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

hiQ Labs, Inc.'s Supplemental Brief On Remand From The Supreme Court Of The United States

Corey Worcester
Renita Sharma
QUINN EMANUEL URQUHART & SULLIVAN, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
(212) 849-7000

Terry L. Wit
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
(415) 875-6331

July 9, 2021

Counsel for Appellee hiQ Labs, Inc.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Plaintiff-Appellee hiQ Labs, Inc. states that hiQ has no parent corporation and that no corporate entity owns more than 10% of Plaintiff-Appellee's stock.

TABLE OF CONTENTS

Page

CORPORATE DISCLOSURE STATEMENT 1
TABLE OF AUTHORITIES ii
INTRODUCTION 1
BACKGROUND 3
A. The Preliminary Injunction 3
B. LinkedIn's Petition And The Supreme Court's Decision In *Van Buren* 8
ARGUMENT 12
I. *Van Buren* Confirms That The District Court's Entry Of The Preliminary Injunction Should Be Affirmed 12
II. LinkedIn's "Counter-bot Measures" And Cease-And-Desist Letters Do Not Constitute "Gates" That Are "Down" 19
CONCLUSION 22

TABLE OF AUTHORITIES

Page

Cases

Emp't Div., Dep't of Human Res. of Or. v. Smith,
494 U.S. 872, 110 S. Ct. 1595 (1990) ……20

hiQ Labs, Inc. v. LinkedIn Corp.,
273 F. Supp. 3d 1099 (N.D. Cal. 2017)..... passim

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

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

LVRC Holdings LLC v. Brekka,
581 F.3d 1127, 1133 (9th Cir. 2009) ……2

United States v. Nosal,
676 F.3d 854 (9th Cir. 2012) …..... 19

United States v. Valle,
807 F.3d 508, 524 (2d Cir. 2015) 17

Sandvig v. Barr,
451 F. Supp.3d 73 (D.D.C. 2020)..... 14, 20

United States v. Van Buren,
940 F.3d 1192 (11th Cir. 2019) 5

Van Buren v. United States,
593 U.S. --- , 141 S. Ct. 1648 (June 3, 2021) ..... passim

Statutes

18 U.S.C. § 1030 ..... passim

18 U.S.C. § 2701 7

Other Authorities

Black's Law Dictionary (10th ed. 2014) 6

H.R. Rep. No. 98-894 (1984) 7

Orin S. Kerr, *Norms of Computer Trespass*,
116 Colum. L. Rev. 1143 (2016) 9

S. Rep. No. 104-357 (1996) 7

INTRODUCTION

The Supreme Court's recent decision in *Van Buren v. United States*, 593 U.S. --- , 141 S. Ct. 1648 (June 3, 2021), confirms the correctness of this Court's prior interpretation of the Computer Fraud and Abuse Act ("CFAA"). As this Court previously held in affirming the district court's entry of a preliminary injunction in favor of Plaintiff-Appellee hiQ Labs, Inc. ("hiQ"), "[i]t is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA." *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003 (9th Cir. 2019) ("*hiQ I*"), *cert. granted, judgment vacated*, No. 19-1116, 2021 WL 2405144 (U.S. June 14, 2021). On this basis, this Court concluded that Defendant-Appellant LinkedIn Corporation ("LinkedIn") was unlikely to show that the CFAA preempted hiQ's claims for tortious interference with contract and unfair competition. *hiQ I*, 938 F.3d at 999.

Nothing in the Supreme Court's decision in *Van Buren* undermines this conclusion. Instead, *Van Buren* confirms that LinkedIn cannot seek to invoke the civil and criminal liability of the CFAA as a means to preclude hiQ (and others) from accessing publicly available data. In fact, the reasoning in *Van Buren*, in which the Supreme Court interpreted the "exceeds authorized access" portion of

the CFAA, closely tracks this Court's analysis of the "without authorization" clause of the same statute.

