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 REPLY 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*

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

STATE CASES

FEDERAL STATUTES

STATE STATUTES

TREATISES

OTHER AUTHORITIES

INTRODUCTION

hiQ's case rests on a faulty premise. hiQ insists that because LinkedIn generally permits members of the public to view its website, LinkedIn must allow hiQ to scrape information from LinkedIn's computer servers. But LinkedIn is a private company that has every right to revoke access to its property when another company violates its policies and seeks to free-ride on its investment and damage its business. No matter how many times hiQ calls LinkedIn's website "public," it cannot alter the reality that LinkedIn's servers—physical computers located in data-storage warehouses—are private property, or deprive LinkedIn of its right to protect its business.

hiQ's theory is that LinkedIn effectively seeks to prohibit hiQ from viewing a "'sign in its storefront window visible … on a public street.'" Answering Brief (AB)-17 (quoting 1ER-15). But that analogy misses the mark. LinkedIn sent its cease-and-desist letter and erected technological barriers to prevent hiQ from re-accessing LinkedIn's *servers*. To obtain the massive amount of data hiQ seeks, it must dispatch thousands of bots to access those servers, and copy the data housed there. In other words, hiQ must enter the "store." It cannot obtain what it wants by viewing from the "street." As such, hiQ's data-scraping is more akin to a company deploying an army of employees to invade a bookstore and copy books—or really, whole bookshelves—without permission and by circumventing the

store's security measures. Like any reasonable business owner, LinkedIn seeks to prohibit hiQ from re-entering the "store" after hiQ engaged in comparable misconduct. hiQ cannot plausibly claim that it has a legal right to access LinkedIn's "store" for the express purpose of copying and selling the information in the "books" that are located inside.

hiQ's affirmative claim for relief depends on the California Unfair Competition Law (UCL), but the UCL does not require LinkedIn to grant hiQ access to scrape LinkedIn's servers in violation of LinkedIn's rules and policies. Insisting that it is not advancing a duty-to-deal claim (even though that is precisely the claim hiQ advanced below and the district court adopted), hiQ now seeks to swap in a newly-minted "exclusive dealing" claim that it never raised below—a sure sign that the district court's injunction rests on shaky ground. Labels aside, the gravamen of hiQ's UCL claim remains that LinkedIn must provide hiQ with the data stored on its servers in the "commercially []feasible" form hiQ prefers. AB-44 n.15. That contention is groundless. No antitrust principle requires LinkedIn to make the data on its servers available to hiQ in bulk at all, much less in an easy-to-analyze, "commercially advantageous" form. *Pacific Bell Tel. Co. v. Linkline Commc'ns, Inc.*, 555 U.S. 438, 450 (2009). And hiQ *still* does not define a relevant market or demonstrate LinkedIn's market power. That, too, is fatal to

hiQ's UCL claim: it is impossible to evaluate hiQ's claim of harm to competition without demonstrating what the market is.

Because hiQ has no entitlement to relief under state law, the preliminary injunction can be vacated on that basis alone. In addition, hiQ's Computer Fraud and Abuse Act (CFAA) arguments are meritless. LinkedIn revoked hiQ's access after hiQ engaged in repeated misconduct while accessing LinkedIn's property. Any attempt to re-access LinkedIn's servers following this clear revocation would be "without authorization" under the CFAA's unambiguous language and this Court's decision in *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), *cert. denied*, No. 16-1105, 2017 WL 978168 (U.S. Oct. 10, 2017). Accordingly, it was wrong to forbid LinkedIn from invoking the CFAA. What's more, the CFAA itself preempts hiQ's state law claims—all of which boil down to an assertion that LinkedIn could not prevent hiQ from accessing LinkedIn's private servers because hiQ has a legal right of access to them.

Ultimately, hiQ asks this Court to create a distinct competition and property law regime for the Internet that would depart radically from the firmly-established legal rules that govern those bodies of law. Unlike brick-and-mortar businesses that may refuse to assist free-riding competitors and may rely on trespass law to eject misbehaving patrons, online businesses could no longer prevent free-riding or exclude bad actors. Such a result would be completely at odds with both core

antitrust principles and the CFAA, which "prohibits acts of computer trespass." *Id.* at 1065. Perversely, it would also threaten the very "open Internet" that hiQ invokes. Companies like LinkedIn would have no choice but to erect password walls if they want to protect their websites against bot-deploying free-riders (and other kinds of copycats and malicious wrongdoers), thereby reducing what is available to the public online. No court has endorsed such a transformative rule. This Court should not be the first. The district court's mandatory preliminary injunction should be vacated.[1]

I. HIQ HAS NOT SHOWN A LIKELIHOOD OF SUCCESS ON THE MERITS, MUCH LESS THE CLEAR ENTITLEMENT TO RELIEF REQUIRED TO JUSTIFY A MANDATORY INJUNCTION

