No. 19-1116

IN THE

Supreme Court of the United States

LINKEDIN CORPORATION,

Petitioner,

v.

HIQ LABS, INC.,

Respondent.

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

BRIEF IN OPPOSITION

R. COREY WORCESTER
Counsel of Record
ELLYDE R. THOMPSON
QUINN EMANUEL URQUHART & SULLIVAN, LLP
51 Madison Avenue
New York, NY 10010
(212) 849-7000
coreyworcester@quinnemanuel.com

Counsel for Respondent

June 25, 2020

QUESTION PRESENTED

Whether a professional networking website may rely on the Computer Fraud and Abuse Act's prohibition on "intentionally access[ing] a computer without authorization" to prevent a competitor from accessing information that the website's users have shared on their public profiles and that is available for viewing by anyone with a web browser.

RULE 29.6 STATEMENT

hiQ Labs, Inc. has no parent company and no publicly held company owns 10% or more of hiQ Labs Inc.'s outstanding common stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Rules and Statutes

Other Authorities

INTRODUCTION

Respondent hiQ Labs, Inc. ("hiQ") respectfully submits this brief in opposition to the petition for a writ of certiorari filed by LinkedIn Corporation ("LinkedIn"). The unanimous decision of the court of appeals affirming the preliminary injunction reflects a commonsense and correct application of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. 1030. Petitioner has identified no basis for further review.

This case concerns a business dispute between competitors during which petitioner LinkedIn attempted to invoke the civil liability of the CFAA as a shield for its efforts to shut down hiQ's business. hiQ is a small data analytics company that analyzes data that LinkedIn users have elected to make publicly available. hiQ analyzes the data to provide recruiting and retention insights to Fortune 500 companies. In 2017, around the same time LinkedIn announced it would provide similar analytics services to companies based on the public profiles of LinkedIn users, LinkedIn informed hiQ that it could no longer gather public data from the LinkedIn 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.

At the preliminary injunction stage, the district court ruled that LinkedIn was unlikely to show that its attempt to block hiQ from collecting public data rendered hiQ's access to the LinkedIn site "without authorization" under Section 1030(a)(2) of the CFAA. Pet. App. 61a-62a. The Ninth Circuit affirmed,

reasoning 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," such that "[h]iQ has therefore raised serious questions about whether LinkedIn may invoke the CFAA to preempt hiQ's possibly meritorious tortious interference claim." Pet. App. 32a.

The court of appeals' correct ruling provides no basis for this Court's review. The interpretation of the phrase "without authorization" to exclude viewing and gathering *public* information—access to which requires no permission—flows naturally from the plain meaning of the phrase. Even were the text ambiguous, the legislative history supports this interpretation, as it confirms that the "the premise of this subsection [18 U.S.C. 1030(a)(2)] is privacy protection." S. Rep. No. 104-357, at 7 (1996) (Conf. Rep.). And the court of appeals' reading comports with the rule of lenity and avoids serious constitutional concerns that otherwise would need to be addressed, such as whether allowing a private party to create civil and criminal liability by restricting the viewing and collection of public data is consistent with the First Amendment.

Contrary to petitioner's assertion, the decision below creates no conflict with any decision of any other court of appeals. The only federal appellate case petitioner identifies dates back to 2003 and concerns the action of a former employee using confidential information to decode information not otherwise usable on the public-facing website at issue. Far from deciding as part of its holding any question on the scope of the CFAA, *EF Cultural Travel BV v. Zefer*

Corp., 318 F.3d 58 (1st Cir. 2003), stands only for the uncontroversial proposition that an injunction may be enforced against a third party. Indeed, none of the cases on which petitioner relies addresses the specific issue on which the Ninth Circuit ruled—that the CFAA's reference to access "without authorization" does not implicate access to publicly available information for which no authorization is required.

The supposed privacy concerns petitioner raises rest on a flawed premise. The data at issue here does not involve any non-public information, but rather information LinkedIn users have chosen to post publicly. LinkedIn itself uses this same information in nearly the same way as hiQ. And LinkedIn's attacks against automated computer processes that collect information in an efficient manner—so-called "bots"—have no bearing on the interpretation of the CFAA, which does not distinguish between manual and automated means of accessing information.

