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

REPLY BRIEF FOR PETITIONER

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

BRIAN P. GOLDMAN
ORRICK HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105
(415) 773-5700

DONALD B. VERRILLI, JR.
Counsel of Record
JONATHAN S. MELTZER
MUNGER, TOLLES & OLSON LLP
1155 F Street NW, 7th Floor
Washington, DC 20004
(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

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

FEDERAL STATUTES

INTRODUCTION

Because of the decision below, anyone can now deploy automated "bots" to scrape and exploit massive quantities of personal information from public-facing websites—even over the objection of website operators and in disregard of the limitations that Internet users have placed upon the dissemination and use of their data.

Although respondent hiQ pretends otherwise, the profound significance of the Ninth Circuit's interpretation of Section 1030(a) of the Computer Fraud and Abuse Act (CFAA) could not be clearer. *E.g.* Pet. 5 & n.3 (quoting head of the Stanford Internet Observatory stating that ruling "eviscerated the legal argument" that allows companies to protect themselves from scrapers); Electronic Privacy Information Center (EPIC) Br. at 5 (The "lower court's decision makes it impossible for companies to fulfil their responsibility [to protect user information] and sets a dangerous precedent that could threaten the privacy of user data.").

The Ninth Circuit has thus neutered the protections that the CFAA affords to website operators and their users. And it has done so at the very moment when the threats posed by unauthorized scraping and misuse of personal information from public-facing websites are exploding. *See* EPIC Br. at 4 (discussing Clearview AI's creation of massive privacy-threatening biometric database). Internet users who choose to make information about themselves available to particular websites for particular purposes under specifically-agreed conditions now find themselves at the mercy of entities that have no obligation to respect those privacy-protecting limitations, and can (and will) exploit such information for any purpose and for all time.

The Ninth Circuit's sweeping and unprecedented interpretation of the CFAA—which opens a circuit split and rests principally on extratextual policy considerations—justifies this Court's review.

ARGUMENT

A. The Decision of the Court of Appeals Creates a Direct Circuit Conflict

The petition demonstrates that the decision below conflicts with *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003). Pet. 15-20. hiQ contends, however, that the First Circuit "never even considered" the scope of "without authorization" in the CFAA. Opp. 11. In fact, the *eight paragraphs* of *EF Cultural Travel* that precede hiQ's cherry-picked quotations are *entirely* about the meaning of Section 1030(a). 318 F.3d at 62-63. The First Circuit explained that under the CFAA, "[a] lack of authorization could be established by an explicit statement … restricting access," and that if a "public website" operator "wants to ban scrapers, let it say so." *Id.* at 62-63. To prevent confusion, the First Circuit continued: "It is also of some use for future litigation among other litigants in this circuit to indicate that, with rare exceptions, *public website* providers ought to say just what *non-password protected access* they purport to forbid." *Id.* at 64 (emphases added). Unsurprisingly, courts have cited *EF Cultural Travel* in holding that the CFAA applies to public websites. *E.g.*, *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595-97 (E.D. Pa. 2016).

Thus, under *EF Cultural Travel*, the question under the CFAA is whether LinkedIn had "spell[ed] out explicitly [to hiQ] what is forbidden." 318 F.3d at 63. LinkedIn did precisely that when it sent hiQ the cease-and-desist letter. Pet. 11-12. Meanwhile, in the Ninth

Circuit, a publicly-accessible website can *never* resort to the CFAA to prevent a scraper from harvesting personal data on that site. The conflict is clear, direct, and outcome determinative.

The Ninth Circuit's decision also broke with every court to have interpreted "without authorization" in this context. Pet. 17-18. hiQ insists that these uniform decisions "do not address the issue the court of appeals decided." Opp. 12. That assertion is false. In fact, hiQ ignores holdings that are directly on point in favor of quotations that are entirely consistent with LinkedIn's interpretation of "without authorization."[1] Each of the cases cited in LinkedIn's petition addresses the *exact* issue here.

hiQ also contends that a district court recently agreed with the Ninth Circuit. Opp. 13 (citing *Sandvig v. Barr*, No. CV 16-1368 (JDB), 2020 WL 1494065 (D.D.C. Mar. 27, 2020)). On the contrary, *Sandvig* explicitly left open the question decided below: "Because no [cease and desist] letters have been sent in this case, the Court need not decide whether they would constitute a revocation of authorization." *Id.* at *8 n.2.