A. hiQ Has No Entitlement to Relief Under the UCL.

The UCL does "not require the courts to protect small businesses from the loss of profits due to continued competition, but only against the loss of profits from practices forbidden by the antitrust laws." *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 186 (1999) (internal quotation marks omitted). In particular, the UCL does not grant courts a roving commission to enjoin

[1] hiQ contends that the injunction is not "mandatory." But by requiring LinkedIn to disable its protections against hiQ's data-scraping bots and to facilitate hiQ's access to LinkedIn's servers, the district court imposed affirmative obligations, putting LinkedIn in a far different position than the "last, uncontested status which preceded the pending controversy." *Regents of Univ. of Cal. v. Am. Broad. Cos.*, 747 F.2d 511, 514 (9th Cir. 1984). In any event, hiQ cannot satisfy the standard for obtaining a prohibitory injunction.

whatever strikes them as "unfair." To justify relief, a plaintiff must prove that a defendant's conduct "threatens an incipient violation of the antitrust law" or has effects that "are comparable to or the same as a violation of the law, or otherwise significantly threaten[] or harm[] competition." *Id.* at 187. Most importantly, a plaintiff must prove harm to competition, and not merely to itself. *Id*. at 186-87.

hiQ purports to acknowledge this requirement. AB-43. But the only injury hiQ actually alleges is to itself, and it seeks protection of its business regardless of what the antitrust laws actually require. *E.g.*, AB-46-47 n.16 (arguing that the "threatened harm to competition is" LinkedIn's attempt to "eliminate[] a competitor"). hiQ tries to repackage these contentions as harms to competition generally, arguing that LinkedIn's conduct "decreas[es] industry output" and "increase[es] the likelihood that LinkedIn will dominate the market." AB-43. But hiQ introduced no evidence below to substantiate those market-wide effects. *See infra* pp. 11-13. To the contrary, the competitive harms hiQ asserts all stem from the same source: alleged injuries to hiQ. hiQ's attempt to equate its own viability with that of the market is insufficient as a matter of law. *E.g.*, *Gorlick Distrib. Ctrs., LLC v. Car Sound Exhaust Sys., Inc*., 723 F.3d 1019, 1025 (9th Cir. 2013)

(rejecting a plaintiff's attempt "to translate its individual harm into harm to competition").[2]

Nor does hiQ offer any response to the argument (Appellant's Opening Brief (AOB)-18) that it is hiQ's forced-sharing rule—not LinkedIn's conduct—that would harm competition. This silence underscores that hiQ does not seek to advance consumer welfare or protect competition in any asserted marketplace. It just wants to free-ride. hiQ's rule would have the perverse effect of deterring entrepreneurs from investing in innovative products and services and engaging in the "vigorous, aggressive" competition that the "antitrust laws are meant to champion." *United States v. Syufy Enters.*, 903 F.2d 659, 669 (9th Cir. 1990). It would permit would-be competitors to leech the assets of successful companies, simply because the aspirant claims it offers a "new, value-added service." AB-3. This position cannot be squared with the bedrock principle that "[a]llowing a

[2] hiQ errs by relying on *Flagship Theaters of Palm Desert, LLC v. Century Theaters, Inc.*, 198 Cal. App. 4th 1366 (2011), to contend that "eliminating one competitor at a time can constitute harm to competition under California law." AB-43-44. *Flagship* addressed "antitrust injury"—a concept not at issue here. It did *not* address whether a defendant has alleged an "injury to competition" sufficient to establish a violation on the merits. *Electronic Waveform Lab, Inc. v. EK Health Servs.*, No. CV 15-8061 DMG (RAOx), 2016 WL 1622505, at *7 (C.D. Cal. Mar. 1, 2016) ("'antitrust injury' … is distinct from 'injury to competition'" and *Flagship* only addressed "antitrust injury"). Indeed, just months after it decided *Flagship*, the same court reiterated that "[i]njury to a competitor is not equivalent to injury to competition; only the latter is the proper focus of antitrust laws." *Marsh v. Anesthesia Servs. Med. Grp., Inc.*, 200 Cal. App. 4th 480, 495 (2011) (internal citation and quotation marks omitted).

business to reap the fruits of its investments … is what 'induces risk taking that produces innovation and economic growth.'" *Four Corners Nephrology Assocs., P.C. v. Mercy Med. Ctr. of Durango*, 582 F.3d 1216, 1221 (10th Cir. 2009) (quoting *Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko*, 540 U.S. 398, 407 (2004)). hiQ's UCL claim—and the arguments it offers to defend it—are meritless.