As to the textual analysis of the statute, the Supreme Court recognized that "authorization" turns on whether one "can … access" a computer. The Supreme Court framed the inquiry in terms of a "gates up" or "gates down" approach, just as this Court considered as a threshold question whether authorization is even required before one "can … access" information, and the result here is the same under either approach. The Supreme Court reasoned the CFAA's prohibitions will not be implicated when the gate is "up", *Van Buren*, 141 S. Ct. 1658-60, just as this Court concluded that "authorization" necessarily "suggests a baseline in which access is not generally available and so permission is ordinarily required." *hiQ* I, 938 F.3d at 1000. That necessarily excludes from the scope of the CFAA's prohibition the publicly available data to which LinkedIn seeks to apply the CFAA. And, like this Court, the Supreme Court read the CFAA in light of its intended purpose—to "target so-called outside hackers—those who 'acces[s] a computer without any permission at all.'" *Van Buren*, 141 S. Ct. at 1658 (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)); *hiQ I*, 938 F.3d at 999-1002.

The Supreme Court likewise warned, as this Court had, that expanding the scope of the "exceeds authorized access" clause would render a vast amount of

conduct criminal and inject arbitrariness into the statute's application. *Van Buren*, 141 S. Ct. at 1661. Such logic applies with particular force here, where LinkedIn attempted to invoke the CFAA to gain a competitive advantage over hiQ after not objecting to hiQ's data collection practices for years. And the district court, this Court, and the Supreme Court all recognized the inherent danger in criminalizing routine conduct, including the use of bots that can gather large amounts of public data quickly for research or other purposes.

Finally, while LinkedIn may argue that its cease-and-desist letter and "counter-bot measures" equate to a "gate" that is "down," that cannot be the case. Such an argument would require distinguishing between any member of the public and bots, which the CFAA does not support. Because any interpretation of the CFAA must be universally applicable, and the data at issue here unquestionably is public, the gate can only be "up."

The Supreme Court's decision in *Van Buren* lends additional support to this Court's prior holding that the CFAA's "without authorization" clause is unlikely to give rise to civil and criminal liability based on accessing publicly available information. The district court's preliminary injunction should be affirmed.

BACKGROUND

A. The Preliminary Injunction

In 2017, around the same time LinkedIn announced it would provide analytics services to companies (similar to those hiQ provided its clients) based on the public profiles of LinkedIn users, LinkedIn informed hiQ that it could no longer gather public data from LinkedIn's website and would face liability under the CFAA if it continued to do so. Facing the likely destruction of its business, hiQ sued LinkedIn for its anti-competitive conduct and sought a declaratory judgment that the CFAA did not apply. hiQ also sought a preliminary injunction enjoining LinkedIn from preventing hiQ's access, copying, or use of public profiles on LinkedIn's website, and from blocking or putting in place any mechanism with the effect of blocking hiQ's access to such public member profiles.

The district court granted hiQ's request for a preliminary injunction. *See hiQ Labs, Inc. v. LinkedIn Corp*., 273 F. Supp. 3d 1099 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019), *cert. granted, judgment vacated*, No. 19-1116, 2021 WL 2405144 (U.S. June 14, 2021). The district court first found that "hiQ unquestionably faces irreparable harm in the absence of an injunction, as it will likely be driven out of business." *Id.* at 1107. The court also found that "the balance of hardships tips sharply in hiQ's favor." *Id.* Thus, the court moved on to

the third inquiry—that is, whether hiQ had raised serious questions going to the merits of its underlying claims. *Id.* at 1107-08.

On this inquiry, the district court explained that "[t]he CFAA was not intended to police traffic to publicly available websites on the Internet" as "the Internet did not exist" when the statute was drafted. *Id.* at 1109. The court further reasoned that "application of the CFAA to the accessing of websites open to the public would have sweeping consequences well beyond anything Congress could have contemplated; it would 'expand its scope well beyond computer hacking.'" *Id.* at 1110 (citation omitted). Thus, the court explained that "hiQ has, at the very least, raised serious questions as to the applicability of the CFAA to its conduct," and, as such, to the merits of its case. *Id.* at 1113-20.

Lastly, the district court determined that the public interest favors the granting of a preliminary injunction where "conferring on private entities such as LinkedIn[ ] the blanket authority to block viewers from accessing information publicly available on its website for any reason, backed by sanctions of the CFAA, could pose an ominous threat to public discourse and the free flow of information promised by the internet." *Id.* at 1119.