The fact is that the Ninth Circuit opened a clear circuit split with the First Circuit and diverges from

---

[1] *E.g.*, *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1183 (N.D. Cal. 2013) ("[U]nder the plain language of the statute, 3Taps was 'without authorization' when it continued to pull data off of Craigslist's website after Craigslist revoked its authorization to access the website."); *Resultly*, 159 F. Supp. 3d at 597 ("[J]ust as a cease-and-desist letter would put a publisher on notice that its actions were prohibited … Resultly [was] on notice that QVC prohibited web-crawling."); *Sw. Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 440 (N.D. Tex. 2004) ("Southwest alleges that it directly informed Outtask that their access was unauthorized.").

every other federal court to have considered the application of Section 1030(a) to unauthorized scraping from public-facing websites. This Court should address this departure from existing consensus in an area where a nationwide rule is particularly important now. *See* Pet. 18-20.

B. The Ninth Circuit's Interpretation of the CFAA is Incorrect

hiQ's defense of the decision below is notable, like the decision itself, for how little it engages with the text of Section 1030(a)(2)(C). As this Court recently stressed, however, "when the express terms of a statute give us one answer and extratextual considerations suggest another, it's no contest. Only the written word is the law." *Bostock v. Clayton County*, 140 S. Ct. 1731, 1737 (2020).

a. The CFAA provides liability for "[w]hoever … intentionally accesses a computer without authorization … and thereby obtains … information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). The ordinary meaning of "without authorization" is that someone can access the protected computer only with permission to do so. Pet. 20. But the Ninth Circuit found that, although LinkedIn informed hiQ that it did not have permission to access LinkedIn's servers, "selective denial of access [w]as a ban" but not "a lack of 'authorization'" under Section 1030(a)(2)(C). Pet. 21. That purported distinction between a "ban" and a "lack of authorization" has no basis in text or common sense. Pet. 20-22.

hiQ contends that LinkedIn "ignores the Ninth Circuit's focus on publicly available information," which led it to rule that "'authorization is only required for password-protected sites or sites that otherwise *prevent the general public from viewing the information*.'"

Opp. 16 (quoting Pet. App. 27a). But hiQ's argument merely exposes the Ninth Circuit's error: Section 1030(a)(2)(C) says *nothing* about whether the information on a private server is publicly available, instead barring "access[ing] a computer without authorization" to obtain "information from *any* protected computer." 18 U.S.C. § 1030(a)(2)(C) (emphasis added). The Ninth Circuit was wrong precisely *because of* its "focus on publicly available information," which appears nowhere in Section 1030(a)(2)(C). The decision below disregarded this unambiguous text due to concerns about "giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data." Pet. App. 35a. Not only is that concern unfounded, Pet. 27-32, but it also an extratextual policy judgment that is the proper province of Congress.

Indeed, the Ninth Circuit's decision to engraft a "nonpublic information" requirement onto Section 1030(a)(2)(C) is particularly inappropriate because Congress placed such a limitation in a neighboring provision, Section 1030(a)(3), but not in Section 1030(a)(2)(C). Pet. 23-24; *see 3Taps*, 964 F. Supp. 2d 1182–83; *Sandvig*, 2020 WL 1494065, at *8 n.2 (questioning the decision below in light of Section 1030(a)(3)). hiQ's response appears to be that the inclusion of "nonpublic" in Section 1030(a)(3) does not foreclose the possibility that Congress silently incorporated the same limitation into Section 1030(a)(2)(C). Opp. 18. That is wholly unpersuasive: "the contrast between these two paragraphs makes clear that Congress knows how to impose express limits" when it so desires. *Hardt v. Reliance Standard Life Ins. Co.*, 560 U.S. 242, 252 (2010).

By any "plain and ordinary meaning" (Pet. App. 23a) of the term "without authorization," LinkedIn re-

voked whatever authorization hiQ may have had to access its website when it informed hiQ via a cease-and-desist letter that it did not have permission to scrape data from LinkedIn's site, and implemented additional technical blocks. It does not matter whether that withdrawal of access is called a "ban," a lack of "official permission," or "a lack of 'authorization,'" Pet. App. 24a—those formulations are indistinguishable. A party acts "without authorization" when it circumvents technical barriers and scrapes data even after receiving a cease-and-desist letter.

