosal (*Nosal II*),
844 F.3d 1024 (9th Cir. 2016) 10, 14

TABLE OF AUTHORITIES
(Continued)

Page

Van Buren v. United States,
141 S. Ct. 1648 (2021) ..... passim

FEDERAL STATUTES

18 U.S.C. § 1030 ..... passim

18 U.S.C. § 2511 14

18 U.S.C. § 2701 *et seq.* 14

OTHER AUTHORITIES

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 19

Jonathan Vanian, *Data from Half a Billion LinkedIn Users Has Been Scraped and Put Online*, Fortune Magazine (Apr. 8, 2021), https://fortune.com/2021/04/08/linkedin-user-data-breach-leak-hackers/ 19

Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. Times (Mar. 7, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html 18

Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html 18

Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, N.Y. Times (Jan. 22, 2020) https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html 25

TABLE OF AUTHORITIES
(Continued)

Page

LinkedIn Data of 500 Million Users Hacked, Up For Sale: Report, The Quint (Apr. 23, 2021) https://www.thequint.com/tech-and-auto/data-of-500-million-linkedin-users-for-sale-on-a-site-report.....19

Matthew Rosenberg & Sheera Frankel, *Facebook's Role in Data Misuse Sets off Storms on Two Continents*, N.Y. Times (Mar. 18, 2018) https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html 24

Random House Unabridged Dictionary (2nd ed. 2001) 10

The Oxford English Dictionary (2d ed. 1989).....10, 11

The Random House Dictionary of the English Language (2d ed. 1987) 10, 11

Webster's Third New International Dictionary (1986) 10, 11

INTRODUCTION

On June 3, 2021, the Supreme Court decided *Van Buren v. United States*, 141 S. Ct. 1648 (2021), and on June 14, 2021, it granted LinkedIn's petition for certiorari, vacated this Court's prior decision and remanded for reconsideration in light of *Van Buren*. *See LinkedIn Corp. v. hiQ Labs, Inc.*, No. 19-1116, 2021 WL 2405144 (U.S. June 14, 2021). That was a significant step. As the Supreme Court has explained: "where intervening developments, or recent developments that we have reason to believe the court below did not fully consider, reveal a reasonable probability that the decision below rests upon a premise that the lower court would reject if given the opportunity for further consideration, and where it appears that such a redetermination may determine the ultimate outcome of the litigation, a GVR order is, we believe, potentially appropriate." *Lawrence ex rel. Lawrence v. Chater*, 516 U.S. 163, 167 (1996). The Supreme Court has thus concluded that there is at least a "reasonable probability" that this Court's prior ruling cannot be reconciled with its decision in *Van Buren*.

In its now-vacated opinion, this Court held that § 1030(a)(2) of the Computer Fraud and Abuse Act (CFAA), which bars accessing a qualifying computer "without authorization," offers public-facing websites no protection from data scraping by companies that harvest and exploit the personal data of the website's users for their own purposes. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir.

2019), *cert. granted, judgment vacated*, 2021 WL 2405144. According to the prior opinion, although LinkedIn had sent hiQ a cease-and-desist letter denying hiQ permission to access the computer servers that host its website, and LinkedIn had installed targeted IP blocks to prevent hiQ from accessing its computer servers, hiQ was not accessing LinkedIn's servers "without authorization" under the statute. *Id.* at 999-1004. That was because, in the Court's view, the CFAA's prohibitions on unauthorized access are categorically inapplicable to public-facing websites. *Id*. at 1001 (holding that a website that makes information publicly available does not grant, and therefore cannot rescind, authorization to access the website). This Court recognized that its categorical exclusion of public-facing websites was "debatable" as a textual matter, but relied on legislative history and policy considerations to support its interpretation of the provision. *Id*. at 1000.

After *Van Buren*, the fundamental premise of the Court's prior opinion is no longer tenable. The Supreme Court stated unequivocally that § 1030(a)(2)'s prohibition on access "without authorization" applies to "*all* information from all computers that connect to the Internet," which necessarily includes publicly-available information on websites. 141 S. Ct. at 1652 (emphasis added). The Supreme Court also clarified the framework for determining whether authorization had been granted, which it explained is a "gates-up-or-down inquiry—one either can or cannot access a computer system." *Id.* at 1658. That binary analysis—in which

authorization either is or is not given to access computer information—abrogates this Court's prior holding that "the CFAA contemplates the existence of *three* kinds of computer information." *hiQ*, 938 F.3d at 1001 (emphasis added). The Supreme Court's interpretation leaves no room for this Court's third option of "information for which access is open to the general public and permission is not required." *Id.*

Van Buren's analysis of § 1030(a)(2) also confirms that hiQ's scraping of LinkedIn's website was "without authorization." The choice to make information on a website publicly available operates as a presumptive grant of authorization for the general public to access the website's servers to view that information. But here, once LinkedIn sent hiQ a cease-and-desist letter and set up targeted IP blocks to prevent hiQ from accessing its servers, any further access by hiQ would have been "without authorization." *See Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1068 (9th Cir. 2016).

