CASE NO. 17-16783

In the United States Court of Appeals
For the Ninth Circuit

HIQ LABS, INC.
Plaintiff-Appellee,

v.

LINKEDIN CORPORATION
Defendant-Appellant,

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

APPELLANT'S OPENING BRIEF

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

MUNGER, TOLLES & OLSON LLP
DONALD B. VERRILLI, JR.
CHAD I. GOLDER
1155 F Street N.W., 7th Floor
Washington, DC 20004-1361
Telephone: (202) 220-1100
Facsimile: (202) 220-2300

Attorneys for Defendant-Appellant *LinkedIn Corporation*

(additional counsel listed inside cover page)

(additional counsel continued from cover page)

ORRICK, HERRINGTON & SUTCLIFFE LLP

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

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

BRIAN P. GOLDMAN
405 Howard Street
San Francisco, CA 94105
(415) 773-5700

Attorneys for Defendant-Appellant *LinkedIn Corporation*

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Defendant-Appellant LinkedIn Corporation states that it is a wholly owned subsidiary of Microsoft Corporation ("Microsoft"). Microsoft is a publicly traded company. No person or entity owns more than 10% of Microsoft's outstanding common stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

FEDERAL CASES

STATE CASES

FEDERAL STATUTES

LEGISLATIVE MATERIALS

TREATISES

OTHER AUTHORITIES

INTRODUCTION

This case poses the question whether LinkedIn has the right to protect itself from anonymous data-scraping "bots" deployed by hiQ—a company that seeks to free ride on the fruits of LinkedIn's labor and investment by scraping massive volumes of data from LinkedIn's computer servers and then repackaging and selling that data to others. Decisions of this Circuit and other courts uniformly establish that LinkedIn has this right. Defying that precedent, the district court issued a first-of-its-kind *mandatory* preliminary injunction that barred LinkedIn from defending itself. That ruling ignored bedrock antitrust principles by imposing on LinkedIn a duty to assist a would-be competitor. *Verizon Commcn's, Inc. v. Law Offices of Curtis V. Trinko*, 540 U.S. 398, 411 (2004). And it blessed precisely the sort of "technological gamesmanship" that this Court has held to be unlawful under the Computer Fraud and Abuse Act (CFAA). *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016). It should be reversed.

LinkedIn invested fifteen years and billions of dollars to become a leader in professional networking. 5ER-824. hiQ's business model, by contrast, is "wholly dependent" on LinkedIn's hard work and success. 1ER-1. Rather than putting in the effort to build its own business, hiQ expropriates member data from LinkedIn's servers on a massive scale, and then turns around and sells that data to companies that wish to furtively monitor their employees. LinkedIn interposed technological

barriers to deny access to hiQ's bots, but hiQ circumvented those barriers. In accordance with this Court's instructions in *Power Ventures*, LinkedIn then implemented additional technical barriers and sent hiQ a cease-and-desist letter, informing hiQ that "'[a]ny future access of any kind' to LinkedIn's servers by hiQ would be 'without permission and without authorization from LinkedIn,'" and would therefore violate the CFAA's prohibition on computer trespass. 1ER-3 (quoting 4ER-743); 4ER-766. In response, hiQ sued to regain access to LinkedIn's servers and sought a preliminary injunction.

The district court granted that injunction, which requires LinkedIn to disable the technical measures it had been using to attempt to block hiQ's bots and forbids LinkedIn from invoking the CFAA against future intrusions by hiQ. In so doing, the court gave short shrift (in a few pages at the end of its opinion) to the "most important … threshold" question: whether hiQ had any substantive legal entitlement to an injunction. *Disney Enters., Inc. v. VidAngel*, No. 2:16-cv-04109, Slip Op. at 12 (9th Cir. Aug. 24, 2017).

Without conducting anything like the serious analysis needed to evaluate an antitrust claim, the court summarily pronounced that hiQ had a potential cause of action under the California Unfair Competition Law (UCL). But hiQ's entire UCL claim rests on the false notion that LinkedIn had an antitrust duty to provide its data to hiQ on hiQ's own terms. It did not, as Supreme Court precedent

unambiguously establishes. *E.g.*, *Trinko*, 540 U.S. 398. Worse than that, the district court's ruling poses a grave risk to competition and innovation. "Without some confidence that they can control access to their own property, real or intellectual, how many firms would be deterred from undertaking the risks associated with, say, a significant new endeavor or facility?" *Four Corners Nephrology Assocs., P.C. v. Mercy Med. Ctr. of Durango*, 582 F.3d 1216, 1221 (10th Cir. 2009) (Gorsuch, J.).

Because hiQ has no entitlement to relief under state law, the preliminary injunction should be vacated on that basis alone. But the district court's analysis was wrong in another respect that warrants vacatur. The district court held that once a company makes information generally available for viewing on its website, it loses any right to invoke the CFAA to protect itself against invasive data-scraping bots deployed by would-be competitors. The only recourse for LinkedIn, according to the district court, is to revamp its entire business by restricting access to the information through a password authentication system. This result, in turn, would undermine a primary way that LinkedIn provides value to consumers because it will limit the ability of search engines to find members' professional profiles (*i.e.*, online resumes). The district court's ruling has no basis in the text, structure, or history of the CFAA, and it would transform the Internet in untold ways that are inimical to disseminating information and robust economic growth.

By contrast, LinkedIn's position flows directly from the unambiguous text of the CFAA and this Court's decisions interpreting it. After hiQ engaged in prolonged misbehavior on LinkedIn's servers by unleashing bots that scraped hundreds of thousands of member profiles, LinkedIn revoked hiQ's access to those servers. It sent hiQ a particularized cease-and-desist letter and imposed targeted blocks on hiQ's corporate IP addresses. Any attempt by hiQ to access LinkedIn's servers after this clear revocation would be "without authorization" and would therefore violate the CFAA. *Power Ventures*, 844 F.3d at 1068. Accordingly, the district court's mandatory preliminary injunction should be vacated.

JURISDICTIONAL STATEMENT

The district court had subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1367. On August 14, 2017, the district court issued a preliminary injunction. LinkedIn filed a timely notice of appeal on September 5, 2017. This Court has jurisdiction under 28 U.S.C. § 1292(a)(1).

STATEMENT OF THE ISSUES

The district court issued a mandatory preliminary injunction barring LinkedIn from using technical and legal measures to protect its servers from data-scraping bots deployed by hiQ, a would-be competitor. The issues in this case are whether the court abused its discretion because it:

1) erred as a matter of law in concluding that hiQ had a potential UCL claim, where hiQ's claim is predicated on LinkedIn having an antitrust duty to assist hiQ by allowing hiQ's bots to scrape LinkedIn's servers and where hiQ failed to allege the basic elements of an antitrust claim;

2) erred as matter of law by holding—contrary to the CFAA's unambiguous text and Circuit precedent—that LinkedIn could not invoke the CFAA after LinkedIn revoked hiQ's access to its servers by sending a particularized cease-and-desist letter and imposing technical measures to block hiQ's data-scraping bots; and

3) erred when crediting hiQ's speculative and unsupported claims of irreparable harm while systematically undervaluing the demonstrated harms to LinkedIn and the public.

STATUTE

The CFAA, 18 U.S.C. § 1030, is reproduced in an addendum to this brief.

STATEMENT OF THE CASE

A. LinkedIn's Protections Against Data-Scraping "Bots"

LinkedIn is a professional networking service that allows its members to create, manage, and share their professional identities and interests online. 5ER-824. The heart of its business is the information that LinkedIn members entrust to LinkedIn—including member work and education history, profile narratives, and headshots—that LinkedIn stores on its computer servers. It has over 500 million

members in over 200 countries, and has created over 10,000 jobs around the world. 5ER-824. This tremendous growth did not happen by accident. Since its creation in its founder's living room in 2002, LinkedIn has invested billions of dollars in developing its services. 5ER-824.

To protect its business and its members, LinkedIn seeks to prevent data-scraping from its computers. 4ER-759. Scraping is the automated, mass-extraction of data directly from a website's servers. 4ER-759. A computer server connected to the Internet stores "electronic information and serves that electronic information directly to the user" by "physically sending ones and zeros over the Internet." *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1159 (9th Cir. 2007) (quotation marks omitted).

Scraping is frequently performed by "bots": computer programs that "query other computers over the Internet in order to obtain a significant amount of information." *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1060 n.2 (N.D. Cal. 2000). Bots can make thousands of server requests per second, "far in excess of what a human can accomplish." *Id.* at 1061. Bots are routinely deployed to copy data from LinkedIn's servers on a massive scale. 4ER-759-760. These bots have been programmed to make complete copies of LinkedIn's website, combine scraped member data with data found elsewhere (such as telephone

numbers or addresses), and otherwise infiltrate LinkedIn's physical servers. Once scraped from LinkedIn's servers, member data can be sold to the highest bidder.

LinkedIn relies on technical barriers and the assertion of legal rights to protect itself and its members from bot-scraping. On the technical side, LinkedIn uses a variety of automated countermeasures, including the:

- FUSE system, which scans and imposes a limit on the activity that a user may initiate on the website;
- Quicksand system, which monitors patterns of access to LinkedIn's servers to look for non-human activity indicative of scraping;
- Sentinel system, which scans, throttles, and at times blocks suspicious activity associated with specific Internet Protocol (or IP) addresses;
- Org Block system, which blocks a manually-created list of IP addresses and contains a program to identify IP addresses used by large-scale scrapers;
- Request Scoring systems, which monitor and restrict activity indicative of access by bots; and
- "robots.txt" file, which provides instructions to bots that attempt to access LinkedIn's servers and prohibits automated programs like those used by data scrapers. "The Internet industry has widely recognized the robots.txt file as a standard for controlling automated access to Web pages since 1994." *Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1113 (D. Nev. 2006).[1]

[1] LinkedIn's robots.txt file does permit—consistent with LinkedIn's Privacy Policy—certain identified crawlers (*e.g.*, search engines such as Google or Bing) to access its computers in order to index certain member profile information. 4ER-761. Permitting search engines to index member profiles benefits members because it makes them findable via the primary way that people locate information on the Internet (via search engines). These search engine results linking to LinkedIn also allow members to present the world with their best professional

4ER759-761. LinkedIn invests millions of dollars annually in this effort to stop bots, which blocks over 95 million bot access attempts per day. 4ER-759, 4ER-761.