b. hiQ attempts to shore up its textual argument with legislative history, Opp. 16-17, but this Court "do[es] not resort to legislative history to cloud a statutory text that is clear." *Ratzlaf v. United States*, 510 U.S. 135, 147–48 (1994). In any event, hiQ concedes the history indicates that trespass law provides guidance on the proper interpretation of the CFAA. Opp. 16. Black letter trespass law gives property owners the right to revoke access to their property at any time, regardless of whether the property is otherwise publicly accessible, Pet. 22-23, which is consistent with legislative history indicating that Congress wanted Section 1030(a)(2) to protect privacy, Pet. 26.

c. hiQ also resorts to the rule of lenity, contending that any statutory ambiguity must be interpreted against potential criminal liability. Opp. 18-19. But "[t]he rule [of lenity] applies only when, after consulting traditional canons of statutory construction, we are left with an ambiguous statute." *Shular v. United States*, 140 S. Ct. 779, 787 (2020) (citation and internal quotation marks omitted). No such ambiguity exists here. *Supra* pp. 4-6; *3Taps*, 964 F. Supp. 2d at 1185. And concerns about uncertainty are misplaced where, as here, liability would be triggered by disregarding an individualized cease-and-desist letter. *See Facebook,*

Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016).

d. Finally, hiQ's invocation of constitutional avoidance (Opp. 19-21) misunderstands and misapplies that doctrine. The avoidance canon comes into play only where "the statute [is] genuinely susceptible to two constructions." *Almendarez-Torres v. United States*, 523 U.S. 224, 238 (1998). Here, the traditional tools of statutory construction "point significantly in one direction." *Id.*

In any event, hiQ has not raised any "grave doubts" regarding the constitutionality of Section 1030(a)'s ordinary meaning. *Rust v. Sullivan*, 500 U.S. 173, 191 (1991) (citation omitted). As a threshold matter, LinkedIn is not a state actor. *See Manhattan Cmty. Access Corp. v. Halleck*, 139 S. Ct. 1921, 1930 (2019) ("[A] private entity who provides a forum for speech is not transformed by that fact alone into a state actor."). Moreover, private parties may not "claim special protection from governmental regulations of general applicability simply by virtue of their First Amendment protected activities." *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 705 (1986). Neutral laws protecting private property against unauthorized intrusion may be enforced without raising First Amendment concerns. *See Lloyd Corp. v. Tanner*, 407 U.S. 551, 568 (1972). The CFAA is just such a law, regulating conduct independently of whether that conduct has any connection to expressive activity. *3Taps*, 964 F. Supp. 2d at 1186 n.8.

By the same token, hiQ has no First Amendment right to take information from a private website operator that has decided not to share it. *Halleck*, 139 S.

Ct. at 1930; *Va. Bd. Of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 756 (1976) (right to access information presupposes "a willing speaker").[2]

C. The Decision Below Raises Issues of Exceptional Importance that Warrant Immediate Review

a. The consequences of preventing website operators from protecting their servers and users from large-scale data-scraping by unauthorized bots are clear and exceedingly detrimental. Pet. 27-31. hiQ brushes off these concerns because "[t]his case deals only with profiles made visible to the general public." Opp. 13 (quoting Pet. App. 3a). But that argument obscures more than it illuminates. LinkedIn's members have chosen to make their information available for viewing *on LinkedIn's website*. They have done so in part because of the agreement they enter with LinkedIn, which places limitations on the use of that information, including the rights that LinkedIn grants them to restrict access to or remove their information. When hiQ scrapes that data on massive scale and makes it available elsewhere, however, LinkedIn's members lose their ability to control where and with whom their personal information is shared, and to remove it from the Internet.

Thus, for example, through scraping LinkedIn, hiQ's Keeper product analyzes every change LinkedIn members make to their profiles, providing their employers with an individualized "flight risk" score assessing the likelihood that the person may leave the

---

[2] *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017) is not to the contrary. It merely prevented a *State* from banning all access to a website where the website would otherwise permit access. *Id.* at 1737. It said nothing that would prevent a private website operator from limiting who may access its property.

company—without members' knowledge, much less consent. hiQ does this even when members have enabled the "Do Not Broadcast" function to specifically conceal updates to their profiles from their connections.