In addition, events that have transpired in the nearly two years since this Court issued its opinion cast serious doubt on the Court's evaluation of the equities and the public interest. The harms from mass-scraping of social media sites by entities like Clearview AI have shown that this Court's skepticism that Internet users care about the privacy of their personal information was misplaced. The interests in preventing the mass-scraping of user data for use in facial recognition, phishing attacks, and

other damaging exploits weigh strongly against affirming the district court's preliminary injunction—which gives a green light to such activities.

Because the Court's prior analysis can no longer stand in light of *Van Buren*, which makes clear that hiQ's continued access to LinkedIn's computers would be "without authorization," this Court should reverse the district court's grant of a preliminary injunction.

THE SUPREME COURT'S *VAN BUREN* DECISION

In *Van Buren*, former police officer Nathan Van Buren used his patrol-car computer to search for a license plate number in a law enforcement database in exchange for a bribe. 141 S. Ct. at 1653. It was undisputed that Van Buren was authorized to access the database, and that his search violated department policy. *Id.* He was charged with, and convicted of, violating the "exceeds authorized access" prong of § 1030(a)(2) of the CFAA, and his conviction was affirmed on appeal. *Id.* at 1653-54. The Supreme Court reversed Van Buren's conviction, finding that he did not "exceed[] authorized access" by obtaining information for an improper motive.

1. The Court began its analysis of § 1030(a)(2) "with the text of the statute." *Id.* at 1654. The Court first confirmed that the text of § 1030(a)(2) prohibits accessing "any information from any computer 'used in or affecting interstate or foreign commerce or communication.' § 1030(e)(2)(B). As a result, the prohibition

now applies—at a minimum—*to all information from all computers that connect to the Internet*. §§ 1030(a)(2)(C), (e)(2)(B)." *Id.* at 1652 (emphasis added). Because LinkedIn's servers are connected to the Internet and affect interstate commerce, § 1030(a)(2) bars access to those servers "without authorization."

The Court then turned to § 1030(a)(2)'s "exceeds authorized access" prong, parsing the statutory definition of that term provided by § 1030(e)(6). *Id.* at 1654-58. In doing so, the Court explained that "[i]f the phrase 'exceeds authorized access' were all we had to go on," the government's argument that the Court should look to the "common parlance" meaning of the phrase would have carried substantial force. *Id.* at 1657. But because the CFAA provided an "explicit definition" of "exceeds authorized access," that statutory definition controlled even if it departed from common parlance. *Id.* The Court therefore applied the statutory definition, relying on contemporaneous dictionary definitions of the terms in § 1030(e)(6) to explicate the meaning of "exceeds authorized access." *Id.* at 1654-55. The Court did not reference the CFAA's legislative history.

2. Because Van Buren had authorization to access his patrol-car computer, the case did not directly raise the question of what it means to access a protected computer "without authorization." The Court nonetheless comprehensively addressed "the statute's structure," *id.* at 1658, and its definitive construction of the statute bears directly on the proper resolution of this case.

The Court explained that its reading of § 1030(a)(2) placed the statute's "two distinct ways of obtaining information unlawfully …. 'into an harmonious whole.'" *Id.* (quoting *Roberts v. Sea-Land Servs., Inc.*, 566 U.S. 93, 100 (2012)). Citing to this Court's decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009), the Court held that the "without authorization" clause protects computers from "those who 'acces[s] a computer without any permission at all.'" *Van Buren*, 141 S. Ct. at 1658 (quoting *Brekka*, 581 F.3d at 1133). The Court explained that under its interpretation of "without authorization," "liability … stems from a gates-up-or-down inquiry—one either can or cannot access a computer system." *Van Buren*, 141 S. Ct. at 1658. The Court then indicated in a footnote that "[f]or 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 1659 n.8.