Those who deploy bots that have been stymied by LinkedIn's technical barriers often redesign their bots to evade those barriers—including anonymous bots that mask their identities to access LinkedIn's servers. 3ER-433. LinkedIn's protections are therefore unable to fully shield its servers from this kind of bot-related gamesmanship. LinkedIn must also employ protective legal measures. One such measure is LinkedIn's User Agreement, which expressly prohibits using automated software—including "bots"—to access and scrape LinkedIn's computers. 4ER-761-762 & 4ER-775. The Agreement also informs members that LinkedIn "reserves the right to restrict, suspend, or terminate" the access of those found to have abused their access privileges. 4ER-763 & 4ER-772.

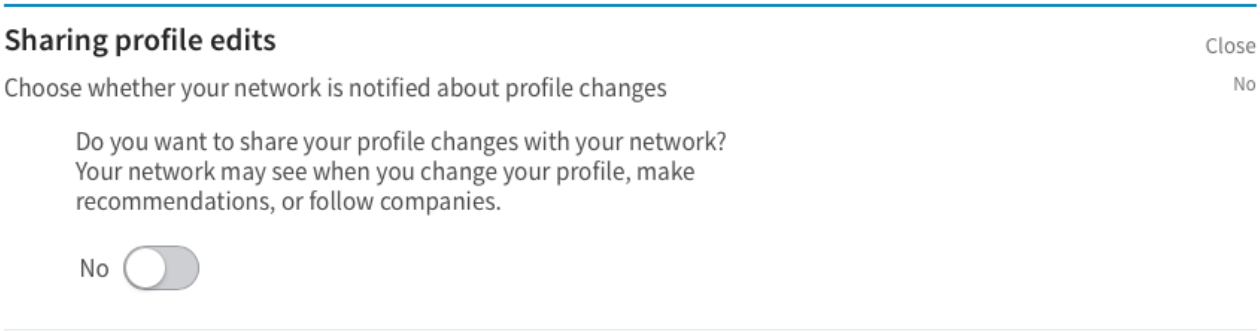
Those who sign up for LinkedIn's services assent to LinkedIn's User Agreement and Privacy Policy—as hiQ has admitted it did. 4ER-763; 5ER-867. But that is not the only time hiQ made this commitment. It did so *multiple times*, including when it bought advertising from LinkedIn in 2016; when it purchased a

---

self—a professional identity that *they* control. LinkedIn informs members that data on their "public" profiles may be indexed by search engines, but permits them to limit the parts of their profiles that search engines index, or to opt out of this feature. 4ER-762-763 & 4ER-775.

license for LinkedIn's Sales Navigator in 2015; and when it created a company webpage on LinkedIn in 2014. 4ER-764-765.

LinkedIn provides its members with various privacy controls and settings. For example, when a member updates the information in her profile, LinkedIn lets that member choose whether to broadcast that change to others. 3ER-427. If a member decides that she does not want to broadcast changes to her profile, that member can make that choice. 3ER-427. LinkedIn provides members the option of electing "Do Not Broadcast" in real-time anytime the member changes her profile. 3ER-428. This feature was specifically developed in response to concerns over employers monitoring changes to their employees' profiles. 3ER-427. LinkedIn members can also go into their privacy settings and select this feature at any time, as demonstrated by this screenshot:



3ER-427. Over 50 million LinkedIn members have elected to employ the "Do Not Broadcast" feature. 3ER-430.

B. hiQ's Data-Scraping Bots Access LinkedIn's Servers Without Authorization

hiQ's business model free rides on LinkedIn's investment and entrepreneurship. hiQ uses bots to continuously scrape hundreds of thousands of member profiles from LinkedIn's servers without the consent of LinkedIn or its members, and then repackages that data to sell to its clients. 4ER-766. hiQ has admitted that "the vast, vast preponderance of the public material" that hiQ uses is scraped from LinkedIn's computer servers using bots. 2ER-74:24-25. hiQ's bots use anonymous IP addresses, meaning they do not identify themselves to LinkedIn's computers as having been tasked by hiQ to scrape data. 4ER-766; *United States v. Forrester*, 512 F.3d 500, 510 n.5 (9th Cir. 2007) ("Every computer … connected to the Internet has a unique IP address."). Nor is hiQ granted permission to access LinkedIn's servers by LinkedIn's "robots.txt" file. 4ER-761. Indeed, the district court found that hiQ circumvents "LinkedIn's measures to prevent use of bots and implementation of IP address blocks." 1ER-16.

After illicitly scraping data from LinkedIn's servers, hiQ incorporates LinkedIn's data into the two products that it sells to its customers: (1) "'Keeper,' which tells employers which of their employees are at the greatest risk of being recruited away, and [2] 'Skill Mapper,' [which offers] a summary of the breadth and depth of aggregate or individual skills possessed." 5ER-859. hiQ introduced no evidence that these services actually benefit employees, and it is easy to

understand how "Keeper" might not: if an employer thinks an employee is about to leave, the employer could terminate her or refuse to give her access to sensitive information, even if she actually has no intention of departing.

LinkedIn's members have complained when they discovered that their profile data has been scraped and made available on other websites. 3ER-431-432. For example, one member complained about finding information he had deleted from his profile available on a third-party website, stating that "these kind of things create a lack of confidence in using [L]inkedIn." 3ER-431.[2] But hiQ's products specifically defeat the privacy protection LinkedIn offers—indeed, a goal of hiQ's "Keeper" product is to tell employers when LinkedIn members change their profiles, even if members have chosen not to broadcast such changes to their connections (including their employers). Consequently, LinkedIn members face the difficult choice of hiding their online professional profile behind a password wall (making it un-indexable by search engines and essentially undiscoverable), or leaving that profile vulnerable to hiQ's surveillance.

[2] The district court stated that LinkedIn only identified "three individual complaints specifically raising concerns about data privacy related to third-party data collection," (1ER-6 (emphasis omitted)), when in fact, the record explained that "LinkedIn has received dozens of such complaints" over the past two years (3ER-431).

C. The Proceedings Below

LinkedIn sent hiQ a cease-and-desist letter on May 23, 2017, demanding that hiQ stop accessing LinkedIn's servers to scrape data. 4ER-742. The letter explained that hiQ's use of bots in violation of the User Agreement and in circumvention of LinkedIn's technological countermeasures was "without authorization" under the CFAA. 4ER-743. LinkedIn informed hiQ that "'[a]ny future access of any kind' would be 'without permission and without authorization from LinkedIn,'" and that LinkedIn had implemented additional "'technical measures to prevent hiQ from accessing, and assisting other to access, LinkedIn's site, through systems that detect[], monitor, and block scraping activity.'" 1ER-3 (quoting 4ER-743). Accordingly, LinkedIn demanded that hiQ "[c]ease and desist accessing or attempting to access" its "computers … and data stored therein." 4ER-743; 4ER-737; 4ER-766.

Having been denied continued access to LinkedIn's servers, hiQ brought suit. 4ER-739; 4ER-746; 5ER-992. hiQ's complaint alleged four affirmative claims for relief based on California tort and constitutional law, and a declaratory judgment that LinkedIn could not lawfully invoke the CFAA against it. 5ER-992. hiQ also brought a motion for a temporary restraining order, which was converted into a motion for a preliminary injunction. The district court granted that motion on August 14, 2017. 1ER-1.

Addressing the equitable factors first, the district court held that they weighed in hiQ's favor after crediting hiQ's conclusory assertion that it would go out of business if it could no longer scrape and exploit LinkedIn's data. 1ER-4-8. The district court then embarked on a lengthy analysis of whether LinkedIn lawfully invoked the CFAA in its cease-and-desist letter. 1ER-8-17. The court acknowledged that precedents of this Circuit interpreting the CFAA's plain text appeared to support LinkedIn's invocation of the CFAA. 1ER-8-11. But the court declined to follow those precedents, distinguishing them on the ground that they involved unauthorized access to password-protected information—even though that fact played no role in this Court's analysis. 1ER-9-10; page 55 *infra*. Relying instead on a law review article, the court held that LinkedIn cannot invoke the CFAA to protect itself against hiQ's bots because its website made member information on its servers available for viewing without requiring a password. 1ER-13-17.

Only after that lengthy analysis did the district court address what should have been the dispositive threshold issue: whether hiQ established a likelihood of success on any cause of action. 1ER-18-23. In a perfunctory analysis, the court held that hiQ raised a serious issue as to its claim under California's UCL that LinkedIn violated the "spirit" of the antitrust laws when it sent its cease-and-desist letter. 1ER-21-23. Based on this reasoning, the court ordered LinkedIn to

withdraw its letter and enjoined LinkedIn from blocking hiQ's data-scraping bots. 1ER-25.

SUMMARY OF ARGUMENT

The district court abused its discretion by issuing its mandatory preliminary injunction.

I. hiQ cannot show any chance of success on the merits for two independent reasons.

A. hiQ lacks a valid cause of action under the UCL because LinkedIn had no antitrust duty to assist hiQ by allowing hiQ's bots to expropriate data from LinkedIn's servers. *MetroNet Servs. Corp. v. Qwest Corp.*, 383 F.3d 1124, 1131 (9th Cir. 2004) (citing *Trinko*, 540 U.S. at 411). Ninth Circuit precedent forecloses the application here of the antitrust theories—"monopoly leveraging" and "essential facilities"—that the district court invoked to justify imposing a duty to deal on LinkedIn. *Alaska Airlines, Inc. v. United Airlines, Inc.*, 948 F.2d 536, 547 (9th Cir. 1991). hiQ also failed to allege the basic prerequisites of an antitrust claim, including the existence of a defined market and the defendant's monopoly power in that market. Finally, this case does not fall into the narrow "spirit"-of-the-law category recognized under the UCL—the entire basis for the district court's decision—because LinkedIn's refusal to assist hiQ does not violate the antitrust laws or harm competition.