Finally, even if this Court were otherwise inclined to address the scope of unauthorized access under the CFAA, it should not do so here. This case has not proceeded to final judgment—indeed, LinkedIn has yet to answer the amended complaint and a motion to dismiss is pending. As a result, the CFAA might not even be material to the resolution of this dispute. This Court, moreover, should permit other courts of appeals to weigh in on the proper interpretation of "without authorization" to determine whether there is any true disagreement as to the meaning of that phrase.

For all these reasons, the petition should be denied.

COUNTERSTATEMENT

1. As originally enacted, the CFAA was designed to prevent the crime of computer hacking. See *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012) (citing S. Rep. No. 99-432, at 9 (1986) (Conf. Rep.)). Initially directed at only a narrow range of computers containing national security information or financial data and those operated by or on behalf of the government, Congress has expanded the CFAA's reach over the years. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102, 98 Stat. 2190, 2190-91; Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(g)(4), 100 Stat. 1213; 18 U.S.C. 1030.

In 1996, when Congress broadened the scope of computers covered by the CFAA, Congress maintained that "the premise of this subsection [1030(a)(2)] is privacy protection." S. Rep. No. 104-357, at 7; *id.* ("The bill would amend section 1030(a)(2) to increase protection for the privacy and confidentiality of computer information."). Section 1030(a)(2)(C) of the CFAA prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." 18 U.S.C. 1030(a)(2)(C). The term "protected computer" is defined as any computer "used in or affecting interstate or foreign commerce or communication." *Id.* 1030(e)(2)(B).

Violations of the CFAA, and of Section 1030(a)(2) in particular, give rise to both civil and criminal liability. *Id.* 1030(c) (violations punished by a "fine," "imprisonment," or "both"). The CFAA permits private civil suits brought by "[a]ny person who

suffers damage or loss by reason of a violation" as a means "to obtain compensatory damages and injunctive relief or other equitable relief," subject to certain conditions. *Id.* 1030(g).

2. Respondent hiQ is a data analytics start-up that applies predictive data science to provide its Fortune 500 clients with "people analytics"—insights into their workforce. To do so, hiQ analyzes public information on the LinkedIn website. hiQ uses automated processes that gather publicly available data in raw form. Such an automated data gathering process often is referred to as "web robot (or 'bot')." Pet. App. 3a, n.2. The use of bots presents a highly efficient means of collecting data for analysis.

hiQ then analyzes the public data to provide its clients with two primary services: "Keeper," a product that identifies the employees most likely to be recruited away from a client; and "SkillMapper," an analysis of the skill set of a client's employees. 5ER-988 (¶¶ 4-6). The data hiQ gathers to conduct such analyses includes only that information that hiQ's clients' employees have designated as public on LinkedIn, such as their names, job titles, skills, and work histories. Users decide what information is available publicly. 5ER-901 ("You control the visibility and reach of your LinkedIn profile."). To facilitate this control, LinkedIn allows members to specify which profile portions are visible to the general "public" and which are visible to only LinkedIn members. 5ER-899.

3. The dispute between LinkedIn and hiQ arose in 2017. At that time, LinkedIn had been aware for years that hiQ created business-insight products based on information from the public profiles of

LinkedIn users. LinkedIn employees had participated in conferences that hiQ held related to these very products. 5ER-989 (¶¶ 12, 13); 4ER-756 (¶¶5, 6, 8). In late 2016 and early 2017, hiQ's former CEO attended in-person meetings with LinkedIn personnel discussing hiQ's business. 5ER-990 (¶14).

In May 2017, however, LinkedIn sought to restrict hiQ's ability to use the public profile data of LinkedIn users. Despite the fact that LinkedIn disclaims any ownership over the data users post for publication on its site, 5ER-893, LinkedIn's counsel sent hiQ a letter stating that hiQ was improperly "access[ing] and copy[ing]" public profile information, 5ER-990 (¶ 15), 5ER-920. The letter demanded that hiQ immediately cease and desist accessing LinkedIn's website or any data stored there. 5ER-921. LinkedIn's letter accused hiQ of violating LinkedIn's User Agreement, state trespass law, the CFAA, California Penal Code § 502, and the Digital Millennium Copyright Act ("DMCA"). *Id.*

Around the same time LinkedIn sent its letter to hiQ, LinkedIn announced it would provide services similar to hiQ's products in an effort to "leverag[e] content and data that members are already sharing publicly." 5ER-932, 5ER-941. One month later, LinkedIn's CEO announced the company would launch a product similar to hiQ's SkillMapper, which would analyze skills data from member profiles. 4ER-0583. "Since then, LinkedIn has announced a new product, Talent Insights, which analyzes LinkedIn data to provide companies with such data-driven information." Pet. App. 6a-7a.