ARGUMENT

The Supreme Court's definitive construction of § 1030(a)(2) in *Van Buren* cannot be reconciled with this Court's prior analysis of the statute. Under *Van Buren*, § 1030(a)(2)'s prohibition on accessing a protected computer "without authorization" applies with full force to the computer servers that host LinkedIn's website. The present case therefore comes down to whether hiQ accessed those servers without authorization. To be sure, the Supreme Court reserved judgment on

whether "this inquiry turns only on technological (or 'code-based') limitations on access or instead also looks to limits contained in contracts or policies." *Van Buren*, 141 S. Ct. at 1659 n.8. But the Supreme Court's reasoning, as well as this Court's CFAA precedents, point to only one conclusion: once LinkedIn interposed technological blocks to deny hiQ access to LinkedIn's servers and sent hiQ a cease-and-desist letter revoking permission to access LinkedIn's servers, hiQ's continuing access to the website would be "without authorization" within the meaning of § 1030(a)(2).

I. *VAN BUREN* CONFIRMS THAT MAKING A WEBSITE PUBLICLY ACCESSIBLE IS A GRANT OF AUTHORIZATION UNDER THE CFAA

A. Under *Van Buren*'s Textual Analysis, Opening a Website to Public Access Is a Grant of Authorization

1. In its prior opinion, this Court analyzed the text of § 1030(a)(2), determining that hiQ's continuing access to LinkedIn's website was not "without authorization." *See hiQ*, 938 F.3d at 999-1000. The Court acknowledged that "without authorization" is a non-technical term, and that its ordinary meaning was "accessing a protected computer without permission," *id.* at 999 (citation omitted)—which as a matter of common parlance would cover any effort by hiQ to access LinkedIn's servers after LinkedIn sent its cease-and-desist letter and implemented technological blocks to keep hiQ out.

This Court nevertheless concluded that hiQ would not violate the CFAA's prohibition of accessing LinkedIn's servers without authorization, because "'[a]uthorization' is an affirmative notion, indicating that access is restricted to those specially recognized or admitted." *Id.* at 1000. As a result, "where access [to a website] is open to the general public, the CFAA 'without authorization' concept is inapplicable." *Id.* In the Court's view, "the CFAA contemplates the existence of three kinds of computer information: (1) information for which access is open to the general public and permission is not required, (2) information for which authorization is required and has been given, and (3) information for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed)." *Id.* at 1001-02. It continued that "[p]ublic LinkedIn profiles, available to anyone with an Internet connection, fall into the first category," such that "the concept of 'without authorization' is inapt." *Id.* at 1002.

In essence, this Court concluded that the prohibitions of § 1030(a)(2) do not apply at all to computer servers that host public-facing websites. Only by reading the statute in that way was the Court able to hold that no legal significance should be attributed to LinkedIn's revocation of hiQ's permission to access LinkedIn's servers (through both technological and written measures). By doing so, the Court

avoided answering the question whether efforts by hiQ to access LinkedIn's servers after LinkedIn took those steps would be "without authorization."

The panel's categorical exclusion of public-facing websites from the scope of the statute cannot be squared with *Van Buren*. Accessing a protected computer is either authorized or unauthorized—there is no third category as to which "the concept of 'without authorization' is inapt." *Id.* That is because, as *Van Buren* held, § 1030(a)(2)'s prohibitions, including its prohibition on access "without authorization," "appl[y]—at a minimum—to all information from all computers that connect to the Internet." *Van Buren*, 141 S. Ct. at 1652. That includes public-facing information on servers that host websites like LinkedIn, which is indisputably "information from [] computers that connect to the Internet." *See also EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63-64 (1st Cir. 2003) (holding that CFAA could apply to scraping of "public websites" and that "public website providers ought to say just what non-password protected access they purport to forbid"). Thus, after *Van Buren*, there is no way to avoid deciding whether hiQ would access LinkedIn's servers "without authorization" if it continued to scrape data after receiving a cease-and-desist letter and notwithstanding LinkedIn's technical blocks.

2. *Van Buren*'s reliance on dictionary definitions to construe § 1030 further undermines the premises of the prior ruling in this case. This Circuit has repeatedly (and correctly) held that "without authorization" is a "non-technical term" that

means "accessing a protected computer without permission." *United States v. Nosal*, 844 F.3d 1024, 1028 (9th Cir. 2016) (*Nosal II*); *see Brekka*, 581 F.3d at 1133 ("Authorization is defined in the dictionary as 'permission or power granted by an authority.'" (quoting Random House Unabridged Dictionary 139 (2001))).[1] The contemporaneous definitions cited by *Van Buren* define the term the same way. *See, e.g.*, The Random House Dictionary of the English Language 139 (2d ed. 1987) (authorization defined as "permission or power granted by an authority"); Webster's Third New International Dictionary 146-47 (1986) (defining "authorization" as "the state of being authorized" and "authorize" as to "permit by or as if by some recognized or proper authority"); 1 The Oxford English Dictionary 798 (2d ed. 1989) (authorization defined as "formal warrant, or sanction").