To appreciate the implications of the Ninth Circuit's decision beyond LinkedIn, one need look only at Clearview. Clearview deploys bots to engage in systemic scraping of social media and other websites, without consent of the operators or their users, to amass a massive facial-recognition database. *See* Pet. 4-5, 28-29; EPIC Br. at 16-24. hiQ ignores Clearview, but Clearview's scraping, which the decision below greenlights just as surely as it does hiQ's scraping, puts the lie to hiQ's suggestion that the decision has no implications for data control and privacy. Because of the decision below, any information placed on any publicly accessible website is available for anyone to take and exploit for any purpose in perpetuity. Indeed, hiQ embraces the decision below precisely because it "prevents companies … from taking legal action to protect their users' privacy." EPIC Br. at 21.

b. hiQ separately contends that LinkedIn exploits member data in "precisely the same" way as hiQ. Opp. 13-14. That is false and belied by the record.

LinkedIn's products protect user privacy in ways that hiQ's do not. Unlike hiQ's products, LinkedIn's tools do not provide members' *current employers* with information about whether they plan to leave their jobs, and they respect the "Do Not Broadcast" feature. Pet. 8; Pet. App. 13a n.7. Moreover, any use by LinkedIn of member data is limited by LinkedIn's User Agreement and Privacy Policy. Pet. App. 46a. But like other third-party scrapers, hiQ is "not bound by the user agreements of the websites they scrape,

nor do they generally provide similar rights to consumers whose data was scraped." EPIC Br. at 13. hiQ has no relationship with LinkedIn's members, and respects none of the limitations to which LinkedIn agrees with its members.[3]

D. This Case Is a Good Vehicle for This Court's Review

hiQ has identified no vehicle concerns that would justify forgoing review.

hiQ first points to the preliminary injunction posture of the case. Opp. 22-23. But this Court regularly reviews decisions affirming (or denying) preliminary injunctions when, as here, the decision definitively construes a federal statute. *See* Pet. 27 n.10 (citing cases). Tellingly, none of the cases hiQ cites involved a petition seeking review of a preliminary injunction decision. Opp. 22.

Next, hiQ notes that the case is not yet final. Opp. 22-23 & n.10. But it is common for this Court to decide a threshold issue in a case, even if there are remaining issues to be litigated on remand. *See, e.g.*, *Intel Corp. Inv. Policy Comm. v. Sulyma*, 140 S. Ct. 768 (2020). And hiQ has not identified any way in which further proceedings could result in a favorable outcome for LinkedIn on the CFAA issue.[4]

---

[3] hiQ suggests that any concerns about data privacy should be left to Congress. Opp. 15. But Congress already acted by passing Section 1030(a)(2), which hiQ admits is aimed at protecting privacy. Opp. 2. Any interpretation of Section 1030(a)(2)(C) will have profound privacy consequences, which counsels in favor of review.

[4] hiQ's preemption argument interposes no barrier to review. The district court has already indicated that LinkedIn's interpretation of the CFAA would require preemption of hiQ's state law claims. *See* Pet. App. 55a.

E. The Court Should Consider This Case Together With *Van Buren v. United States*

This Court's grant of certiorari in *Van Buren v. United States*, No. 19-783, strengthens the case for review here. Section 1030(a)(2)(C) prohibits obtaining information by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access." While *Van Buren* addresses the meaning of "exceeds authorized access," this case addresses what it means to act "without authorization." Those questions have each divided the Courts of Appeals, giving this Court the opportunity to provide clarity as to both terms, and ensuring that they are construed harmoniously. It would therefore serve judicial economy to consider the cases together, rather than creating the possibility of future litigation adjudicating how this Court's decision in *Van Buren* bears upon the proper interpretation of "without authorization."

At a minimum, this Court should hold LinkedIn's petition pending the outcome of *Van Buren*. In evaluating claims that an individual has "exceed[ed] authorized access" or acted "without authorization," courts have often opined on the meaning of "authorization" in a manner that bears on both terms. *See, e.g.*, *EF Cultural Travel*, 318 F.3d at 62-63 (discussing how a "lack of authorization" could be established to prove that a scraper "exceed[ed] authorized access"); *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011) (comparing and construing both terms); *Int'l Airport Centers, LLC v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (same).

CONCLUSION

The petition for a writ of certiorari should be granted. Alternatively, the petition should be held pending *Van Buren v. United States*, and then disposed of as appropriate in light of the disposition of that case.

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

BRIAN P. GOLDMAN
ORRICK HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105
(415) 773-5700

DONALD B. VERRILLI, JR.
Counsel of Record
JONATHAN S. MELTZER
MUNGER, TOLLES & OLSON LLP
1155 F Street NW, 7th Floor
Washington, DC 20004
(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

July 16, 2020