4. LinkedIn's cease-and-desist letter not only threated criminal and civil liability for hiQ's

conduct—of which LinkedIn had long been aware—but it also threatened hiQ's business model. Absent access to public profile data, hiQ would be unable to offer the services it contracted to provide to clients. The specter of the destruction of hiQ's business caused hiQ to lose investors and employees. Pet. App. 48a.

Unable to access LinkedIn's website without risk that LinkedIn would refer it for criminal prosecution, hiQ sued to enjoin LinkedIn's conduct as violating California's unfair competition law and constituting intentional interference with contract.[1] At the preliminary injunction stage, the district court enjoined LinkedIn's conduct aimed at preventing hiQ from accessing public profiles, holding that hiQ had satisfied the likelihood of success inquiry as to its unfair competition claim. Pet. App. 72a, 75a-76a. The district court also rejected LinkedIn's defense that the CFAA barred hiQ's state-law claims, reasoning that hiQ raised serious questions as to "whether visiting and collecting information from a publicly available website may be deemed 'access' to a computer 'without authorization' within the meaning of the CFAA where the owner of the web site has selectively revoked permission." Pet. App. 52a.

5. The court of appeals affirmed in a unanimous decision. Pet. App. 1a-36a. The court concluded that hiQ met each factor required to obtain preliminary injunctive relief. Pet. App. 9a-35a. Absent access to public profile data on LinkedIn, hiQ was likely to experience the destruction of its business. Pet. App.

---

[1] hiQ also sought a declaratory judgment that LinkedIn could not lawfully invoke the CFAA, the DMCA, California Penal Code § 502(c), or the common law of trespass, but did not seek injunctive relief based on those claims.

9a-11a. hiQ already had lost both financing for its business and employees. Pet. App. 10a.

The court of appeals likewise held the balance of equities and public interest favored hiQ. Pet. App. 11a-14a. Although LinkedIn asserted the privacy interest of its members as a public interest that caused the equities to tip in its favor, the Ninth Circuit determined that LinkedIn's privacy arguments were overstated. Pet. App. 12a. "There 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." Pet. App. 12a (quoting LinkedIn's privacy policy, which states that "[a]ny information you put on your profile and any content you post on LinkedIn may be seen by others" such that users should not "post or add personal data to your profile that you would not want to be public").

LinkedIn's privacy assertion was further undermined by LinkedIn's own analytics product that allowed recruiters to track profile changes for potential candidates. Pet. App. 13a. The court of appeals "agree[d] 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." Pet. App. 35a. The court of appeals further concluded that LinkedIn's anti-competitive conduct satisfied the likelihood of success

inquiry for hiQ's claims for intentional interference with contract. Pet. App. 15a-22a.

The Ninth Circuit addressed the CFAA only with regard to LinkedIn's defense that the CFAA preempted hiQ's state law claims. Pet. App. 22a-34a. In this analysis, the court of appeals first assessed whether the CFAA even applied to hiQ's collection and analysis of the public profile data on LinkedIn and concluded it did not.

First, the 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." Pet. App. 24a. Such a reading is consistent with the dictionary definition of the word "authorization." Pet. App. 24a (citing BLACK'S LAW DICTIONARY (10th ed. 2014) (defining "authorization" as "[o]fficial permission to do something; sanction or warrant")).

Second, the court of appeals 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." Pet. App. 25a (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 'to increase protection for the privacy and confidentiality of computer information.'" Pet. App. 27a (quoting S. Rep. No. 104-357, at 7). Based on this legislative history, the court of appeals 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." Pet. App. 27a.

Third, the Ninth Circuit concluded that prior CFAA decisions had not decided whether "without authorization" extended to websites accessible to "anyone with a web browser." Pet. App. 29a. 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." Pet. App. 29a-31a.

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. Pet. App. 31a-32a.

Petitioner filed a petition for *en banc* review, which was denied without dissent. Pet. App. 77a.