B. The CFAA bars hiQ's attempt to reinvade LinkedIn's servers after LinkedIn clearly withdrew authorization for hiQ's data-scraping bots to access them. Under the unambiguous text of the CFAA and this Court's definitive interpretations of it, "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly." *Power Ventures*, 844 F.3d at 1067. That is exactly what happened here. hiQ's data-scraping bots circumvented a pre-existing array of technological barriers in violation of LinkedIn's User Agreement. After LinkedIn responded by sending hiQ a clear cease-and-desist letter and imposing additional technical measures (targeted IP blocks), hiQ sought to regain access to LinkedIn's servers so that it could engage in the same forbidden free-riding misbehavior that caused it to have its access revoked in the first place. That re-deployment of bots would be "without authorization" under the CFAA. Accordingly, not only does hiQ lack a valid declaratory judgment claim, but its alleged state law causes of action are preempted and barred.

The district court's sweeping holding that the only permissible way to revoke access to a publicly-available website is to impose a password authentication requirement contradicts the text, structure, and history of the CFAA, as well as this Court's precedent. And adopting this unprecedented rule would make the Internet less open because companies would be forced to erect password

walls to protect their information, and it would discourage innovators from developing new platforms because would-be competitors could simply free-ride on that entrepreneurship by unleashing data-scraping bots.

II. hiQ cannot demonstrate irreparable harm because it has no cognizable right to engage in behavior that violates the CFAA and it has offered insufficient evidence demonstrating that it will go out of business if it cannot illegally access LinkedIn's servers.

III. The balance of the equities and public interest factors weigh heavily in LinkedIn's favor. hiQ's behavior jeopardizes the privacy of LinkedIn's members and LinkedIn's ability to safeguard its business from data-scraping bots. The public has a strong interest in preserving the openness of the Internet and the vibrancy of the Internet economy, both of which are endangered by the district court's sanctioning of hiQ's behavior.

STANDARD OF REVIEW

This Court reviews a decision granting a preliminary injunction for abuse of discretion. *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011). A "district court abuses its discretion if the court rests its decision on an erroneous legal standard" or "on a clearly erroneous finding of fact," which results "from a factual finding that was illogical, implausible, or without support in inferences that may be drawn from the facts in the record." *Pom Wonderful LLC v.*

Hubbard, 775 F.3d 1118, 1123 (9th Cir. 2014) (internal quotation marks omitted). A court's "legal conclusions" are reviewed *de novo*. *Id*.

In considering whether a district court abused its discretion, this Court applies the familiar preliminary injunction standard: "A plaintiff … must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). This Court has adopted a "sliding scale" approach, "so that a stronger showing of one element may offset a weaker showing of another." 632 F.3d at 1131. But where a "party has not shown any chance of success on the merits, no further determination of irreparable harm or balancing of hardships is necessary." *Global Horizons, Inc. v. U.S. Dep't of Labor*, 510 F.3d 1054, 1058 (9th Cir. 2007).

hiQ faces an especially high hurdle because the preliminary injunction did not merely preserve the status quo, but affirmatively required LinkedIn to disable the technical measures it had been using to block hiQ's bots and to withdraw its cease-and-desist letter. Mandatory injunctions are "particularly disfavored," and "court[s] should deny such relief unless the facts and law clearly favor the moving party." *Stanley v. Univ. of S. Cal.*, 13 F.3d 1313, 1320 (9th Cir. 1994) (internal

citations and quotation marks omitted). hiQ cannot remotely satisfy that exacting standard.

ARGUMENT

I. HIQ HAS NO PROSPECT OF SUCCESS ON THE MERITS

A. hiQ Has No Entitlement to Relief Under California's Unfair Competition Law

The district court imposed a mandatory preliminary injunction because it believed that hiQ had a potentially meritorious antitrust claim under California's UCL. But the court's perfunctory antitrust analysis does not come close to establishing that hiQ raised a serious question on the merits—much less the clear legal entitlement to relief that is needed to justify a mandatory injunction forbidding LinkedIn from protecting its business.

In fact, the district court's decision—not LinkedIn's conduct—will harm competition. LinkedIn blocked hiQ's data-scraping bots to protect the value and quality of LinkedIn's services for its members. *United States v. Syufy Enterprises*, 903 F.2d 659, 669 (9th Cir. 1990) ("We make it clear today, if it was not before, that an efficient, vigorous, aggressive competitor is not the villain antitrust laws are aimed at eliminating. Fostering an environment where businesses fight it out using the weapon of efficiency and consumer goodwill is what the antitrust laws are meant to champion."). If allowed to continue, hiQ's activities could have degraded LinkedIn's user experience and eroded the trust LinkedIn has worked hard to

develop with its members. Such consequences would materially harm LinkedIn's ability to compete with other professional networks and social media services. It was perfectly reasonable for LinkedIn to defend its business, which represents the fruits of a multi-billion-dollar investment that came at considerable risk. *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-05780 JW, 2010 WL 3291750, at *14 (N.D. Cal. July 20, 2010) (if a company "has the right to manage access to and use of its website, then there can be nothing anticompetitive about taking legal action to enforce that right"). If the district court's decision is upheld, it will discourage entrepreneurs from making the same kinds of investments, because they will know that other companies will invoke the antitrust laws to free-ride rather than compete on the merits, undermining the letter *and* spirit of the antitrust laws.

a. LinkedIn's conduct does not violate the antitrust laws

To prove a UCL violation, hiQ must establish that LinkedIn's conduct "threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition." *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 187 (1999). Under this standard, theories that are untenable under the antitrust laws do not magically become actionable by focusing on the amorphous "spirit" of those laws. *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1136-37 (9th Cir. 2014) (plaintiff's general

UCL allegations did not suffice to allege what "amounts to a violation of antitrust laws" or conduct that "otherwise significantly threatens or harms competition.").

Where, as here, the plaintiff claims that a potential rival violates the UCL by unlawfully exploiting its monopoly power through unilateral action, the plaintiff must prove that the defendant is engaging in conduct that harms *competition* in a defined product and geographic market in which the defendant possesses market power. *Spectrum Sports Inc. v. McQuillan*, 506 U.S. 447, 458 (1993); *Cel-Tech*, 20 Cal. 4th at 180 (UCL incorporates federal antitrust standards). Where, as here, a company does not have the power to control prices or exclude competition, and the only alleged harm is to a particular *competitor*, there is no antitrust violation. *Syufy Enterprises*, 903 F.2d at 664-72.

hiQ did not even attempt to meet these exacting standards. Instead it served up an unsupported claim that LinkedIn violated the "spirit" of the antitrust laws by refusing to give hiQ access to LinkedIn's servers in the manner that hiQ preferred (via bot scraping) so that hiQ could free-ride on the database that LinkedIn worked so hard to create. In particular, hiQ made no effort to show that LinkedIn's refusal to give access to hiQ's bots would foreclose competition, and thereby harm consumers, in the "data analytics" market or any other. hiQ only complains about injury to itself.

That is insufficient as a matter of law. Under the UCL, as under the federal antitrust laws, "[i]njury to a competitor is not equivalent to injury to competition; only the latter is the proper focus of antitrust laws." *Cel-Tech*, 20 Cal. 4th at 186. Courts routinely rely on this bedrock antitrust principle to dismiss UCL claims. *Oracle Am., Inc. v. Hewlett Packard Enter. Co.*, No. 16-cv-01393-JST, 2016 WL 3951653, at *8 (N.D. Cal. July 22, 2016); *Total Recall Techs. v. Luckey*, No. C 15-02281 WHA, 2016 WL 1070656, at *5 (N.D. Cal. Mar. 18, 2016). This Court should do the same.

Most fundamentally, the antitrust laws do not impose any duty on LinkedIn to allow hiQ access to LinkedIn's servers or to cooperate with hiQ in any other way. "As a general rule, businesses are free to choose the parties with whom they will deal, as well as the prices, terms and conditions of the dealing." *Pacific Bell Tel. Co. v. Linkline Commc'ns, Inc.*, 555 U.S. 438, 448 (2009). Even companies with monopoly power may generally choose to deal, or not deal, with potential competitors on the terms they find competitively advantageous.

Trinko is on point. There, the plaintiff alleged that Verizon used its power in the wholesale market for network elements (*i.e.*, inputs necessary to provide local telephone service) to disadvantage a would-be competitor in the downstream market for retail customers by denying the competitor fair and timely access to network elements that were necessary to compete in the retail market. 540 U.S. at

404. The Supreme Court unanimously rejected that claim, holding that "as a general matter 'there is no duty to aid competitors.'" *MetroNet*, 383 F.3d at 1131 (quoting *Trinko*, 540 U.S. at 411). As the Court explained, forcing a successful company to allow a rival to expropriate the fruits of its innovation and investment can damage rather than promote competition, "since it may lessen the incentive for the monopolist, the rival, or both to invest in those economically beneficial facilities." *Trinko*, 540 U.S. at 407-08. The antitrust laws exist to promote competition, not free-riding.

hiQ's claim here closely tracks the claim rejected in *Trinko*. hiQ argues that LinkedIn refused to provide its data to hiQ in the form hiQ prefers so that it could compete more effectively in the "data analytics" market. LinkedIn has no duty, however, to allow hiQ to access LinkedIn's data at all, much less in whatever form hiQ desires. *Linkline*, 555 U.S. at 450-51 ("a firm with no duty to deal in the wholesale market has no obligation to deal under terms and conditions favorable to its competitors"); *Four Corners*, 582 F.3d at 1223 (hospital not required to grant staff privileges to a particular doctor because it "is entitled to recoup its investment without sharing its facilities with a competitor").

The California Court of Appeal rejected a similar UCL claim when considering Verizon's practice of releasing new cellular phones to its own stores before allowing independent dealers to sell them. *People's Choice Wireless, Inc.*

v. Verizon Wireless, 131 Cal. App. 4th 656, 660-61 (2005). Explaining that the "mere refusal to deal does not violate the spirit or policy of antitrust law," it held that a company is not required to "'share the source of [its] advantage." *Id.* at 667 (quoting *Trinko*, 540 U.S. at 407). hiQ's claims fail for the same reasons.