Although the prior panel opinion acknowledged the dictionary meaning of "authorization," it grafted an atextual gloss onto the term. According to the panel, "authorization" was not merely about whether a party had permission to access the

[1] Nothing in *Van Buren* casts doubt on the longstanding interpretation by this Court and other courts of appeals of "without authorization" in § 1030(a)(2) as a non-technical term that should be given its plain and ordinary meaning. Although the Court construed the term "access" to take on a computer-specific meaning, *see* 141 S. Ct. 1657-58 & n.6, 1659 & n.10, it did not do so for the term "authorization" in § 1030(a)(2). And nothing in the text, structure, or legislative history of the statute suggests that any definition other than the plain and ordinary meaning of the term "without authorization" should be used. This Court's definitive construction of the term "without authorization" therefore remains binding.

servers that host a website. Instead, "authorization" requires a "baseline" in which "access is not generally available," and access is granted only "to those specially recognized or admitted." *hiQ*, 938 F.3d at 1000. But nothing in the text of the statute supports this supposed distinction between individualized and widely-granted permission.

The prior panel opinion's chosen example demonstrates the problem with its analysis: according to the opinion, "[w]here the default is free access without authorization, in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of 'authorization.' *Cf. Blankenhorn v. City of Orange*, 485 F.3d 463, 472 (9th Cir. 2007) (characterizing the exclusion of the plaintiff in particular from a shopping mall as 'bann[ing]')." *Id.* While it is certainly true that excluding an individual from a shopping mall would constitute a "ban," that same individual lacks "permission or power" from the mall to enter, The Random House Dictionary of the English Language 139, is not "permit[ted] by" the mall to enter, Webster's Third New International Dictionary 146-47, and has no "formal warrant, or sanction" to enter, 1 The Oxford English Dictionary 798. Applying the dictionary definition of "authorization," as the Supreme Court made clear was the proper course in *Van Buren*, confirms that this Court's prior reasoning cannot stand.

3. *Van Buren*'s explanation of how the "without authorization" clause operates in practice also confirms that this Court's prior analysis of "without

authorization" is incorrect. The Supreme Court held that liability under the "without authorization" clause "stems from a gates-up-or-down inquiry—one either can or cannot access a computer system." *Van Buren*, 141 S. Ct. at 1658. The inquiry is therefore binary—the gates are up, and access is with authorization, or the gates are down, and access is without authorization. The prior panel opinion's additional category of computer information—"information for which access is open to the general public and permission is not required," *hiQ*, 938 F.3d at 1001, that is, information for which gates do not and cannot exist—runs contrary to the Supreme Court's construction of the statute. In other words, *Van Buren* confirms that there is no distinction between access without authorization and a "ban" on access. *Id.* at 1000. Both constitute the gates being down, and therefore access "without authorization."[2]

[2] In any event, LinkedIn's servers do not host "information for which access is open to the general public and permission is not required." *hiQ*, 938 F.3d at 1001. As the panel noted, using various technical measures, LinkedIn blocks approximately 95 million automated attempts to scrape data from its servers on a daily basis. *See id.* at 991. Thus, while making parts of its site public-facing is a grant authorization in the first instance, LinkedIn prevents access to its servers nearly one-hundred million times per day. It is therefore hardly "open to all comers," *id.* at 1002 (citation omitted), as many users such as hiQ lack "any permission at all" to access LinkedIn's servers. *Brekka*, 581 F.3d at 1133.

B. *Van Buren* Makes Clear that the Panel Erred by Disregarding Statutory Structure

Acknowledging that its brief textual analysis was "debatable," the prior panel opinion relied heavily on the statute's legislative history to buttress its reading of the text. *See hiQ*, 938 F.3d at 1000-02. At the same time, the prior opinion accorded no weight to the indications in the structure of the statute indicating that its reading of § 1030(a)(2) was incorrect. In *Van Buren*, the Supreme Court took precisely the opposite approach. It accorded no weight to the legislative history and looked instead to statutory structure to illuminate the provision's meaning.