REASONS FOR DENYING THE WRIT

I. THE PETITION DOES NOT WARRANT REVIEW

The decision below does not warrant this Court's grant of certiorari. The decision of the court of appeals is correct and does not conflict with any decision of this Court or any other federal court of appeals. Nor does it involve any important question of federal law warranting the Court's immediate intervention.

A. There Is No Conflict Supporting Review

Petitioner's contention (Pet. 15) that a "[c]lear and [d]irect [c]ircuit [c]onflict" exists rests on a single First Circuit decision from 2003, *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003). But that purported conflict is wholly illusory because the First Circuit did not even decide as part of its holding the question presented here. Indeed, the decision in that case required no determination of the scope of the CFAA at all.

EF Cultural Travel BV v. Zefer Corp. held that a preliminary injunction premised on *another party's* misuse of confidential information was binding on the defendant, Zefer Corp., which was "constrained only in helping a tentatively-identified wrongdoer in exploiting that confidential information." 318 F.3d at 64. The First Circuit simply ruled that Zefer Corp.—which had been hired to create a tool used to gather the information from the plaintiff's website—was "merely precluded, like anyone else with notice, from acting in concert with, on behalf of, or at the direction of" the enjoined party. *Id.* at 63 ("There is no reason why Zefer should be freer than any other third party who was never in this litigation to assist EF to violate the injunction against it or to do so on EF's behalf or at its direction. As we read the injunction, that is all that is forbidden."). The First Circuit never even considered the issue that the Ninth Circuit decided below—whether "access 'without authorization' limits the scope of the statutory coverage to computer information for which authorization or access

permission, such as password authentication, is generally required." Pet. App. 27a-28a.[2]

Lacking a true circuit conflict, petitioner relies upon a purported conflict with several disparate district court cases. Those cases do not provide any basis for this Court's review. See Sup. Ct. R. 10. They also do not address the issue the court of appeals decided.[3]

---

[2] See *Sandvig v. Barr*, Civil No. 16-1368 (JDB), 2020 WL 1494065, at *12 n.3 (D.D.C. Mar. 27, 2020), *appeal filed*, Dkt. 20-5153 (D.C. Cir. May 28, 2020) (explaining that "the First Circuit's holding relied upon the 'relatively narrow grounds' that the injunction applied to 'anyone else with notice' and thus 'precluded [Zefer] from acting to assist the enjoined party from violating the decree [and] from doing so on behalf of that party'") (citing *EF Cultural Travel BV*, 318 F.3d at 61, 63).

[3] *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013) (addressing on motion to dismiss defendant's position that, "by making the classified ads on its website publicly available, craigslist has 'authorized' the world, including 3Taps, to access craigslist.org"); *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595-97 (E.D. Pa. 2016) (assuming on motion to dismiss that "Resultly (and any other web user) had permission to access information on QVC.com, a publicly available website"); *Sw. Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 437 (N.D. Tex. 2004) (not considering on motion to dismiss whether authorization is required for a public website in the first place); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 244, 251 (S.D.N.Y. 2000), *aff'd as modified*, 356 F.3d 393 (2d Cir. 2004) (same); *Ticketmaster LLC v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1102-03, 1113 (C.D. Cal. 2007) (stating without discussion that "[i]t appears likely that Plaintiff will be able to prove that Defendant gained unauthorized access to, and/or exceeded authorized access to, Plaintiff's protected computers"); *United States v. Lowson*, Criminal No. 10-114 (KSH), 2010 WL 9552416, at *5 (D.N.J. Oct. 12, 2010) (same).

For this reason, petitioner's claim that "the Ninth Circuit's opinion breaks sharply with every federal court that has interpreted Section 1030(a)" (Pet. 4), is misleading. It is also incorrect: A court recently reached the same conclusion as the Ninth Circuit. See, *e.g.*, *Sandvig v. Barr*, Civil Action No. 16-1368 (JDB), 2020 WL 1494065, at *8 (D.D.C. Mar. 27, 2020), *appeal filed*, Dkt. 20-5153 (D.C. Cir. May 28, 2020) (holding that wording of Section 1030(a)(2) "thus contemplates a view of the internet as 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 there exists no circuit conflict on the question presented, the petition should be denied.