The one "limited exception" to the no-duty-to-deal doctrine provides no legal cover for hiQ's attempts to free-ride on LinkedIn's business. In rare situations, a monopolist may violate the antitrust laws if it terminates a previously profitable cooperative venture with a rival (while continuing to provide that same service to others) in order to achieve anticompetitive ends. *Trinko*, 540 U.S. at 408; *see Novell v. Microsoft Corporation*, 731 F.3d 1064, 1072 (10th Cir. 2013) (Gorsuch, J.) ("Put simply, the monopolist's [refusal to deal] must be irrational but for its anticompetitive effect"). Nothing like that occurred here. The mere allegation that LinkedIn initially may not have objected to hiQ's scraping activity, or entered into agreements with hiQ involving non-scraping activities, is not the sort of voluntary cooperative venture discussed in *Trinko*, let alone a profitable one. 540 U.S. at 408. Nor does hiQ allege that LinkedIn sells the ability to scrape its servers to others. *Id.* Thus, hiQ cannot fit itself within this limited exception, which is "at or near the outer boundary" of actionable conduct. *Id.*

Ignoring this settled law, the district court invoked the outmoded theory of "monopoly leveraging" to justify its preliminary injunction. 1ER-21-23. But this

Court has rejected "monopoly leveraging" claims of the kind that hiQ advances—the argument that a company with market power in one market violates the antitrust laws by attempting to use that power to gain an advantage in an adjacent market. *Alaska Airlines*, 948 F.2d at 547. It has held that the "anticompetitive dangers that implicate the Sherman Act are not present when a monopolist has a lawful monopoly in one market and uses its power to gain a competitive advantage in the second market." *Id.* at 548. To the contrary, "[m]onopoly leveraging is just one of a number of ways that a monopolist can permissibly benefit from its position." *Id.*

In the face of this authority, the district court inexplicably did exactly what Circuit precedent forecloses: it held that there were serious questions as to whether LinkedIn engaged in unlawful "monopoly leveraging" on the theory that it might have been seeking to gain a future competitive advantage over hiQ. Making matters worse, it did so without finding that LinkedIn had any probability of monopolizing the market for "data analytics"—a market that neither hiQ nor the district court tried to define (*see infra*). That ruling was plainly an abuse of discretion.

Nor can the district court's ruling be justified under the other moribund theory it mentioned: "essential facilities," *i.e.*, "when one firm, which controls an essential facility, denies a second firm reasonable access to a product or service

that the second firm must obtain in order to compete with the first." *Alaska Airlines*, 948 F.2d at 542. The Supreme Court has "never recognized such a doctrine," *Trinko*, 540 U.S. at 411, and leading authorities on antitrust law have opined that "[o]ne is hard-pressed to see any separate vitality remaining in the essential facility doctrine," Phillip E. Areeda & Herbert Hovenkamp, Antitrust Law: An Analysis of Antitrust Principles and Their Application § 772d3 (4th ed.).

Although this Court has kept "essential facilities" alive as a theoretical possibility, it has never imposed liability on that basis. In addition, it has described *Otter Tail Power Co. v. United States*, 410 U.S. 366, 377 (1973), which the district court exclusively relied upon, as an "extreme case" where a monopolist had "eliminated all possibility of competition in the downstream market." *Alaska Airlines*, 948 F.2d at 543; *see Aerotec Int'l, Inc. v. Honeywell Int'l, Inc.*, 836 F.3d 1171, 1185 (9th Cir. 2016).

Here, hiQ has not attempted to show that LinkedIn's alleged monopoly over the professional network market eliminates *all possibility* of competition in the undefined "data analytics market." hiQ nowhere explains how any control LinkedIn has over its own servers can eliminate all competition in that market—which has been described as a $130 billion dollar market that is expected to grow to more than $203 billion in 2020 (4ER-708-709)—or even that access to LinkedIn's data is essential to competition, given how many others are competing

without deploying bots to scrape LinkedIn's servers. hiQ did not—and could not—show that LinkedIn's actions eliminated *all competition* in this purported market. *Paladin Assocs., Inc. v. Mont. Power Co.*, 328 F.3d 1145, 1163 (9th Cir. 2003).

In sum, there is no basis for concluding that LinkedIn had an antitrust duty to provide unfettered access to its servers, and to turn over its member database to hiQ, or that LinkedIn's servers and the data they contain constitute an essential facility under that exceedingly narrow antitrust theory (if it has viability at all after *Trinko*). The district court abused its discretion concluding otherwise.

b. hiQ did not even try to establish the basic prerequisites of an antitrust claim

The district court's ruling is fatally flawed for another reason. The court imposed a preliminary injunction despite the complete absence of proof establishing the requisites for a claim of unlawful monopolization: definition of the relevant product and geographic markets in which the defendant possesses market power.

The first step in any monopolization case is defining a relevant market. An antitrust plaintiff must show (typically through expert testimony) that no other products are reasonable substitutes for those alleged to be in the relevant market (in other words, that if the monopolist increased the price of the product, customers would not switch to another product in response to the price increase) within a

defined geographic area. *Morgan, Strand, Wheeler & Biggs v. Radiology, Ltd.*, 924 F.2d 1484, 1491 (9th Cir. 1991). The need for proof of market definition is particularly strong here because hiQ's antitrust claim depends on allegations about *two* separate markets—that LinkedIn is a monopolist in the "professional networking market" and is using that market power to try to monopolize the "data analytics" market. Absent such proof, it is impossible to evaluate possible harm to the competitive process. *Tanaka v. Univ. of S. Cal.*, 252 F.3d 1059, 1063-64 (9th Cir. 2001). Because hiQ did not even try to establish the contours of the "professional networking market," the district court had no basis for concluding (even provisionally) that LinkedIn had monopoly power in that market. Likewise, because hiQ did not even try to establish the contours of the "data analytics" market, the district court had no basis for concluding that LinkedIn's actions posed any risk of monopolizing that market. Those deficiencies foreclose relief.

An antitrust plaintiff also must show that the defendant has market power, which is "the power to control prices or exclude competition" in a defined market. *Image Tech. Servs. Inc. v. Eastman Kodak Co.*, 125 F.3d 1195, 1202 (9th Cir. 1997). The record contains no evidence that LinkedIn possesses market power in the "professional network" market. Indeed, the record refutes that premise. Other platforms have significant amounts of professional data on them, including those geared toward specific industries and those with a broader focus that also contain

professional information. 5ER-825; 4ER-621-622. For example, Facebook, which has *1.8 billion more* monthly users than LinkedIn, provides users the opportunity to populate professional information into their profiles. 5ER-825. Recent survey evidence indicates that comparable numbers of people use Facebook and LinkedIn for professional purposes. 4ER-621 & 4ER-687. Facebook also has a self-service advertising tool that permits advertisers to target Facebook users using criteria such as employer name, industry, job title, education level, field of study, or school attended, and a comparison of Facebook's tool to a similar tool on LinkedIn shows comparable levels of professional data between the platforms across several identified employers. 4ER-621-622. The district court's conclusory assertion regarding LinkedIn's dominance thus lacks any foundation.

hiQ likewise offered no proof that LinkedIn possesses market power in, or poses any risk of dominating, the "data analytics" market. Whatever LinkedIn's position in the "professional network" market, it plainly has no ability to control prices or exclude competition in the vast and growing "data analytics" market. Even with respect to analyzing professional information (which hiQ did not show was a separate submarket), hiQ's competitors (such as Glint) obtain data inputs other than by scraping LinkedIn. 4ER-621 & 4ER-650. And websites like Facebook contain significant amounts of professional data, making it impossible for LinkedIn to control who may compete or what prices they may charge. That

the district court interposed a mandatory preliminary injunction despite hiQ's total failure of proof vividly underscores that it abused its discretion.

c. The District Court erred by resorting to the "spirit" of the antitrust laws and LinkedIn's "purpose"

Papering over the absence of any basis for finding a probable antitrust violation, the district court invoked the "spirit" of the antitrust laws to justify its mandatory injunction. This Court has previously rejected UCL claims where plaintiffs have alleged that defendants' conduct violates the "spirit" of antitrust laws, but fail to allege a cognizable antitrust violation, and it should do the same here. *Levitt*, 765 F.3d at 1136-37. But even considering just the "spirit" of the antitrust laws, the district court misunderstood what that concept means under California law. Conduct "(1) violates the policy or spirit of the antitrust laws because the effect of the conduct is comparable to or the same as a violation of the antitrust laws, or (2) it otherwise significantly threatens or harms competition." *People's Choice Wireless*, 131 Cal. App. 4th at 662 (citing *Cel–Tech*, 20 Cal. 4th at 187). hiQ established neither.

First, hiQ cannot establish that LinkedIn's conduct is "comparable" or the "same" as a violation of the antitrust laws. Courts have rejected UCL claims where conduct falls short of an antitrust violation recognized in law, absent "unusual circumstance[s]." And in *Cel-Tech*—the only "spirit" case the district court cited—the California Supreme Court recognized a potential UCL claim only

because the defendant was "one of two holders of a lucrative government-licensed duoply." 20 Cal. 4th at 190. The court found it "critical" that the defendant had a "legally privileged status" due to a government-issued license. *Id.* at 188-190. No privileged status, or anything like it, exists here, so *Cel-Tech* cannot support the court's ruling. *Creative Mobile Techs., LLC v. Flywheel Software, Inc.*, No. 16-cv-02560-SI, 2017 WL 679496, at *6 (N.D. Cal. Feb. 21, 2017) (dismissing UCL claim where counterclaimant "ha[d] not pointed to any 'unusual' aspect of the alleged conduct); *Synopsis, Inc. v. ATopTech, Inc.*, No. C 13-2965 MMC, 2015 WL 4719048, at *10 (N.D. Cal. Aug. 7, 2015) (same).

Second, hiQ never attempted to establish that LinkedIn's conduct "otherwise significantly threatens or harms competition." As demonstrated, hiQ introduced no evidence that there would be any harm to *competition*; at best, it only alleged harm *to itself*. That is insufficient.

Left with neither the letter nor the "spirit" of the law, the district court ultimately fell back on LinkedIn's purported anticompetitive "purpose" to justify its injunction. 1ER-22-23. But "the Sherman Act regulates anti-competitive conduct, not merely anticompetitive aspirations or an independent decision on terms of dealing with a competitor." *Aerotec*, 836 F.3d at 1184.