This Court affirmed, agreeing with the district court that hiQ had demonstrated a likelihood of irreparable harm on account of LinkedIn's conduct and that the balance of hardships tips sharply in hiQ's favor. *hiQ I*, 938 F.3d at

994-1005.[1] This Court then concluded that "hiQ has raised at least serious questions going to the merits of its tortious interference with contract claim"[2] and that the public interest favors a preliminary injunction. *hiQ I*, 938 F.3d at 994-1005.

In addressing LinkedIn's argument that the CFAA preempts hiQ's causes of action, this Court determined it did not. *Id.* at 999. The CFAA provides that "[w]hoever … intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer … shall be punished" criminally and may be subject to civil liability. 18 U.S.C. § 1030(a)(2)(C). This Court concluded that the CFAA did not extend to hiQ's scraping of publicly available information, relying on four primary rationales.

First, this Court examined the plain text of the statute. Although the CFAA does not define "without authorization," the phrase necessarily "suggests a baseline in which access is not generally available and so permission is ordinarily required."

---

[1] This Court's finding that the balance of hardships tips in hiQ's favor is supported in hindsight by the fact that LinkedIn agreed to stay discovery (and thus to delay resolution of the underlying case) pending a ruling from the Supreme Court on its petition for certiorari (17-cv-3301-EMC, Dkt. 129) and thus, unlike hiQ, which has been run out of business, LinkedIn cannot be heard to say it has been harmed by the preliminary injunction.

[2] This Court found that, "[a]s that showing on the tortious interference claim [wa]s sufficient to support an injunction prohibiting LinkedIn from selectively blocking hiQ's access to public member profiles," it was not necessary to "reach hiQ's unfair competition claim." *hiQ I*, 938 F.3d at 999.

hiQ I, 938 F.3d at 1000. Such a reading is consistent with the dictionary definition of the word "authorization." *Id.* (citing BLACK'S LAW DICTIONARY (10th ed. 2014) (defining "authorization" as "[o]fficial permission to do something; sanction or warrant")).

Second, this Court confirmed its unambiguous plain-text interpretation with the applicable legislative history. As initially conceived, "section 1030 deal[t] with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer." *hiQ I*, 938 F.3d at 1000 (quoting H.R. Rep. No. 98-894, at 20 (1984)). In expanding the reach of the CFAA in 1996 to cover "protected computers," that is, those used in interstate commerce, "the Senate Judiciary Committee explained that the amendment was designed 'to increase protection for the privacy and confidentiality of computer information.'" *Id.* at 1001(quoting S. Rep. No. 104-357, at 7). Based on this legislative history, this Court held that "the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort." *Id.*

Third, the Court concluded that prior CFAA decisions had not decided whether the prohibition on accessing information "without authorization" extended to websites accessible to "anyone with a web browser." *Id.* at 989. But the Court explained that its prior interpretation of the phrase "without authorization" in the

Stored Communications Act, 18 U.S.C. § 2701, supported a "distinction between 'private' computer networks and websites, protected by a password authentication system and 'not visible to the public,' and websites that are accessible to the general public." *Id.* at 1003.

Finally, the Court held that, because the CFAA imposes criminal penalties based on the same language, the rule of lenity favors a narrow reading of the covered conduct. *Id.* Thus, the Court concluded that "[i]t is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA. The data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using such an authorization system." *Id.* at 1003-04. As a result, the Court "conclude[d] that hiQ has raised a serious question as to" whether, "where access is open to the general public, the CFAA 'without authorization' concept is inapplicable." *Id.* at 1000.

B. LinkedIn's Petition And The Supreme Court's Decision In *Van Buren*

LinkedIn petitioned the Supreme Court for a writ of certiorari. While the petition was pending, however, the Supreme Court granted the petition in another case addressing the CFAA, *Van Buren*.