B. There Is No Issue Of Exceptional Importance Warranting Review

LinkedIn fares no better in arguing (Pet. 27) that the petition presents an issue of exceptional importance.

First, LinkedIn's suggestion (Pet. 27-28) that this Court's review is needed to protect the privacy interests of hundreds of millions of users of websites disregards that, as the court of appeals explained, "[t]his case deals only with profiles made visible to the general public." Pet. App. 3a. All of the information hiQ gathers is publicly available, and LinkedIn's users have chosen to make it so. Pet. App. 2a-3a. Indeed, LinkedIn's invocation of privacy concerns is particularly disingenuous given that LinkedIn itself seeks to use and monetize precisely the same user-generated information on its site in the same way hiQ used it for years before LinkedIn decided to enter the

market hiQ innovated. Pet. App. 7a & n.6 (referring to LinkedIn's "Talent Keeper" tool, which provides similar analysis to hiQ's products); Pet. App. 13a (referring to LinkedIn's "Recruiter" tool, which allows subscribers to "export data from members' public profiles, such as 'name, headline, current company, current title, and location'"). As the Ninth Circuit concluded, "there 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." Pet. App. 12a.

Second, LinkedIn wrongly seeks (Pet. 3, 9, 28) to distinguish between any member of the public and bots. The CFAA does not support drawing such a line. Any interpretation of the CFAA will be universally applicable. If anything, LinkedIn's argument reinforces the concern of the courts below that LinkedIn is seeking to be the one deciding whose access to its website runs afoul of federal law. See Pet. App. 35a ("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.").[4]

---

[4] LinkedIn's argument that "if the Ninth Circuit rule persists, Craigslist could not prevent an entity from scraping data to 'essentially replicate[] the entire craigslist website,'" Pet. 32 (quoting *3Taps*, 964 F. Supp. 2d at 1180), ignores entirely the other mechanisms companies have available to prevent such use.

Finally, and in any event, data privacy in the age of the Internet—even if relevant here—presents a complex issue that requires balancing various interests, such as the use of publicly available data to promote academic research, and is therefore better suited for the legislative branch to address as needed. Congress contemplated as much in its 1996 amendments to the CFAA. S. Rep. No. 104-357, at 5 ("As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime. The NII Protection Act will likely not represent the last amendment to this statute[.]").

II. THE DECISION BELOW IS CORRECT

The petition should be denied for the further reason that the decision of the court of appeals is correct.

A. The Decision Below Properly Interpreted The CFAA

The CFAA imposes civil and criminal liability on whoever "intentionally accesses a computer without authorization . . . and thereby obtains . . . information from any protected computer." 18 U.S.C.

The CFAA—which is intended to protect privacy and confidentiality—need not be used to address such situations, which may be subject to claims for "copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy," as the Ninth Circuit noted. Pet. App. 33a (citing *Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 561 (S.D.N.Y. 2013) (denying fair use defense to claim of copyright violation in scraping and aggregating copyrighted news articles)).

1030(a)(2)(C). "Without authorization" necessarily presupposes a predicate that access to the protected computer requires "authorization." Thus, as the Ninth Circuit correctly concluded, "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." Pet. App. 32a.

Petitioner wrongly contends (Pet. 21) that, in giving the text its plain meaning, the court of appeals "effectively convert[ed] the statutory phrase 'without authorization' into 'without prior authorization in the form of a password or other authentication barrier.'" That argument ignores the Ninth Circuit's focus on publicly available information. The Ninth Circuit used a password requirement only as an example of a type of "authorization" and confirmed that "authorization is only required for password-protected sites or sites that otherwise *prevent the general public from viewing the information*." Pet. App. 27a (emphasis added).[5]

Petitioner's argument (Pet. 22) that trespass law supports its own interpretation of the CFAA misunderstands the court of appeals' decision. The references to trespass in the CFAA's legislative history must be read in conjunction with the legislative history for the 1996 amendments—which is exactly what the Ninth Circuit did. Pet. App. 25a-27a. Although the narrow version of the CFAA as

---

[5] The Ninth Circuit did not "acknowledge[] that the textual basis for reading the statute this way is 'debatable,'" as petitioner claims (Pet. 21), but rather stated that, "*even if* this interpretation is debatable, the legislative history of the statute confirms [this] understanding." Pet. App. 24a (emphasis added).