The district court's emphasis on anticompetitive purpose underscores its failure to appreciate that the antitrust laws do not require LinkedIn to assist hiQ in

free-riding on LinkedIn's business. Companies are "under no duty to help" their competitors "survive or expand." *California Computer Prods., Inc. v. Int'l Bus. Machs. Corp.*, 613 F.2d 727, 744 (9th Cir. 1979). While "[m]ost businessmen don't like their competitors, or for that matter competition," what is relevant under the antitrust laws is whether they "use methods calculated to make consumers worse off in the long run," and "[c]onsumers would be worse off if a firm with monopoly power had a duty to extend positive assistance to new entrants." *Olympia Equip. Leasing Co. v. W. Union Tel. Co.*, 797 F.2d 370, 379 (7th Cir. 1986) (Posner, J.). Because hiQ's UCL claim is a gussied-up request for a helping hand from LinkedIn, it is "simply too far removed from cognizable antitrust evils to warrant intervention" under California law. *People's Choice Wireless*, 131 Cal. App. 4th at 668.

B. The District Court's Tortious Interference Footnote is Meritless

The district court similarly erred regarding hiQ's tortious interference claim, stating in a footnote that it "overlaps with the analysis of the unfair competition claim." 1ER-23 n.14. Because the court incorrectly analyzed hiQ's UCL claim, this conclusion is erroneous. Separately, hiQ's tortious interference claims are meritless because: (1) LinkedIn acted with "legitimate business purpose[s]," *Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal. 4th 26, 57 (1998), *i.e.*, protecting its members' data and the investment made in developing its platform;

enforcing its User Agreement's prohibitions on automated scraping; and asserting its rights under federal and state law; and (2) hiQ's contracts with its clients are premised on unlawful access to LinkedIn's data and are thus "tainted with illegality," *Marathon Entm't, Inc. v. Blasi*, 42 Cal. 4th 974, 996 (2008); *In re R2D2, LLC*, No. CV 13-3799 PSG, 2014 WL 12589668, at *8 (C.D. Cal. Jan 9, 2014).

C. The District Court Erred as a Matter of Law in Holding That hiQ Would Not Violate The CFAA by Re-Accessing LinkedIn's Servers

hiQ's failure to establish a valid UCL cause of action requires vacatur of the preliminary injunction. But even if hiQ had a UCL cause of action, vacatur would still be required because hiQ's continued use of bots to scrape data from LinkedIn's servers would violate the CFAA. As explained below, LinkedIn would be entitled to an injunction under the CFAA *preventing hiQ* from accessing its computers "without authorization." *Facebook, Inc. v. Power Ventures, Inc.*, No. 08-CV-05780-LHK, 2017 WL 1650608, at *16 (N.D. Cal. May 2, 2017) (the "public interest weighs in favor of an injunction" to "ensur[e] that computers are not accessed without authorization"). But the district court granted hiQ the opposite—an injunction under state law *forcing LinkedIn* to grant hiQ unconstrained access to its computers. Accordingly, hiQ's request for an injunction is preempted because, if granted, the injunction would "stand as an

obstacle to the accomplishment … of the full purposes and objectives of [federal]" law. *Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 372-73 (2000) (internal quotation marks omitted); *Flamingo Indus. (USA) Ltd. v. USPS*, 302 F.3d 985, 996-97 (9th Cir. 2002), *reversed on other grounds by* 540 U.S. 736 (2004) ("using the [UCL] to challenge procurement decisions made by the Postal Service involving the Postal Service's requirements for mail bags … conflicts with federal law"). Similarly, it is well-established that "an action under the antitrust laws will not lie where the business conducted by the plaintiff, and alleged to have been restrained by the defendant, was itself unlawful." *Modesto Irrigation Dist. v. Pac. Gas & Elec. Co.*, 309 F. Supp. 2d 1156, 1169-70 (N.D. Cal. 2004); *Snake River Valley Elec. Ass'n v. PacifiCorp*, 357 F.3d 1042, 1050 n.8 (9th Cir. 2004). Thus, not only does hiQ lack a valid declaratory judgment claim under the CFAA, but its UCL claim and request for injunctive relief are also barred.

At the outset, it is important to be clear about the declaratory judgment that hiQ seeks with its CFAA claim. The question before this Court is whether LinkedIn can invoke the CFAA *prospectively* to bar hiQ's use of data-scraping bots that circumvent technological barriers *after* LinkedIn withdrew hiQ's authorization to access its servers. Here, LinkedIn unmistakably rescinded hiQ's permission to access its computers because hiQ's bots violated the terms on which LinkedIn provides access to its servers and caused serious harm to LinkedIn's

business and members' privacy. Once LinkedIn sent hiQ a "particularized" cease-and-desist letter and implemented additional technical measures, *United States v. Nosal*, 844 F.3d 1024, 1034 (9th Cir. 2016) (*Nosal II*), hiQ's re-deployment of bots to scrape data from LinkedIn's computers would violate the plain terms (and this Court's definitive interpretation) of the CFAA.

In the district court's and hiQ's view, however, LinkedIn granted *irrevocable* authorization to hiQ's data-scraping bots as a result of "the general permission it granted to the public to access the information on its website." *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013). They insist that the only way to withdraw such permission is by placing a publicly-accessible website behind a password wall. But that is plainly wrong. LinkedIn "own[s] and control[s] access to its computers." *Nosal II*, 844 F.3d at 1035. It is therefore permitted under the CFAA to revoke hiQ's permission "on a case-by-case basis," *3Taps*, 964 F. Supp. 2d at 1182—and especially after hiQ engaged in gross misbehavior on LinkedIn's servers by unleashing bots (anonymized to hide hiQ's true identity) that circumvented LinkedIn's technical barriers and scraped massive amounts of information. The district court's newly-invented password revocation requirement finds no support in the text, structure, and history of the CFAA. Nor does it find support in this Court's precedents, which establish that once LinkedIn revoked hiQ's access via a cease-and-desist letter and

implementation of technical measures, hiQ's continued efforts to access LinkedIn's computers with data-scraping bots would plainly be "without authorization" within the meaning of the CFAA.

1. hiQ was "without authorization" to access LinkedIn's servers after LinkedIn revoked hiQ's permission and interposed technical measures to block its data-scraping bots

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 statute defines a "protected computer" as any computer that "is used in or affecting interstate or foreign commerce or communication," which undisputedly includes LinkedIn's servers. *Id.* § 1030(e)(2)(B). This Court has held that "'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission." *Nosal II*, 844 F.3d at 1028. As this Court has further observed, the "CFAA prohibits acts of computer trespass by those who are not authorized users." *Power Ventures*, 844 F.3d at 1065. Consistent with basic principles of trespass law, "[i]mplicit in the definition of authorization is the notion that someone, including an entity, can grant or revoke that permission" to access a protected computer. *Nosal II*, 844 F.3d at 1035.[3]

[3] *See Oliver v. United States*, 466 U.S. 170, 183 n.15 (1984) ("The law of trespass recognizes the interest in possession and control of one's property and for that reason permits exclusion of unwanted intruders.… [U]nlicensed use of property by

Automated bots, like those used by hiQ, directly access and extract "data on [a computer owner's] physical servers." *Power Ventures*, 844 F.3d at 1068. For this reason, "authorization" from the server's *owner* is "needed" to avoid CFAA liability. *Id*.

Here, LinkedIn unambiguously revoked hiQ's access to its servers after hiQ used data-scraping bots to circumvent LinkedIn's technological measures and access its servers in ways that caused harm to LinkedIn's business and its members' privacy. Those actions included: (1) supplementing its pre-existing technological countermeasures with targeted IP blocks to specifically prevent hiQ's corporate computers from deploying data-scraping bots to access LinkedIn's servers; and (2) sending a cease-and-desist letter revoking "[a]ny future access of any kind by hiQ." 4ER-766; 4ER-743; 4ER-737. These actions made it crystal clear to hiQ that any generalized permission that may have once been granted by virtue of making LinkedIn's website available for human viewing was "categorically revoked." *Nosal II*, 844 F.3d at 1038. As such, hiQ's continued

---

others is presumptively unjustified, as anyone who wishes to use the property is free to bargain for the right to do so with the property owner."); Restatement (Second) of Torts § 168 cmt. d (trespass occurs when a party performs an "unauthorized act" despite having been granted access to property, and particularly when that "forbidden act is likely to cause serious harm to the possessor of the [property]").

deployment of bots is "without authorization" under the unambiguous text of the CFAA and this Court's precedents. *Id*. at 1035, 1038.

This Court's caselaw compels the conclusion that hiQ's attempt to access LinkedIn's servers following clear revocation would violate the CFAA. Together, these decisions establish the "general rule[] in analyzing authorization under the CFAA" that "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly." *Power Ventures*, 844 F.3d at 1067. In *LVRC Holdings v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009), for example, this Court held that "a person uses a computer 'without authorization' under [§] 1030(a)(2) … when … the employer has rescinded permission to access the computer and the defendant uses the computer anyway." Similarly, *Nosal II* held that when a company "owned and controlled access to its computers … it retained *exclusive discretion* to issue or revoke access to [information on them]." 844 F.3d at 1035-36 (emphasis added). Once that company "unequivocally conveyed" to the defendant that he had "no authorization to access [the company's] computer system," any further attempts at access were "without authorization." *Id*. at 1036. *Nosal II* emphasized that where the defendant "received particularized notice of his revoked access" there were "no … difficulties" in finding a CFAA violation. *Id*.

Power Ventures is directly on point. In that case, Power Ventures used "automated scripts to collect information" from Facebook's servers and then use the information for competitive purposes, much like hiQ's strategy here. 844 F.3d at 1067-68 & n.4. Facebook "sent a 'cease and desist' letter to Power [Ventures] instructing [it] to terminate" its scraping activities and from "otherwise interacting with Facebook through automated scripts." *Id.* at 1063, 1067. Indeed, "Facebook explicitly revoked authorization for *any* access." *Id*. at 1068. To enforce that complete revocation, Facebook "instituted an Internet Protocol ('IP') block in an effort to prevent Power from accessing the Facebook website from computers from Power's IP address." *Id*. at 1063. Power Ventures "responded" to this technical barrier "by switching IP addresses to circumvent the Facebook block." *Id.* Given this behavior, this Court held that Power Ventures: (1) "deliberately disregarded the cease and desist letter and accessed Facebook's computers without authorization to do so," and (2) "circumvented IP barriers that further demonstrated that Facebook had rescinded permission for Power to access Facebook's computers." *Id*. at 1068. Accordingly, Power Ventures "accessed Facebook's computers 'without authorization' within the meaning of the CFAA and is liable under that statute." *Id*.