In *Van Buren*, the Supreme Court addressed the CFAA's "exceeds authorized access" clause. *Van Buren*, 141 S. Ct. at 1652. Van Buren, a former

police sergeant, was convicted of violating the CFAA's "exceeds authorized access" clause when he "ran a license-plate search in a law enforcement computer database in exchange for money" in violation of his department's policy permitting him to use the database only for law enforcement purposes. *Id.* Van Buren appealed his conviction, and the Eleventh Circuit affirmed, holding that Van Buren "had violated the CFAA by accessing the law enforcement database for an 'inappropriate reason.'" *Id.* at 1654 (quoting *United States v. Van Buren*, 940 F.3d 1192, 1208 (11th Cir. 2019)). The Supreme Court granted certiorari.

Because Van Buren did not dispute that he had "access[ed] a computer [namely, the law enforcement database] with authorization" or that he "obtain[ed] … information in the computer," *id.* at 1654, the only question in *Van Buren* was whether Van Buren was "entitled so to obtain" the information he took from the database. *Id.* The Supreme Court concluded that "[t]he phrase 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access," *id.* at 1655, and rejected the Government's interpretation of the word "so" as also "refer[ring] to information one was not allowed to obtain *in the particular manner or circumstance in which he obtained it*," *id.* at 1654-55 (emphasis in the original).

In adopting Van Buren's interpretation of the statute, the Supreme Court explained that an interpretation of the statute that does not incorporate use

restrictions aligns with the statutory structure. *Id.* at 1658. Indeed, this interpretation "makes sense of the statutory structure because it treats the 'without authorization' and 'exceeds authorized access' clauses consistently." *Id.* That is, "[u]nder Van Buren's reading, liability under both 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 1658-59. Reading these "clauses to adopt a gates-up-or-down approach," the Supreme Court explained, "aligns with the computer-context understanding of access as entry." *Id.* at 1659.

On another structural note, the Supreme Court explained that construing the "exceeds authorized access" clause as including violations of use restrictions makes little sense when considering that the statute also gives rise to civil liability where a plaintiff can show "damage" or "loss," which, as defined, "focus[es] on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data." *Id.* at 1659-60. These terms, the Court reasoned, are inapposite where a plaintiff claims "misuse" of information obtained in a computer to which the defendant had authorized access. *Id.* at 1660.

Although the Court found that the text of the statute was clear enough that canons like the rule of lenity and constitutional avoidance need not come into play, the Court nevertheless found these canons provide "extra icing on a cake already

frosted" to support *Van Buren*'s CFAA interpretation. *Id.* at 1661. Specifically, the Court noted that construing the "exceeds authorized access" clause to incorporate use restrictions "would attach criminal penalties to a breathtaking amount of commonplace computer activity." *Id.* at 1661. In particular,

> [i]f the "exceeds authorized access" clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals. Take the workplace. Employers commonly state that computers and electronic devices can be used only for business purposes. So on the Government's reading of the statute, an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA. Or consider the Internet. Many websites, services, and databases—which provide "information" from "protected computer[s]," § 1030(a)(2)(C)—authorize a user's access only upon his agreement to follow specified terms of service. If the "exceeds authorized access" clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers. And indeed, numerous *amici* explain why the Government's reading of subsection (a)(2) would do just that—criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook.

Id. These far-reaching consequences, the Court noted, only lend further support to the narrower reading of the statute. *Id.*

Lastly, the Court held that reading the CFAA to prohibit use restrictions "would inject arbitrariness into the assessment of criminal liability." *Id.* at 1662. Specifically, the Court explained that the "exceeds authorized access" clause does not prohibit misuse of information, but that purpose-based restrictions may be written as either access or use restrictions—the former of which would be

actionable under the Government's reading, and the latter of which would not. *Id.* "An interpretation that stakes so much on a fine distinction controlled by the drafting practices of private parties is hard to sell as the most plausible." *Id.*

Against these textual, structural, and policy analyses, the Court definitively held that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." *Id.* at 1662. Because Van Buren was permitted to access the law enforcement database, he could not have violated the CFAA's "exceeds authorized access" clause. *Id.*

On June 14, 2021 the Supreme Court granted LinkedIn's petition, vacated this Court's judgment, and remanded the matter for further consideration in light of its decision in *Van Buren*. *LinkedIn Corp. v. hiQ Labs, Inc.*, No. 19-1116, 2021 WL 2405144, at *1 (U.S. June 14, 2021). This Court subsequently directed the parties to brief the effect of *Van Buren* on LinkedIn's appeal. Dkt. 97.