originally enacted applied only to a small subset of computers that necessarily encompassed private information, the legislative history for the 1996 expansion of the CFAA made clear that the CFAA still would apply only to private and confidential information on computers. S. Rep. No. 104-357, at 7. The Ninth Circuit thus correctly concluded that Section 1030 "is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort." Pet. App. 27a. As a result, "[w]ith regard to such information, the 'breaking and entering' analogue invoked so frequently during congressional consideration has no application, and the concept of 'without authorization' is inapt." Pet. App. 28a.[6]

Petitioner's attempt (Pet. 25-27) to call into question the Ninth Circuit's conclusion through the use of legislative history also fails. The legislative history states that "the premise of this subsection [Section 1030(2)(2)] is *privacy protection*" and that the bill sought to "amend section 1030(a)(2) to increase protection for the *privacy and confidentiality* of computer information." S. Rep. No. 104-357, at 7 (emphasis added).[7]

---

[6] Petitioner's lengthy discussion (Pet. 22-23) of entry to restaurants offers no useful analogy. But, if an analogy from the CFAA could be drawn, it would be to the "private eating club[s]" that petitioner contends would fall within the scope of the Ninth Circuit's decision, Pet. 23, which is consistent with the legislative history confirming application to "private and confidential" information.

[7] Contrary to LinkedIn's assertion (Pet. 25), the Ninth Circuit did not "focus[] on the *wrong* legislative history" but rather relied on the 1996 Senate report that made clear that the expansion of

Likewise, the addition of "nonpublic" to Section 1030(a)(3)—concerning government computers—offers no support for LinkedIn's position, despite LinkedIn's argument to the contrary (Pet. 24). Although the relevant section here—Section 1030(a)(2)(C)—is framed in terms of obtaining "information from a protected computer," Section 1030(a)(3) does not incorporate the phrase "protected computer" but instead refers to "any nonpublic computer of a department or agency of the United States," *id.* 1030(a)(3). As a result, the use of "nonpublic" does not affect the meaning of "without authorization." There is no debate over whether the computers at issue here are "protected computers" because they are "used in or affecting interstate or foreign commerce or communication." *Id.* 1030(e)(2)(B). And thus LinkedIn's purported "structure" argument has no relevance to a determination of the question presented.[8]

Finally, the rule of lenity further justifies the Ninth Circuit's correct decision. A violation of Section 1030(a) carries with it both civil and criminal penalties. "Because [this Court] must interpret the

---

Section 1030(a)(2) to any "protected computer" was intended to cover "private and confidential" information. S. Rep. No. 104-357, at 7.

[8] Facing this clear congressional intent that renders its interpretation inconsistent with the legislative history, LinkedIn argues that "the Ninth Circuit's construction actually undermines privacy protection." Pet. 26. But, as discussed *infra*, one of several flaws with LinkedIn's counterintuitive argument—in addition to being based on unproven factual assertions—is that it depends on an interpretation of "without authorization" that distinguishes between manual and automated access, which the CFAA does not do.

statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies." *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). Application of the rule of lenity ensures that "no citizen should be held accountable for a violation of a statute whose commands are uncertain." *United States v. Santos*, 553 U.S. 507, 514 (2008) ("The rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them."). Here, even if the meaning of "without authorization" were ambiguous after considering the text, legislative history, and purpose of the CFAA, the court of appeals' interpretation adopts the narrower reading, as the rule of lenity requires.

B. The Decision Below Avoids An Interpretation That Would Raise Serious Constitutional Concerns

The Ninth Circuit's decision also is compelled by the doctrine of constitutional avoidance because LinkedIn's proposed statutory interpretation raises serious concerns about the constitutionality of the CFAA.

Even if LinkedIn's proposed interpretation of the CFAA provision were plausible (it is not), "where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988). Such an analysis requires assessment of only whether a proposed interpretation "presents a significant risk that [constitutional provisions] will be

infringed." *NLRB v. Catholic Bishop of Chi.*, 440 U.S. 490, 502 (1979)).

As explained *supra*, the court of appeals' interpretation is not plainly contrary to Congress' intent of protecting private and confidential information. But LinkedIn's position that individual website owners can subject those who view and collect public data to civil and criminal liability under the CFAA presents serious constitutional problems, in particular a substantial risk of violation of the First Amendment.