As LinkedIn previously argued, the structure of § 1030(a) powerfully supports LinkedIn's construction of "without authorization." *See* LinkedIn Opening Br. at 42-43; LinkedIn Reply Br. at 21. In § 1030(a)(3), which applies to government computers and was adopted at the same time (in 1996) as its neighboring provision § 1030(a)(2), Congress proscribed "intentionally, without authorization to access any *nonpublic* [government] computer …, access[ing] such a computer." 18 U.S.C. § 1030(a)(3) (emphasis added). Congress could easily have done the same with § 1030(a)(2), thereby limiting its reach to exclusively nonpublic information. But Congress did not do so. As Judge Breyer has noted, "Congress apparently knew how to restrict the reach of the CFAA to only certain kinds of information, and it appreciated the public vs. nonpublic distinction—but § 1030(a)(2)(C) contains no such restrictions or modifiers." *Craigslist Inc. v. 3Taps, Inc.*, 964 F. Supp. 2d 1178,

1182-83 (N.D. Cal. 2013); *see also Sandvig v. Barr*, 451 F. Supp. 3d 73, 85 n.2 (D.D.C. 2020) ("[T]he fact that receipt of a cease-and-desist letter might render the recipient's future visits to an otherwise public website 'unauthorized' does provide one possible distinction between § [1030(a)(2)] and § [1030(a)(3)] that helps to give meaning to the term 'nonpublic' in the latter provision.").[3]

The panel opinion did not address this structural argument. Instead, the panel relied heavily on the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*, which it described as "nearly identical to the CFAA provision at issue." *hiQ*, 938 F.3d at 1002-03. But the SCA expressly carves out from liability access to communications "readily accessible to the general public." 18 U.S.C. § 2511(2)(g). The CFAA contains no analogous language. *See 3Taps*, 964 F. Supp. 2d at 1183.

[3] The prior panel opinion found that § 1030(a)(6)'s ban on password trafficking bolstered "the idea that authorization is only required for password protected sites or sites that otherwise prevent the general public from viewing the information." *hiQ*, 938 F.3d at 1001. But § 1030(a)(6) says merely that a password is one way "through which a computer may be accessed without authorization," 18 U.S.C. § 1030(a)(6). It nowhere suggests that it is the only way a computer may be accessed "without authorization." And indeed, this Court has previously held that the CFAA applies more broadly than only when a party circumvents a technological barrier such as a password. *See Nosal II*, 844 F.3d at 1038-39 ("Nosal challenges the instruction on the basis that the CFAA only criminalizes access where the party circumvents a technological access barrier. Not only is such a requirement missing from the statutory language, but it would make little sense because some § 1030 offenses do not require access to a computer at all. For example, § (a)(6) imposes penalties for trafficking in passwords 'through which a computer can be accessed without authorization....'" (footnote & citation omitted)).

The presence of a carve-out for "public" communications in the SCA, and its absence in the CFAA, therefore confirms that the CFAA should *not* be read to include such an exception. *See id*. (distinguishing SCA and noting that "[n]o such language appears in the CFAA provision at issue here"); *see also Marx v. Gen. Revenue Corp.*, 568 U.S. 371, 384 (2013) (Congress's "use of explicit language in other statutes cautions against inferring a limitation" not present in the plain text, as "Congress' explicit use of [language] in other provisions shows that it specifies such restrictions when it wants to." (citation omitted)). Just as with § 1030(a)(3), the SCA makes a distinction between public and nonpublic that § 1030(a)(2) does not make.

C. Policy Considerations Counsel Against the Panel Decision's Prior Interpretation of "Without Authorization"

Van Buren also undermines the prior panel opinion's concerns about the breadth of LinkedIn's interpretation of § 1030(a)(2). *Van Buren* found that the text and structure of § 1030(a)(2) were clear, such that no resort to the rule of lenity was necessary. 141 S. Ct. at 1661. *Van Buren* addressed the petitioner's policy argument regarding overcriminalization only because it "underscore[d] the implausibility of the Government's interpretation. It is 'extra icing on a cake already frosted.'" *Id*. (citation omitted). As in *Van Buren*, the text and structure are clear here, and the prior opinion thus erred in resorting to the rule of lenity. But even taking into account the relevant policy considerations, they only offer further support for LinkedIn's interpretation of the statute.

At the outset, *Van Buren* confirms that LinkedIn's proposed construction of § 1030(a)(2) will not risk criminalizing routine or innocent conduct. The Court in *Van Buren* was concerned that the government's interpretation of the "exceeds authorized access" clause "criminalizes every violation of a computer-use policy," such that "millions of otherwise law-abiding citizens [would be] criminals." *Id.* The government, for its part, did not endorse any limitation that alleviated that concern. *Id.* at 1661-62.

No similar risk is present in this case. The Ninth Circuit has already held that "a violation of the terms of use of a website-without more—cannot establish liability under the CFAA." *Power Ventures*, 844 F.3d at 1067; *see also United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (en banc) (*Nosal I*). Thus, regardless of how the Court rules in this case, there is no danger of criminalizing routine behavior without notice.