Just as in *Power Ventures*, LinkedIn completely revoked hiQ's access to its computers following hiQ's data-scraping activity. *Id*. at 1067. Just as in *Power*

Ventures, hiQ unleashed bots to access and scrape information from LinkedIn's physical servers. Just as in *Power Ventures*, LinkedIn erected a series of technical measures to guard against data-scraping software, including targeted IP address blocks. Just as in *Power Ventures*, LinkedIn sent hiQ a cease-and-desist letter that "plainly put [hiQ] on notice that it was no longer authorized to access [LinkedIn's] computers." *Id*. at 1067 n.3. Just as in *Power Ventures*, hiQ seeks to engage in future "technological gamesmanship" by re-deploying its anonymous, data-scraping bots to evade LinkedIn's technical barriers, *id*. at 1067—only this time it has enlisted the judiciary to tear down those barriers through a mandatory preliminary injunction. And just as in *Power Ventures*, this Court should hold that hiQ lacks authorization "within the meaning of the CFAA" to access LinkedIn's computers following LinkedIn's revocation of "[a]ny future access of any kind." 4ER-743.

Recognizing LinkedIn's right to enforce the CFAA here would be fully consistent with an unbroken line of CFAA cases holding that companies may revoke "authorization" for data-scraping software to access their computers, even where those companies operate public websites. For example, in *3Taps Inc.*, 964 F. Supp. 2d 1178, Craigslist alleged that "3Taps copies (or 'scrapes') all content posted to Craigslist in real time, directly from the Craigslist website," which it then allowed third parties to access in its competing products. *Id*. at 1180. Craigslist

"sent a cease and desist letter" informing 3Taps that it was "no longer authorized to access" the Craigslist website, and "configured its website to block access from IP addresses associated with 3Taps," which "3Taps bypassed" using "different IP addresses and proxy servers to conceal its identity, and continued scraping data." *Id*. at 1180-81. Even though "Craigslist gave the world permission (i.e., 'authorization') to access the public information on its public website," Judge Breyer held that Craigslist "rescinded that permission for 3Taps. Further access by 3Taps after that rescission was 'without authorization.'" *Id*. at 1184.

Numerous other courts have reached the same conclusion in comparable circumstances. *See, e.g.*, *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595-97 (E.D. Pa. 2016); *Couponcabin LLC v. Savings.com, Inc.*, No. 2:14-CV-39-TLS, 2016 WL 3181826, at *3-4 (N.D. Ind. June 8, 2016); *Sw. Airlines Co. v. Farechase, Inc*., 318 F. Supp. 2d 435, 437 (N.D. Tex. 2004); *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); *Ticketmaster L.L.C. v. RMG Techs., Inc*., 507 F. Supp. 2d 1096, 1102-03, 1113 (C.D. Cal. 2007); *United States v. Lowson*, Criminal No. 10-114 (KSH), 2010 WL 9552416, at *5-*7 (D.N.J. Oct. 12, 2010). Strikingly, neither hiQ nor the district court cite *a single case* in which a court has held that a free-riding competitor can access a publicly-available website—with data-scraping

bots or any other tool—after access has been revoked through a particularized cease-and-desist letter and technological barriers.

2. The district court's password revocation requirement contravenes the CFAA's text, structure, legislative history, and precedent

Notwithstanding the CFAA's unambiguous text, and the binding authority interpreting it, the district court issued a sweeping decision holding that once a company makes information available for public viewing, the only way to revoke permission to access its servers is through the use of password authentication systems that withdraw information from the public altogether. 1ER-15-16. That interpretation writes into the statute a limitation that is simply not there.

Turning first to text, the district court sought to justify its narrowing of the statute by claiming to find the statute ambiguous. 1ER-10 ("whether 'access' to a publicly viewable site may be deemed 'without authorization' under the CFAA where the website host purports to revoke permission is not free from ambiguity"). But this Court's precedents hold that "'without authorization' is an unambiguous, non-technical term that … means accessing a protected computer without permission." *Nosal II*, 844 F.3d at 1028. Under that unambiguous text, once hiQ received "particularized notice of [its] revoked access," *id.* at 1036, in the form of "an individualized cease-and-desist letter," *Power Ventures*, 844 F.3d at 1069, permission was rescinded and any future access to LinkedIn's servers with data-scraping bots would violate the CFFA.

The CFAA's structure also forecloses the district court's distinction between public and non-public websites. As Judge Breyer explained, "Congress might have written § 1030(a)(2) to protect only 'nonpublic' information. A neighboring provision in the CFAA includes that very modifier, and prohibits access without authorization to 'nonpublic' government computers. *See* 18 U.S.C. § 1030(a)(3). Another adjacent provision applies only to certain kinds of financial information. *See* § 1030(a)(2)(A)." *3Taps*, 964 F. Supp. 2d at 1182. This structure demonstrates that Congress "knew how to restrict the reach of the CFAA to only certain kinds of information, and it appreciated the public vs. nonpublic distinction—but § 1030(a)(2)(C) contains no such restrictions or modifiers." *Id*. at 1182-83; *see S.E.C. v. McCarthy*, 322 F.3d 650, 656 (9th Cir. 2003). The district court erred by rewriting the statute to impose the same public/non-public distinction through the terms "access" and "authorization" even though it is absent from the statutory text.

The CFAA's legislative history likewise offers no support to the district court's interpretation. *3Taps*, 964 F. Supp. 2d at 1186 ("This court has no grounds for favoring one set of vague statements [from the CFAA's legislative record] over the other."). To begin, there is no need to resort to legislative history because the CFAA's text is unambiguous. *Whitfield v. United States*, 543 U.S. 209, 215

(2005). If anything, that history disproves the district court's reading of the CFAA.

The district court thought it critical that Congress enacted the CFAA in 1984 to deal with problems that antedated the emergence of the public Internet. 1ER-10 ("the Internet did not exist in 1984"). Even if accurate, that observation would not justify narrowing the CFAA's plain terms. "[S]tatutory prohibitions often go beyond the principal evil to cover reasonably comparable evils, and it is ultimately the provisions of our laws rather than the principal concerns of our legislators by which we are governed." *Oncale v. Sundowner Offshore Servs., Inc*., 523 U.S. 75, 79 (1998).

But the observation was not accurate. The provision at issue here, § 1030(a)(2)(C), was added to the CFAA in ***1996***—not 1984—and as part of the same set of amendments that added the "nonpublic" modifier to government computers in § 1030(a)(3). By the mid-1990s, the publicly-accessible Internet was well-known. Shortly before Congress added these amendments, it passed the Telecommunications Act of 1996, which declared that "[it] is the policy of the United States to promote the continued development of the Internet and other interactive computer services and other interactive media." Pub. L. No. 104-104, §240, 110 Stat 56, 62-63 (1996). And when Congress added § 1030(a)(2)(C), it understood that "accessing" a "publicly available" computer "*via an agency's*

World Wide Web site" without authorization could trigger CFAA liability, *see* S. REP. NO. 104-357, at 8-9 (1996) (emphases added), and it added "nonpublic" to § 1030(a)(3) to avoid that result in the context of government computers. It did not do so for § 1030(a)(2)(C), however.

Moreover, Congress amended the CFAA again in 2001, 2002, and 2008—*after* courts applied the CFAA to bar the use of automated software devices to scrape data from publicly-available websites. *See* page 49 *supra* (discussing cases). Congress did not overturn these cases, nor did it carve out publicly-available webpages from the CFAA's reach, further underscoring the district court's misreading of the CFAA's legislative history. *Bateman v. Am. Multi-Cinema, Inc.*, 623 F.3d 708, 720 (9th Cir. 2010) (presuming that Congress is aware of past judicial interpretations when construing subsequently-amended statutes).

The district court's judicial rewrite of the CFAA also is foreclosed by Circuit precedent. *Power Ventures* was quite clear that unauthorized scraping violated the CFAA, even if individual users whose data was scraped had consented to make the information available to the scraper. 844 F.3d at 1068 ("Permission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter."). This Court found a CFAA violation because Facebook, "which stored this data on its physical servers," had revoked all authorized access. *Id.* For the same reason, the fact that LinkedIn's members may

allow their information to be indexed by search engines in order for their LinkedIn profiles to be found more easily online does not give hiQ permission to scrape their data from LinkedIn's servers over LinkedIn's objection. Indeed, the CFAA violation here is even more stark because (in contrast to Facebook's users), "the fact that a user has set his profile to public does not imply that he wants any third parties to collect and use that data for all purposes," as the district court acknowledged. 1ER-23.

The district court nevertheless distinguished *Power Ventures* on the theory that the defendant was scraping data found on "a portion of a website … that w[as] protected by a password," whereas here the information was "public." 1ER-9-10. But this Court's reasoning in *Power Ventures* did not turn on the existence of a password authorization system. The word "password" never appears in the decision. Nor does any comparable concept. Quite the contrary, this Court's reasoning was based on Power Ventures' use of automated software to scrape data from Facebook's servers without Facebook's permission, in disregard of IP blocks and a cease-and desist-letter completely revoking access to its computers—*precisely the circumstances that exist here*.

In this respect, the district court's reliance on *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017), was misplaced. 1ER-13-14. It read *Packingham* to support its novel and far-reaching presumption in favor of open access to the

Internet in the absence of password walls. But *Packingham* was concerned with North Carolina completely barring a person from accessing social media altogether—not an individual platform deciding whom to admit onto its servers. It was in the context of this far-reaching regulation that *Packingham* referred to the Internet as the "modern public square," 137 S. Ct. at 1737, but the decision itself was narrowly focused on the *scope* of the North Carolina law, which made it a felony for registered sex offenders to access all social networking sites where the offender knows that the site permits minors to become members or maintain webpages. *Id.* ("[T]he statute here enacts a prohibition *unprecedented in the scope* of First Amendment speech it burdens.… In sum, to foreclose access to social media *altogether* is to prevent the user from engaging in the legitimate exercise of First Amendment rights." (emphases added)).