A high risk exists that LinkedIn's attempt to restrict unilaterally who can view and gather public information would run afoul of the First Amendment. The First Amendment protects access to information. See *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council*, *Inc.*, 425 U.S. 748, 756-57 (1976) ("[T]his Court has referred to a First Amendment right to receive information and ideas, and that freedom of speech necessarily protects the right to receive.") (citations, internal quotation marks omitted). And this Court has held that the First Amendment protects the right to access the Internet generally, specifically including social media websites. *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735, 1737 (2017) (social media websites, including specifically LinkedIn, "for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge"); Pet. App. 63a n.12 (district court statement that "the

act of viewing a publicly accessible website is likely protected by the First Amendment").[9]

LinkedIn not only seeks to prohibit hiQ outright from engaging in the protected activity of gathering publicly available information but also seeks to wield the CFAA as a tool to chill use of the information on its website that it does not like, whether because it objects to a competitor's use of the data users chose to make public on its site or for any other reason. "A government regulation that allows arbitrary application" violates the First Amendment "because such discretion has the potential for becoming a means of suppressing a particular point of view." *Forsyth Cty., Ga. v. Nationalist Movement*, 505 U.S. 123, 130-31 (1992) (internal quotation marks omitted).

The Ninth Circuit's well-grounded interpretation of "without authorization" avoids the serious constitutional concerns that LinkedIn's proposed interpretation raises. As a result, the doctrine of constitutional avoidance provides yet another reason why the court of appeals' decision is correct.

---

[9] The fact that LinkedIn is not a government body does not insulate its conduct from the reach of the First Amendment, which applies even in a private civil suit for damages. See *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767, 777 (1986) ("[T]he need to encourage debate on public issues that concerned the Court in the governmental-restriction cases is of concern in a similar manner in this case involving a private suit for damages[.]"). Thus, this Court repeatedly has held that the First Amendment protects speech from government suppression sought by private parties in civil cases. See, *e.g.*, *New York Times Co. v. Sullivan*, 376 U.S. 254, 265 (1964) (defamation); *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 917 n.51 (1982) (malicious interference with business).

III. THIS CASE PRESENTS A POOR VEHICLE FOR REVIEW

Even if the question presented warranted review (it does not), this case presents a poor vehicle to consider it.

At the threshold, the decision below concerns a preliminary injunction issued at the very start of the case. This Court typically requires "special circumstances [to] justify the exercise of [its] discretionary certiorari jurisdiction to review [an] interlocutory order." *Office of Senator Mark Dayton v. Hanson*, 550 U.S. 511, 515 (2007); see *Abbott v. Veasey*, 137 S. Ct. 612, 613 (2017) (statement of Roberts, C.J., respecting denial of certiorari) (issues "better suited for certiorari review" after entry of final judgment); *Va. Military Inst. v. United States*, 508 U.S. 946, 947 (1993) (opinion of Scalia, J., respecting denial of certiorari) ("We generally await final judgment in the lower courts before exercising our certiorari jurisdiction.").

As one member of the court of appeals' panel noted in a special concurrence, "appealing from a preliminary injunction to obtain an appellate court's view of the merits often leads to 'unnecessary delay to the parties and inefficient use of judicial resources.'" Pet. App. 37a (Wallace, J., concurring) (quoting *Sports Form, Inc. v. United Press Int'l, Inc.*, 686 F.2d 750, 753 (9th Cir. 1982)). This principle applies even more so here, where petitioner asks this Court to intervene even though a determination of the question presented may not materially advance resolution of the dispute. That is so because, even if the CFAA does apply, LinkedIn also must show that the CFAA preempts hiQ's state-law claims. LinkedIn, however,

is unlikely to be able to do so: The CFAA triggers neither express nor field preemption, and there is no conflict preemption here because the CFAA's civil and criminal penalties for access "without authorization" can easily co-exist with any generally applicable state laws concerning whether a website owner may block certain individuals or entities from public web pages. See *Fla. Lime & Avocado Growers, Inc. v. Paul*, 373 U.S. 132, 142 (1963) ("[F]ederal regulation of a field of commerce should not be deemed preemptive of state regulatory power in the absence of persuasive reasons—either that the nature of the regulated subject matter permits no other conclusion, or that the Congress has unmistakably so ordained."); see also *CDK Global LLC v. Brnovich*, No. CV-19-04849-PHX-GMS, 2020 WL 2559913, at *4 (D. Az. May 20, 2020) ("Plaintiffs have cited no evidence that the CFAA has preempted any state statute in its 35-year history").[10]