ARGUMENT

I. *VAN BUREN* CONFIRMS THAT THE DISTRICT COURT'S ENTRY OF THE PRELIMINARY INJUNCTION SHOULD BE AFFIRMED

Van Buren confirmed, just as this Court held, that CFAA liability cannot be based on access to public information.

First, *Van Buren* aligns with this Court's textual analysis of the "without authorization" clause. At the threshold, both this Court and the Supreme Court

understood "without authorization" to turn on whether one "can … access" a certain computer. *Van Buren's* discussion of the "without authorization" clause also makes clear that the question of one's "authorization" is whether "one either can or cannot access a computer system." *Van Buren*, 141 S. Ct. at 1658. This is the "gates-up-or-down inquiry" that the Court was satisfied harmonizes the "without authorization" and "exceeds authorized access" clauses and also "aligns with the computer-context understanding of access as entry." *Id.* at 1658-59. The Supreme Court explained that a "specific type of authorization [is in question]—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. These guiding principles—that the authentication-based, gates-up-or-down for access approach—closely mirror this Court's reasoning in affirming the preliminary injunction.

In *hiQ I*, this Court addressed the question of whether one "can … access" a computer system if it is publicly available and held that one does not need "authorization" to do so. While the Supreme Court's "gates-up-or-down" analysis addresses whether authorization has been *granted*, *hiQ I* addresses a threshold gates-up-or-down analysis: that is, whether authorization (i.e., a "gate") is even *required* before one "can … access" information. In its discussion of the public/private information distinction, this Court specifically referenced the statutory history describing what could be considered gates to access ("warnings,

encryptions, password requests, or other indicia of intended privacy") and found that, because those kinds of checkpoints are not placed on publicly available information, it would run counter to congressional intent to find that such data can be accessed "without authorization." *Id.* at 1003.

In this regard, *Van Buren's* discussion of the "gates-up-or-down approach" with respect to the "without authorization" clause is wholly consistent with this Court's conclusion that the CFAA's "prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort." *hiQ I*, 938 F.3d at 1001.[3]

Other courts' application of *hiQ I* demonstrates the harmony between the *Van Buren* gates-up-or-down approach and this Court's conclusion that the CFAA does not apply to publicly available information. For example, in *Sandvig v. Barr*, which the Supreme Court cites in *Van Buren* in support of its discussion as to the potential far-reaching implications of a broad reading of the "exceeds authorized access" provision, *Van Buren*, 141 S. Ct. at 1661, the district court for the District of Columbia explained that *hiQ I*

[3] The fact that the Supreme Court stated that the CFAA's "prohibition now applies—at a minimum—to all information from all computers that connect to the Internet," 141 S. Ct. at 1652, does not alter this conclusion because—at a minimum—public access equates to authorization to access the public website.

> contemplates a view of the internet that is divided into at least two realms—public websites (or portions of websites) where no authorization is required and private websites (or portions of websites) where permission must be granted for access. Because many websites on the internet are open to public inspection, a website or portion of a website becomes "private" only if it is "delineated as private through use of a permission requirement of some sort."

451 F. Supp. 3d 73, 85 (D.D.C. 2020) (emphasis in original) (quoting *hiQ I*, 938 F.3d at 1001). Taking this discussion to its logical next step, if a portion of an otherwise publicly available website is restricted from public access through a permission requirement (such as a password authentication requirement), *Van Buren's* gates-up-or-down inquiry might *then* be triggered. But, until information becomes unavailable to the public, the gate cannot be considered down.

Second, both the Supreme Court and this Court confirmed the accuracy of this interpretation by looking to the intent of the CFAA's "without authorization" clause as intended to deter outside hackers. In discussing the "without authorization" clause, the Supreme Court credited Van Buren's view that this clause "protects computers themselves by targeting so-called outside hackers—those who 'access[s] a computer without any permission at all.'" *Id.* at 1658 (citation omitted). This reading, which tracks with the statutory history of the CFAA responding to the insufficiency of trespass statutes for new digital crimes, *id.* at 1652, is entirely consistent with this Court's prior analysis in *hiQ I*.