Attaching civil or criminal liability to a failure to heed a targeted cease-and-desist letter, or to an effort to circumvent targeted technical barriers, would not risk turning the CFAA "into a 'sweeping Internet-policing mandate.'" *hiQ*, 938 F.3d at 1003 (quoting *Nosal I*, 676 F.3d at 858). As an initial matter, "the average person does not use 'anonymous proxies' to bypass an IP block set up to enforce a banning communicated via personally-addressed cease-and-desist letter." *3Taps*, 964 F. Supp. 2d at 1184. Moreover, targeted cease-and-desist letters and IP blocks are an

expensive remedy. There is therefore little chance that they will be used indiscriminately. To the extent that a website provider were to issue cease-and-desist letters indiscriminately, *Power Ventures* suggested that an automatic, boilerplate cease-and-desist letter may not qualify as a revocation of authorization under § 1030(a)(2). *See* 844 F.3d at 1067 n.1.

In addition, because the statute requires that a person "intentionally" access a protected computer "without authorization," 18 U.S.C. § 1030(a)(2), there is no danger that an individual that is unaware that she is circumventing targeted IP blocks (or unaware of a targeted cease-and-desist letter) would be subject to criminal or civil liability. The statute's intent requirement and this Court's preexisting rule that terms-of-use violations cannot establish CFAA violations therefore together address the very concerns that *Van Buren* and this Court identified regarding the possibility that routine conduct would be subject to liability.

As a result, finding a revocation of authorization in these limited circumstances offers no risk of the kind that concerned the Court in *Van Buren*. *See, e.g.*, *3Taps*, 964 F. Supp. 2d at 1184 ("Nor does prohibiting people from accessing websites they have been banned from threaten to criminalize large swaths of ordinary behavior."). The rule of lenity and policy concerns offer no reason to depart from the text and structure of § 1030(a)(2).

Indeed, the policy considerations cut decisively in the opposite direction in this case. Since the panel rendered its decision, the grave threat to privacy—the very interest Congress sought to protect when it enacted the CFAA—from massive unauthorized data harvesting of the kind practiced by hiQ has become undeniable. For example, the company Clearview AI has deployed bots to engage in the systematic scraping of social media websites to amass a database of more than three billion photos, without the consent of those websites or their users. Clearview has exploited that scraped data to support a powerful facial recognition technology that it has already licensed to more than 600 law enforcement agencies and offered to some private individuals and companies. *See* Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. Times (Mar. 7, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html; Electronic Privacy Information Center (EPIC) Br. in Supp. of Cert. at 4, *LinkedIn Corp. v. hiQ Labs, Inc.*, No. 19-1116 (U.S. Apr. 13, 2021).[4] And data from hundreds

[4] *Available at* https://www.supremecourt.gov/DocketPDF/19/19-1116/141519/20200413154644290_19-1116%20Amicus%20Curiae%20Brief%20in%20Support%20of%20Certiorari%20by%20Electronic%20Privacy%20Information%20Center.pdf.

of millions of social network users have been scraped, compiled, and made available, either for profit or through breach, for bad actors to use as they see fit. *See, e.g.*, Jonathan Vanian, *Data from Half a Billion LinkedIn Users Has Been Scraped and Put Online*, Fortune Magazine (Apr. 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); *LinkedIn Data of 500 Million Users Hacked, Up For Sale: Report*, The Quint (Apr. 23, 2021) https://www.thequint.com/tech-and-auto/data-of-500-million-linkedin-users-for-sale-on-a-site-report (same).

Thus, not only are the policy concerns voiced by *Van Buren* not present in this case; the nearly two years since this Court issued its prior opinion have demonstrated that policy considerations cut in precisely the opposite direction.

* * *

In sum, *Van Buren*'s textual analysis and its use of the gates-up-or-down framework make clear that the "without authorization" clause of § 1030(a)(2)

presents a binary question in which authorization to access a protected computer, including a public-facing website, has been either granted or denied. And policy considerations powerfully reinforce the importance of reading the statute according to its plain terms. This Court's alternate approach, which carved out a third category for which authorization is never needed and therefore can never be revoked, cannot be squared with *Van Buren*. After *Van Buren*, the proper inquiry is straightforward: whether information that is accessed from a protected computer was accessed with or without permission.