In addition, this Court's "ordinary practice" is to "deny[] petitions insofar as they raise legal issues that have not been considered by additional Courts of Appeals." *Box v. Planned Parenthood of Ind. & Ky., Inc.*, 139 S. Ct. 1780, 1782 (2019) (per curiam); *id.* at 1784 (Thomas, J., concurring) ("[F]urther percolation may assist our review of this issue of first impression."); *Arizona v. Evans*, 514 U.S. 1, 23 n.1 (1995) (Ginsburg, J., dissenting) ("We have in many instances recognized that when frontier legal

[10] Likewise, LinkedIn specifically opted not to press certain other claims or defenses at the preliminary injunction stage. Pet. App. 15a (noting LinkedIn chose only "to focus on a defense based on the CFAA, so that is the sole defense to hiQ's claims that we address here" but that LinkedIn asserts that it has "claims under the Digital Millennium Copyright Act and under trespass and misappropriation doctrines").

problems are presented, periods of 'percolation' in, and diverse opinions from, state and federal appellate courts may yield a better informed and more enduring final pronouncement by this Court.").

In this instance, petitioner has identified only one court of appeals case in purported conflict with the Ninth Circuit's decision here. Pet. 15. These two cases are nearly twenty years apart and, as discussed *supra*, the fact-bound First Circuit case actually presents no conflict at all. But, even if it did, the length of time between the cases weighs in favor of awaiting decisions from additional courts of appeals. Indeed, the Internet itself (and the way the public uses it), has changed dramatically in the past twenty years.[11] Thus, the more prudent course is to provide the First Circuit "an opportunity to correct its error without the need for this Court to intervene." *Hittson v. Chatman*, 135 S. Ct. 2126, 2128 (2015) (Ginsburg, J., concurring in the denial of certiorari); see also Stephen M. Shapiro et al., SUPREME COURT PRACTICE ch. 6.37.(I)(1)(11th ed. 2020) (denial warranted where it is "reasonable to expect that the courts that rendered [conflicting decisions] would reconsider their results in light of intervening developments").

---

[11] Petitioner's contention (at 19) that this Court should act now because otherwise measures LinkedIn uses to protect against the collection of data from bots will be subject to copy-cat actions is misplaced. The Ninth Circuit specifically noted that LinkedIn had not challenged the scope of the injunction but that, in any event, "the district court made clear that the injunction does *not* preclude LinkedIn from continuing to engage in 'technological self-help' against bad actors—for example, by employing 'anti-bot measures to prevent, e.g., harmful intrusions or attacks on its server.'" Pet. App. 35a.

This petition therefore presents a stark departure from the petition this Court recently granted in another CFAA case, *Van Buren v. United States*, Dkt. 19-783 (pet. for cert. granted Apr. 20, 2020). The petitioner in *Van Buren* identified a well-developed split between the First, Fifth, Seventh, and Eleventh Circuits and the Second, Fourth, and Ninth Circuits regarding how the improper use of password-protected information should be treated. Pet., *Van Buren v. United States*, at 7-11 (Dec. 18, 2019). The Eleventh Circuit affirmed the CFAA felony conviction there because it was bound by a prior panel decision, but in doing so urged a revisiting of the Eleventh Circuit's approach. *United States v. Van Buren*, 940 F.3d 1192, 1208 (11th Cir. 2019). The split among seven courts of appeals that had decided the issue in *Van Buren* highlights the absence of such a conflict here.[12]

[12] There is no need to hold the petition for a decision in *Van Buren* because, as LinkedIn itself has acknowledged (Pet. 18 n.8), the petitions present "distinct" issues.

CONCLUSION

The petition should be denied.

Respectfully submitted,

R. COREY WORCESTER
Counsel of Record
ELLYDE R. THOMPSON
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
51 Madison Avenue
New York, NY 10010
(212) 849-7000
coreyworcester@
quinnemanuel.com

Counsel for Respondent

June 25, 2020