In its decision, this Court recognized that the phrase "'access[] … without authorization,' … suggests a baseline in which access is not generally available and so permission is ordinarily required." *hiQ I*, 938 F.3d at 1000. Accordingly, the "without authorization" concept (and, thus, the CFAA) is inapplicable when it comes to computer "information for which access is open to the general public and permission is not required." *Id.* at 1001-02. *hiQ I* recognized that this conclusion is supported by the CFAA's genesis as a response to computer hacking, a crime which was framed similarly to breaking and entering. *Id.* at 1001. This kind of crime necessarily requires an expectation of generalized exclusion—put differently, a person is incapable of hacking or breaking into a repository of information that has already been made public. *Id.* In no sense of the word is an individual "hacking" when she types a name into Google, clicks on the public LinkedIn profile that has expressly been made available to Google's search results, and then reads the information she finds on that public profile.

As a prelude to its discussion of the gates-up-or-down approach, the Supreme Court agreed 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.'" *Van Buren*, 141 S. Ct. at 1658 (quotations omitted). Thus, the *Van Buren* Court agreed that the "exceeds authorized access" clause "provide[s] complementary protection for certain information within

computers … by targeting so-called inside hackers—those who access a computer with permission, but then 'exceed the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend.'" *Id.* (quoting *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015)). In other words, "Van Buren's account of subsection (a)(2) makes sense of the statutory structure because it treats the 'without authorization' and 'exceeds authorized access' clauses consistently." *Id.* That is, "[u]nder Van Buren's reading … one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Id.* at 1658-59.

This Court's holding that the CFAA's "without authorization" clause does not apply to publicly available information squares with the Supreme Court's above analysis. Like the Supreme Court, this Court recognized the "[t]he CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking." *hiQ* I, 938 F.3d at 1000. This intent, *hiQ I* explained, is demonstrated by the 1984 House Report on the CFAA, which "explicitly analogized the conduct prohibited in section 1030 to forced entry." *Id.* After further analyzing the statute's legislative history, the Court concluded that "[t]he legislative history of section 1030 … makes clear that the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some

sort." *Id.* at 1001. Stated differently, where publicly available information is at issue, the concept of "computer hacking" that the Supreme Court considered in discussing the gates-up-or-down approach with approval is simply inapplicable.

Third, this Court's conclusion that the rule of lenity "favor[s] a narrow interpretation of the CFAA's 'without authorization' provision," *id.* at 1003, is only underscored by the Supreme Court's concerns in *Van Buren* of the potential consequences of adopting an expansive reading of the CFAA's "exceeds authorized access" provision. Specifically, the Supreme Court reasoned that "[i]f the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals." *Van Buren*, 141 S. Ct. at 1661. For example, any employee subject to an employer's policy that prohibits personal use of employer computers "who sends a personal e-mail or reads the news using her work computer has violated the CFAA." *Van Buren*, 141 S. Ct. at 1661. Similarly, under a broad reading of the "exceeds authorized access" clause, any visitor of a public website who violates that website's terms of service (even by, for example, "embellishing an online-dating profile [or] using a pseudonym on Facebook") could be subject to criminal liability. *Id.* (citations omitted).

Just as the Supreme Court found that "[t]he Government's interpretation of the 'exceeds authorized access' clause would attach criminal penalties to a

breathtaking amount of commonplace computer activity," *id.*, this Court correctly raised the concern that a broader interpretation of the "without authorization" clause might "turn a criminal hacking statute into a 'sweeping Internet-policing mandate'", *hiQ I*, 938 F.3d at 1003 (quoting *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012)). A ruling in LinkedIn's favor by this Court would undermine *Van Buren's* recognition of the need to inject a degree of certainty into an analysis of a statute that imposes criminal liability.

In sum, the *Van Buren* decision is entirely consistent with this Court's analysis in *hiQ I*.