II. HIQ'S CONTINUED ACCESS TO LINKEDIN'S WEBSITE WOULD BE WITHOUT AUTHORIZATION

The analysis set forth in *Van Buren* and this Court's precedents together confirm that hiQ's continued access to LinkedIn's website would be "without authorization." By making a website open to the public, a website operator puts its "gates up" and presumptively authorizes access to the general public to access the site's servers. In two mutually reinforcing ways, however, LinkedIn here revoked hiQ's authorization to access LinkedIn's servers. First, it sent a targeted cease-and-desist letter to hiQ, informing hiQ that it lacked authorization. Second, LinkedIn set up additional, targeted technical measures to block hiQ's access to its servers. Under the plain meaning of the statute and this Court's precedents, those actions each revoked any authorization hiQ previously had, and any subsequent accessing of LinkedIn's servers would be "without authorization."

1. When LinkedIn sent hiQ a targeted cease-and-desist letter, informing hiQ that any further scraping of LinkedIn's servers would be "without authorization" for purposes of the CFAA, that action revoked any authorization that LinkedIn had granted to hiQ to access its site. In the words of *Van Buren*, it lowered LinkedIn's gates to a "down" position for hiQ. As this Court previously explained, in *Power Ventures*, "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability." *Power Ventures*, 844 F.3d at 1067 (emphasis added). *Power Ventures* held that the use of a cease-and-desist letter was a clear revocation of permission to access a website. *Id.* ("Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter to Power ….").

The prior panel opinion distinguished *Power Ventures* on the theory that it applied only to "situations in which authorization generally is required and has either never been given or has been revoked." *hiQ Labs*, 938 F.3d at 1002. According to the panel, this case was different because information was "presumptively open to all comers," meaning authorization was not required and therefore could not be revoked. *Id.* (citation omitted). But for the reasons set forth above, after *Van Buren*, that reading of § 1030(a)(2) is no longer tenable. Making access "presumptively

open to all comers" is a grant of authorization, and as *Power Ventures* makes clear, that authorization can be, and was here, revoked.

2. In addition, as in *Power Ventures*, LinkedIn's cease-and-desist letter stated that it was putting in place additional, targeted IP blocks to prevent hiQ's corporate computers from accessing LinkedIn's servers. 4ER-736. As *Power Ventures* explained, such "IP barriers … further demonstrated that [a website operator] had rescinded permission for [a scraper] to access [its] computers." *Power Ventures, Inc.*, 844 F.3d at 1068.

Such IP blocks are "technological" or "code-based" restrictions on access. *Van Buren*, 141 S. Ct. at 1659 n.8. *Van Buren* left open whether non-code-based measures such as cease-and-desist letters qualify as a revocation of access (though *Power Ventures* resolves that issue in this Circuit, *see supra* pp. 21-22). But it left no doubt that technological limitations on access do qualify as a "gate" being lowered. *See Van Buren*, 141 S. Ct. at 1659 n.8. As hiQ has now explicitly alleged in its amended complaint, LinkedIn employed "technological means that could determine when hiQ accessed" LinkedIn's website, which "made it so hiQ's programs could not obtain any of the data" from the site. Dist. Ct. ECF 131 ¶ 44. In short, as hiQ has acknowledged, LinkedIn employed a technological gate. Thus, even if, contrary to *Power Ventures*, a cease-and-desist letter were somehow insufficient to indicate a withdrawal of authorization, the IP blocks that specifically

targeted hiQ are exactly the kind of technological, code-based measures that *Van Buren* indicated would undoubtedly withdraw any prior authorization.

III. THE BALANCE OF THE EQUITIES AND THE PUBLIC INTEREST FAVOR LINKEDIN

The prior panel opinion affirmed the district court's grant of a preliminary injunction in part because the Court found that the balance of the equities and the public interest favored hiQ. *See hiQ*, 938 F.3d at 994-95, 1004-05. Addressing the balance of the equities, the Court found that although LinkedIn argued "that the injunction threatens its members' privacy," and that "LinkedIn's assertions have some merit; … there are reasons to discount them to some extent." *Id.* at 994; *see also id.* ("[T]here is little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly, and it is doubtful that they do."). According to the Court, LinkedIn's members "quite evidently intend the[ir profiles] to be accessed by others, including for commercial purposes." *Id.* at 995. And in discussing the public interest, the Court found that although "Internet companies and the public do have a substantial interest in thwarting denial-of-service attacks and blocking abusive users, identity thieves, and other ill-intentioned actors," the Court did "not view the district court's injunction as opening the door to such malicious activity." *Id.* at 1004-05 (footnote omitted).