In contrast to *Packingham*, LinkedIn revoked only hiQ's corporate access to its servers after hiQ engaged in gross misbehavior. LinkedIn does not seek to preclude hiQ's individual employees (or any other living, breathing human) from viewing the LinkedIn website. It has not taken action against any individual's account, nor has it barred hiQ's employees from viewing LinkedIn from their personal computers for professional networking purposes. LinkedIn has only

revoked hiQ's access after it deployed bots to perform forbidden acts that cause profound harm to LinkedIn's business and its members' privacy.[4]

In any event, even if *Packingham* had announced a new presumption in favor of open access to the Internet, the Court expressly sanctioned "narrowly tailored laws" to prohibit "specific criminal" uses of a website. 137 S. Ct. at 1737. Similarly, *Power Ventures* assumed that entities could run afoul of the CFAA, even if websites are presumptively "open," so long as "permission [to access them] is revoked expressly." 844 F.3d at 1067 n.2; *see EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003) ("Our basis for this view is not, as some have urged, that there is a 'presumption' of open access to Internet information. The CFAA, after all, is primarily a statute imposing limits on access and enhancing control by information providers."); *3Taps*, 964 F. Supp. 2d at 1184 (holding that while a website operator may give "the world permission (i.e., 'authorization') to access the public information on its public website," it may "rescind[] that

[4] For this reason, the district court was wrong that constitutional avoidance principles should be applied to the CFAA because "the act of viewing a publicly accessible website is likely protected by the First Amendment." 1ER-17 n.12. Not only is the avoidance doctrine inapplicable where the statute is unambiguous, *United States v. Shill*, 740 F.3d 1347, 1355 (9th Cir. 2014), but LinkedIn does not seek here to bar any living person from viewing a website or engaging in First Amendment activity. 1ER-17 n.12.

permission" for particular parties). That is exactly what happened here—and exactly why hiQ lacks authorization to access LinkedIn's servers.[5]

Lacking any support in the CFAA's text, structure, legislative history, and precedent, the district court ultimately could point only to a single law review article to support its effort to write a password revocation requirement into the CFAA. 1ER-13-16 (discussing Orin Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016)). But academic declarations about "the normatively desirable rules and standards that should govern Internet use," 116 Colum. L. Rev. at 1158, are not a proper basis for deciding cases under the law as it exists. Instead, this Court has consistently followed a modest, incremental approach that focuses on how the statutory text that Congress wrote applies to the facts of a given case. *E.g.*, *Power Ventures, Inc.*, 844 F.3d at 1067 n.2 (declining to address whether platforms are "presumptively open to all comers"); *Nosal II*, 844 F.3d at

[5] The district court also erred by concluding that "'authorization,'" as used in § 1030(a)(2), is "most naturally read in reference to the *identity* of the person accessing the computer or website, not *how* access occurs." 1ER-15. LinkedIn denied "access of any kind" to hiQ, (4ER-743), and so the district court's identity-based reading of "authorization" was irrelevant. In any event, the district court ignored that "authorization" modifies the term "access," and the CFAA plainly permits computer owners to revoke permission for certain types of "access." *3Taps Inc.*, 942 F. Supp. 2d at 969 (the "*methods* by which information may be accessed" are "more properly considered 'access' restrictions under the CFAA"); *United States v. Phillips*, 477 F.3d 215, 220-21 (5th Cir. 2007) (same). After all, a restaurant can prohibit a person entering on horseback but not on foot, and the person's equestrian-entry would be an unauthorized "access."

1029 (declining to address password sharing). And on *these facts*, the CFAA bars the use of data-scraping bots to access LinkedIn's computers after LinkedIn imposed technological barriers and sent a cease-and-desist letter revoking hiQ's access.

The district court first turned to Professor Kerr for its premise that the Internet is "generally perceived as 'inherently open,'" and the assertion that "courts should … 'adopt[] presumptively open norms for the Web.'" 1ER-13. But Kerr did not profess to describe prevailing law. Kerr *disagrees* with this Court's reasoning in *Power Ventures* and *Nosal II*,[6] and the far-reaching presumptions about Internet access that the district court invoked (based on Kerr's academic theories) cannot be squared with this Circuit's caselaw.

Next, the court adopted Kerr's view that "'authorization,' in the context of the CFAA, should be tied to an authentication system, such as password protection." 1ER-14. That conclusion is flatly at odds with this Court's holdings about the "unambiguous" meaning of the term "authorization." The district court

[6] Orin Kerr, *9th Circuit: It's a Federal Crime to Visit a Website After Being Told Not To Visit*, Wash. Post: The Volokh Conspiracy (July 12, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/12/9th-circuit-its-a-federal-crime-to-visit-a-website-after-being-told-not-to-visit-it/?utm_term=.a85a098d2c62; Orin Kerr, *Password-Sharing Case Divides Ninth Circuit in Nosal II*, Wash. Post: The Volokh Conspiracy (July 6, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/06/password-sharing-case-divides-ninth-circuit-in-nosalii/?utm_term=.7b9422653b81.

"impermissibly graft[ed] onto the statute" a new password "requirement nowhere to be found in the statute's text." *U.S. ex rel. Hartpence v. Kinetic Concepts, Inc.*, 792 F.3d 1121, 1127-28 (9th Cir. 2015) (en banc). Such extra-textual grafting was particularly inappropriate here because, as the district court acknowledged, this Court "has specifically rejected the argument that 'the CFAA only criminalizes access where the party circumvents a technological access barrier.'" 1ER-11 (quoting *Nosal II*, 844 F.3d at 1038). Indeed, a "password requirement is designed to be a technological access barrier" (*Nosal II*, 844 F.3d at 1039)—which the district court, in direct contravention of Ninth Circuit authority, engrained as a legal requirement under the CFAA.

The district court further erred when, applying "Professor Kerr's analysis," it held that "anti-bot measures" and cease-and-desist letters are legally insufficient to revoke permission. 1ER-15-16. There is no basis to conclude that passwords are the *only* measures that can be used to revoke authorization to information stored on a server connected to the Internet. Identical to the facts here, *Power Ventures* held that IP blocking, coupled with a cease-and-desist letter, unambiguously signal revocation. 844 F.3d at 1068.

Finally, the district court's physical space analogy reveals that the court simply misunderstood the facts of this case. It stated that "when a business displays a sign in a storefront window for the public to view, it may not prohibit on

pain of trespass a viewer from photographing that sign or viewing it with glare reducing sunglasses." 1ER-16 n.9. But hiQ's bots are not like photographers or glare reducing glasses that are used on the outside to look in. hiQ's bots physically connect to and access LinkedIn's servers. They are more like surreptitiously-planted video- or audio-recording devices that allow someone to monitor a space from within, without taking breaks to eat, use the bathroom, or perform other human functions. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1074 (9th Cir. 2004) (observing that a "police officer who, invited into a home, conceals a recording device for the media" would engage in trespass).[7]

Accordingly, the more apt analogy would treat LinkedIn as the equivalent of a massive job fair, held at a convention center and open to all comers. LinkedIn invites eager professionals of all stripes, including some who want to meet potential new employers. Knowing this, hiQ deploys legions of interns—each wearing a body camera—to fan out and station themselves at every table. They

[7] Indeed, humans could not gain access to the scope of information that hiQ's bots access and scrape without the use of those automated tools. *Cf. United States v. Jones*, 565 U.S. 400, 406 (2012); *id*. at 416 (Sotomayor, J., concurring) ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements."); *American Civil Liberties Union Found. of S. Cal. v. Superior Court*, 400 P.3d 432, 435, 437-38 (Cal. 2017) (emphasizing "the large volume of data that plate scanners and other similar technologies now enable agencies to collect indiscriminately"). As such, bots are entirely different from the acts of individual users who might view a website and manually record information, page by page.

covertly track the movements of every attendee and record every sign-in sheet and resume. hiQ then crunches that information and sells it to attendees' current employers. LinkedIn would be well within its rights to send a letter instructing hiQ and its camera-clad minions to stay out of its fair. And if the snoops returned and tried to reenter the convention center, LinkedIn would be able to sue for trespass. No court would enjoin LinkedIn from protecting its own business interests and the privacy of its attendees. The result should not be any different under the CFAA's computer-trespass prohibition simply because hiQ uses digital devices—or "bots"—to access, capture, and expropriate the data on LinkedIn's servers

3. The district court's rule imperils open Internet access and entrepreneurial innovation

The district court professed that it was attempting to preserve "the delicate balance between open access to information and privacy." 1ER-12. It failed in that effort, however, by declaring a sweeping rule that would expose every company whose business relies on a public website to mass scraping by automated software, so long as those websites do not have password authentication systems. That rule will profoundly damage open access to the Internet and the digital economy.

The first consequence of the district court's rule is that platforms seeking to protect their information and the privacy of their users will be forced to put their systems behind walls. As noted, LinkedIn blocks approximately 95 million

automated calls to its servers every day, and it has received numerous complaints from members who have discovered their scraped-profiles on other sites. Under the district court's and hiQ's rule, every company with a public portion of its website that is integral to the operation of its business—from online retailers like Ticketmaster to social networking platforms like Twitter—will be exposed to invasive bots deployed by free-riders unless they place those websites entirely behind password barricades. But once that happens, those websites will no longer be indexable, which will make information less available to discovery by the primary means by which people obtain information on the Internet—search engines. 4ER-762. The district court's password requirement would slam the door shut on the "openness and accessibility of that forum to all comers," (1ER-14)—the very value that drove the court's conclusion.

The district court's rule also threatens to stifle innovation. Entrepreneurs would have less reason to develop groundbreaking platforms if technological-copycats could hide behind the district court's reading of the CFAA. For example, if the district court's broad rule is upheld, Craigslist could not prevent an entity from scraping data to "'essentially replicate the entire craigslist website,'" *3Taps*, 964 F. Supp. 2d at 1180, simply because Craigslist's business required that the information on its website be available to the public. *See also* Appellant's Request for Judicial Notice, Ex. A ¶ 47 (Second Am. Complaint, *LinkedIn Corp. v.*

Scraping Hub Ltd., No. 5:16-cv-4463 (LHK) (N.D. Cal. June 7, 2017), ECF No. 39) ("Scrapinghub SAC") (pending action by LinkedIn against defendant Scrapinghub who allegedly scraped and sells dataset containing "nearly 300 million records" of LinkedIn profiles). Nor could online retailers prevent their sites from being scraped by bots, again because a publicly-available website could not revoke authorization absent a password system. *QVC, Inc.*, 159 F. Supp. 3d at 581, 591.

Minimizing these threats, the district court suggested that a website could still use "anti-bot measures" and other legal tools to prevent "harmful intrusions or attacks on its server[s]." 1ER-16. That is wrong.