II. LINKEDIN'S "COUNTER-BOT MEASURES" AND CEASE-AND-DESIST LETTERS DO NOT CONSTITUTE "GATES" THAT ARE "DOWN"

To the extent LinkedIn argues that its technical measures and cease-and-desist letter constitute "gates" that are "down," such an argument cannot succeed.

In *Van Buren*, the Supreme Court noted that, in the case before it, it "need not address whether [the access] 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. Here, neither type of limitation would equate to a "gate" being "down" because LinkedIn concedes that the information is publicly available. And counter-bot measures and cease-and-desist letters do nothing to change that fact because they focus on the users accessing

public information, and do not convert such public information to non-public information.

As to the cease-and-desist letter, this Court already rejected the idea that a cease-and-desist letter purporting to prohibit access to a public website would trigger a violation of the CFAA. *hiQ I*, 938 F.3d at 1002. As this Court recognized, "the legislative history of section 1030 … makes clear that the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort." *hiQ I*, 938 F.3d at 1001. Indeed, were it otherwise, private companies would decide selectively whose access to their websites runs afoul of federal law. *See hiQ I*, 938 F.3d at 1005 ("We agree with the district court that giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest."); *see also Sandvig*, 451 F. Supp. 3d at 87 ("Criminalizing terms-of-service violations risks turning each website into its own criminal jurisdiction and each webmaster into his own legislature. Such an arrangement, wherein each website's terms of service 'is a law unto itself,' would raise serious problems.") (quoting *Emp't Div., Dep't of Human Res. of Or. v. Smith*, 494 U.S. 872, 890, 110

S. Ct. 1595 (1990)). Such an approach is consistent with the *Van Buren* gate-based approach because a cease-and-desist letter does not convert public information to private information. *See hiQ I*, 938 F.3d at 1002 ("While Power Ventures was gathering user data that was protected by Facebook's username and password authentication system, the data hiQ was scraping was available to anyone with a web browser.").

For this same reason, "counter-bot measures" do not slam the gate shut because they do not change the information from publicly available to non-publicly available. Rather, counter-bot measures focus on a specific type of *user*, but not on the scope of access to information more generally. LinkedIn does not dispute that the information it is attempting to block hiQ's technology from accessing can be accessed without the use of a bot. Any purported "gate" that purports to block access of information by automated technology but not by any other means would impermissibly expand the CFAA into the realm of public information where it was never intended to operate.[4] In addition, under LinkedIn's counter-bot measure approach, one might not even know that such measures rendered access "unauthorized" unless the bot happened to encounter such counter-bot measures.

[4] Moreover, even if this Court wished to determine what type of technology would qualify as a "gate" preventing access of otherwise publicly available information, the record before this Court does not support such a finding. LinkedIn adduced no evidence on the scope of these counter-bot measures that could support a finding that such measures put the gate down, even if permissible as a matter of law.

As the Supreme Court advised, this approach to the CFAA would render the statutory scheme unworkable. *Van Buren*, 141 S. Ct. at 1661. And, in fact, any approach that has the effect of criminalizing access to public information would render the CFAA unconstitutional. hiQ Br. (Dkt. 36) at 25-30.

CONCLUSION

This Court should affirm the district court's grant of the preliminary injunction.

Dated: July 9, 2021

Respectfully Submitted,

/s/ Terry L. Wit

Terry L. Wit
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California St., 22nd Floor
San Francisco, CA 94111
(415) 875-6311

Corey Worcester
Renita Sharma
QUINN EMANUEL URQUHART & SULLIVAN, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
(212) 849 7000

Attorneys for Plaintiff-Appellee hiQ Labs, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on July 9, 2021 I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

Dated: July 9, 2021

/s/ Terry L. Wit

Terry L. Wit
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California St., 22nd Floor
San Francisco, CA 94111
(415) 875-6600
(415) 875-6700 facsimile

Attorneys for Plaintiff-Appellee hiQ Labs, Inc.

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

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

I am the attorney or self-represented party.

This brief contains 5,079 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.

[X] complies with the length limit designated by court order dated June 14, 2021.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature */s/ Terry Wit* **Date** July 9, 2021