As noted above, in the time since this Court issued its prior decision, the harms that it downplayed have proven very real: They have caused and will continue to cause great harm to LinkedIn's members and to the general public. *See supra* pp. 18-19 (describing scraping on a massive scale and the use of scraped data by hackers and other bad actors). Widespread uproar over Clearview AI and episodes like Cambridge Analytica's massive misuse of Facebook user information,[5] undermine this Court's skepticism that "LinkedIn users who choose to make their profiles public [do not] actually maintain an expectation of privacy with respect to the information that they post publicly." *hiQ*, 938 F.3d at 994. In fact, LinkedIn members care deeply about their information being used only for the limited purposes that LinkedIn agrees it will use such data. *See* LinkedIn Opening Br. at 59-60; LinkedIn Reply Br. at 28. LinkedIn members make their information visible to the public *on LinkedIn*, where they can alter or remove it, and where any use of LinkedIn member data by LinkedIn is limited by LinkedIn's User Agreement and Privacy Policy. Placing their information on LinkedIn servers does not, however, mean that members consent to any and all companies harvesting their data, storing it permanently in databases, tracking their disclosures across time on one or many

[5] *See, e.g.*, Matthew Rosenberg & Sheera Frankel, *Facebook's Role in Data Misuse Sets off Storms on Two Continents*, N.Y. Times (Mar. 18, 2018), https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html.

sites, and using the data for any purpose. But because third party scrapers like hiQ do not enter into enforceable contracts with consumers, "nor do they generally provide similar rights to consumers whose data was scraped," LinkedIn members possess none of the control over scraped information that they have when the information is on LinkedIn's website. EPIC Br. at 13.

In the face of these increasing threats to privacy, the prior panel decision denied operators of public-facing websites a critical means of protecting user data from unauthorized third-party scrapers. It suggested that its decision would not "open[] the door to … malicious activity" like that of Clearview and other scrapers. *hiQ*, 938 F.3d at 1005. But privacy and Internet experts disagree. EPIC notes that "[c]ompanies in privity with their users must be able to protect users by limiting third-party access to personal data" in order to prevent misuse of that data. EPIC Br. at 23-24. And one prominent commentator stated that the prior decision "eviscerated the legal argument that" websites like LinkedIn previously used to block entities like hiQ and Clearview. *See* Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, N.Y. Times (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html (quoting director of Stanford Internet Observatory Alex Stamos).

These subsequent developments have thus made clear that the balance of the equities and the public interest favor reversing the preliminary injunction granted by the district court.

CONCLUSION

For the reasons discussed above, in light of the Supreme Court's decision in *Van Buren*, hiQ's continued use of bots to scrape data from LinkedIn's servers violates the CFAA. The district court's decision granting hiQ a preliminary injunction must therefore be reversed.

Respectfully submitted,

Dated: July 9, 2021

/s/ Donald B. Verrilli, Jr.

DONALD B. VERRILLI, JR.
JONATHAN S. MELTZER
MUNGER, TOLLES & OLSON LLP
601 Pennsylvania Ave. N.W., Suite 500E
Washington, DC 20001
Telephone: (202) 220-1100
Facsimile: (202) 220-2300
Donald.Verrilli@mto.com
Jonathan.Meltzer@mto.com

JONATHAN H. BLAVIN
ROSEMARIE T. RING
NICHOLAS D. FRAM
MARIANNA MAO
MUNGER, TOLLES & OLSON LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105-2907
Telephone: 415-512-4000
Facsimile: 415-512-4077
Jonathan.Blavin@mto.com
Rose.Ring@mto.com
Nicholas.Fram@mto.com
Marianna.Mao@mto.com

Attorneys for Defendant-Appellant
LinkedIn Corporation

ORRICK, HERRINGTON & SUTCLIFFE LLP

E. JOSHUA ROSENKRANZ
51 West 52nd Street
New York, NY 10019
(212) 506-5000
jrosenkranz@orrick.com

ERIC A. SHUMSKY
1152 15th Street, NW
Washington, DC 20005
(202) 339-8400
eshumsky@orrick.com

Attorneys for Defendant-Appellant
LinkedIn Corporation

CERTIFICATE OF COMPLIANCE

I certify pursuant to Federal Rules of Appellate Procedure 32(a)(7)(C) and Circuit Rule 32-1 that the attached brief is proportionately spaced, has a typeface of 14 points, and, according to the word count feature of the word processing system used to prepare the brief (Microsoft Word 2010), contains 6,016 words.

Dated: July 9, 2021

By: */s/ Donald B. Verrilli, Jr.*
Donald B. Verrilli, Jr.

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 9, 2021.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Laurence H. Tribe
Harvard Law School
1575 Massachusetts Avenue
Cambridge, MA 02138

Dated: July 9, 2021

By: */s/ Donald B. Verrilli, Jr.*
Donald B. Verrilli, Jr.