First, and most immediately, LinkedIn cannot protect itself through technical measures because the district court's injunction requires LinkedIn to disable its defenses against hiQ's bots. The court forced LinkedIn to grant hiQ unlimited access to all data on its public site, for seemingly any use at all. And this is not a problem for LinkedIn alone. Every company that seeks to protect itself from free-riding would-be competitors will face the risk of a suit just like hiQ's.

Second, no technical barrier is perfect. Of the millions of bot attempts that LinkedIn blocks, some are still able to circumvent those measures through crafty technological gamesmanship, as this case demonstrates. 4ER-766; *see*

ScrapingHub SAC ¶¶ 49-50 (Scrapinghub statements that it circumvented LinkedIn's "very sophisticated bot counter-measures").

Third, the legal options the district court identified are inadequate. The court referenced § 1030(a)(5)(A) of the CFAA, which creates a cause of action against those who "cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer." But "damage" is defined as "any impairment to the integrity or availability of data, a program, a system or information," 18 U.S.C. § 1030(e)(8)(A), and data-scraping will not necessarily satisfy this definition.[8]

Similarly, the district court referenced the possibility of a trespass to chattels claim. 1ER-16 n.11. But such a claim also requires "some actual or threatened interference with the computers' functioning." *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1353 (2003). Demonstrating that any particular data-scraper has impaired the integrity of data or physically harmed LinkedIn's computer systems will be challenging. And courts have rejected trespass claims involving automated

[8] In passing the CFAA, Congress made clear that the CFAA was intended to cover "simple trespass against computers," whereas "subsection 1030(a)(5)" was "designed to penalize those who intentionally alter, damage, or destroy certain computerized data belonging to another." S. REP. NO. 99-432, at 7-13 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2484-91. By imposing a damage-to-computers requirement, the district court deprived LinkedIn of the "simple trespass" remedy Congress made available under the CFAA.

scrapers where the website operator could not show actual interference with the functioning of the site. *E.g.*, *Ticketmaster Corp. v. Tickets.com, Inc.*, No. 99CV7654, 2000 WL 1887522, at *2 (C.D. Cal. Aug. 10, 2000).

Finally, the district court's own speculative parade of horribles does not justify its ruling. In its view, the CFAA cannot reach "publicly viewable information" because that would allow websites owners to "block access by individuals or groups on the basis of race or gender discrimination," allow "[p]olitical campaigns" to "block selected news media, or supporters of rival candidates, from accessing their websites," or companies to "prevent competitors or consumer groups from visiting their websites to learn about their products or analyze pricing." 1ER-11-12.

But the facts of this case do not implicate these concerns. Holding that hiQ's continued access to LinkedIn is "without authorization" under the CFAA would in no way "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) (*Nosal I*). After all, most people do not use sophisticated automated software to evade anti-bot technological barriers after receiving a targeted cease-and-desist letter. *3Taps*, 964 F. Supp. 2d at 1184 (an "average person does not use 'anonymous proxies' to bypass an IP block set up

to enforce a banning communicated via [a] personally-addressed cease-and-desist letter").

Nor would applying the CFAA in this case endorse the kinds of abuses that worried the district court. The CFAA has been on the books for more than two decades, and the district court could not cite a single case or real-world example to support its hypotheticals. This is, in part, because alleged CFAA violations must cause loss "aggregating at least $5,000 in value," 18 U.S.C. § 1030(c)(4)(A)(i)(1), and it is unlikely that the CFAA could be arbitrarily enforced against individuals given the need to prove such losses. In addition, because the CFAA is both a criminal and civil statute, it should be read to bar "selective enforcement" by private plaintiffs in the same ways as such enforcement would be barred by prosecutors. *Shlay v. Montgomery*, 802 F.2d 918, 924-25 (7th Cir.1986) (recognizing "selective enforcement" claim for civil actions); *Salem Blue Collar Workers Ass'n v. City of Salem*, 832 F. Supp. 852, 863 n.9 (D.N.J. 1993) (same). And to the extent that private plaintiffs seek to enforce the CFAA to advance discriminatory ends, courts could invoke well-established precedent to reject those claims. *See Shelley v. Kraemer*, 334 U.S. 1 (1948); *United States v. Redondo-Lemos*, 27 F.3d 439, 443 (9th Cir. 1994) ("government endorsement or adoption of private discriminatory conduct that affects third parties can amount to a violation of equal protection"). In any event, the district court's approach does not come

close to eliminating the concerns that motivated the court to adopt it. That approach would not stop platforms from blocking users from getting login credentials, revoking login credentials, or using the CFAA to withdraw authorization to password-protected portions of their websites on the basis of race, gender, sexual orientation, or political affiliation.

All in all, the district court's rule would have the perverse effect of making the Internet less open and economically vibrant. Even if the CFAA were ambiguous, these consequences would be sufficient to reject the district court's approach. But there is no conceivable justification for adopting that approach in the face of statutory text, structure, history, and binding precedent that refute it. It is "for Congress to weigh the significance of those consequences and decide whether amendment would be prudent." *3Taps*, 964 F. Supp. 2d at 1187.

II. THE DISTRICT COURT ERRED IN ITS IRREPARABLE HARM ANALYSIS

Because hiQ failed to show that it has even a fair chance of succeeding on the merits, the district court erred in considering the remaining preliminary injunction factors. *Global Horizons*, 510 F.3d at 1057-58. It also erred in concluding that hiQ would suffer irreparable harm absent an injunction.

First, hiQ's alleged harm—that it will be forced to go out of business if it cannot access and scrape LinkedIn's website—is not cognizable because it stems from hiQ's inability to engage in illegal activity, *i.e.*, a violation of the CFAA.

Triad Sys. Corp. v. Se. Express Co., 64 F.3d 1330, 1338 (9th Cir. 1995). "One who elects to build a business on a product found to [be unlawful] cannot be heard to complain if an injunction … destroys the business so elected." *Windsurfing Int'l, Inc. v. AMF, Inc.*, 782 F.2d 995, 1003 n.12 (Fed. Cir. 1986); *Facebook, Inc. v. Power Ventures, Inc.*, No. 08-CV-5780-LHK, 2013 WL 5372341, at *16 (N.D. Cal. Sept. 25, 2013).

Second, even assuming hiQ's claimed injury could constitute cognizable harm, the court's finding that hiQ will go out of business absent the injunction constitutes clear error. The only evidence to support this claim are conclusory statements from hiQ's CEO. 5ER-991. In "seeking a preliminary injunction," however, hiQ needed to "establish a likelihood of irreparable harm that is grounded in evidence, not in conclusory or speculative allegations of harm." *Pom Wonderful*, 775 F.3d at 1133. hiQ offered no evidence to support its assertion that it could not shift its business model to rely on data from sources other than LinkedIn's servers, as several other companies operating in the data analytics space successfully do. 4ER-621.

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

The district court also erred in its consideration of the remaining preliminary injunction factors. As to the balance of equities, the court placed dispositive weight on hiQ's speculative (and non-cognizable) alleged harm of being precluded

from scraping LinkedIn, while downplaying the tangible injury LinkedIn will suffer from the court's injunction. For example, the injunction harms the trust and goodwill LinkedIn has developed with its members because the injunction places their privacy at risk. As the district court itself noted, "the fact that a user has set his profile to public"—including the 50 million LinkedIn members who specifically have used the "Do Not Broadcast" feature—"does not imply that he wants any third parties to collect and use that data for all purposes." 1ER-23; 3ER-430. The district court, however, brushed aside these privacy concerns. Furthermore, other parties will view the court's order as a "tacit invitation" to gain unauthorized access to LinkedIn's computers and scrape them or engage in other harmful conduct. *Guthy-Renker Corp. v. Evolution Skin Therapy, LLC.*, No. CV 08-911-VBF(FMOx), 2008 WL 5479112, at *3 (C.D. Cal. Dec. 16, 2008). This threatens to deprive LinkedIn of its ability to protect its site from any number of other malicious actors.

Finally, the "public has an interest in ensuring that computers are not accessed without authorization," as "courts have consistently held in CFAA cases." *Power Ventures, Inc.*, 2017 WL 1650608, at *16. Likewise, the public has a strong interest in the vibrancy of the modern Internet. As explained above, the district court's ruling puts those public interests in serious jeopardy.

CONCLUSION

For the foregoing reasons, the district court's decision granting hiQ a preliminary injunction must be reversed.

Respectfully submitted,

Dated: October 3, 2017

/s/ Donald B. Verrilli, Jr.

DONALD B. VERRILLI, JR.
CHAD I. GOLDER
MUNGER, TOLLES & OLSON LLP
1155 F Street N.W., 7th Floor
Washington, DC 20004-1361
Telephone: (202) 220-1100
Facsimile: (202) 220-2300
Donald.Verrilli@mto.com
Chad.Golder@mto.com

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

Attorneys for Defendant-Appellant
LinkedIn Corporation

ORRICK, HERRINGTON & SUTCLIFFE LLP

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

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

BRIAN P. GOLDMAN
405 Howard Street
San Francisco, CA 94105
(415) 773-5700
brian.goldman@orrick.com

Attorneys for Defendant-Appellant
LinkedIn Corporation

STATEMENT OF RELATED CASES

LINKEDIN is not aware of any related cases pursuant to Federal Rule of Appellate Procedure 28-2.6.

CERTIFICATE OF COMPLIANCE

I certify pursuant to Federal Rules of Appellate Procedure 32(a)(7)(C) and Circuit Rule 32-1 that the attached brief is proportionately spaced, has a typeface of 14 points, and, according to the word count feature of the word processing system used to prepare the brief (Microsoft Word 2010), contains 13,988 words.

Dated: October 3, 2017

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

STATUTORY ADDENDUM

18 U.S.C.A. § 1030

§ 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of--

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

> **(i)** an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or
>
> **(ii)** an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of--

> **(i)** an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or
>
> **(ii)** an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

> **(i)** an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or
>
> **(ii)** an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for--

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

[(5) Repealed. Pub.L. 110-326, Title II, § 204(a)(2)(D), Sept. 26, 2008, 122 Stat. 3562]

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States

that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of

the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States--

> **(A)** such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and
>
> **(B)** any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on October 3, 2017.

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

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

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

Dated: October 3, 2017

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