1. Despite its protestations, hiQ's UCL claim *does* seek to impose a duty to deal.

hiQ argues that this case is "unlike *Trinko*, and even unlike *Aspen Skiing*, because the basis for hiQ's claim is not a refusal to deal by LinkedIn." AB-49. That is a remarkable assertion. hiQ argued below—and the district court accepted—that LinkedIn was "unfairly leveraging" its asserted (but unproven) monopoly power by refusing to deal with hiQ. 1ER-21. That shift in theory alone is reason to doubt the propriety of the injunction.

hiQ also cannot escape *Trinko* so easily. Whatever label hiQ now attaches to its UCL claim, there is no doubt that hiQ seeks an order compelling LinkedIn to disable its technological barriers and provide hiQ's bots with access to LinkedIn's servers so that hiQ can obtain data in a "commercially []feasible" form best suited to its business model. AB-44 n.15. That is a paradigmatic duty-to-deal claim. But under the UCL, "the mere refusal to deal does not violate the spirit or policy of antitrust law." *People's Choice Wireless, Inc. v. Verizon Wireless*, 131 Cal. App.

4th 656, 667 (2005). "*Trinko* … makes clear that if a firm has no antitrust duty to deal with its competitors at wholesale, it certainly has no duty to deal under terms and conditions that the rivals find commercially advantageous." *Linkline*, 555 U.S. at 450.

Nor is there any merit to hiQ's argument that it is entitled to access LinkedIn's servers "on the same terms as other members of the public (including commercial services like Google and Bing that use automation)." AB-48-49. "[B]usinesses are free to choose the parties with whom they will deal." *Linkline*, 555 U.S. at 448. LinkedIn has no duty to grant hiQ's bots access to its servers simply because LinkedIn decided to provide some other companies with access. LinkedIn has good reason to treat hiQ differently from Google and Bing. Access by those search engines furthers LinkedIn's and its members' objectives to be discovered online, whereas hiQ's intrusions damage LinkedIn's business and its relationship with its members. And given that its technological barriers block an average of 95 million bot incursions *every day*, 4ER-761, LinkedIn can hardly be accused of singling out hiQ's bots.[3]

[3] While some bots perform positive functions on the Internet, there is no doubt that others—like hiQ's free-riding bots—are "bad." Adrienne Lafrance, *The Internet Is Mostly Bots*, The Atlantic (Jan. 31, 2017), https://www.theatlantic.com/technology/archive/2017/01/bots-bots-bots/515043/. These "bad" bots include those that have "caused mass internet disruptions," as well as "unauthorized-data-scrapers, spambots, and scavengers seeking security vulnerabilities to exploit." *Id*. Bots also can threaten privacy. Electronic Privacy Information Center (EPIC) Br. 15,

hiQ nonetheless insists that there is no "meaningful difference" between allowing hiQ employees to read member profiles "one at a time" and allowing them to unleash bots on LinkedIn's servers to scrape that information *en masse*. AB-44 n.15. But hiQ itself spotlights the critical difference: hiQ's scraping enables it to expropriate data far "more quickly with automation," thereby allowing hiQ to obtain LinkedIn's aggregated information in a "commercially []feasible" manner. *Id*. As hiQ admits, it does not want to hire "thousands of employees to manually read and copy" LinkedIn's website. *Id*. That is, hiQ doesn't want to make an investment or take a risk comparable to what LinkedIn did to build its own database. Instead, hiQ wants LinkedIn to turn over that information in a commercially advantageous form that would allow hiQ to free-ride on LinkedIn's investment. LinkedIn has no antitrust duty to give hiQ that shortcut.[4]

ECF No. 18 ("By prohibiting LinkedIn from implementing [anti-bot] measures, the lower court has effectively eliminated key techniques that protect the privacy of user data."). And some "Grinch-bots" have even been accused of stealing Christmas. Samantha Raphelson, '*Grinch Bots' Attempt To Steal Christmas By Driving Up Toy Prices* (Dec. 5, 2017), https://www.npr.org/2017/12/05/568624246/grinch-bots-attempt-to-steal-christmas-by-driving-up-toy-prices. The antitrust laws do not require LinkedIn to provide access to "bad," free-riding, data-scraping bots, simply because it welcomes a limited number of "good" bots.

[4] *Authenticom, Inc. v. CDK Global, LLC*, 874 F.3d 1019 (7th Cir. 2017), confirms this. Like hiQ, Authenticom claimed that it was being blocked from accessing and scraping defendants' data, and that "without relief it [was] likely to be forced to shutter its business altogether." *Id*. at 1023. (Unlike hiQ, *Authenticom* introduced *some* evidence of harm to competition, including increased prices. *Id*.) The Seventh Circuit held that the trial court's order was "inconsistent with *Trinko*"

2. hiQ's new "exclusive dealing" theory is meritless.

Because its duty-to-deal theory so plainly lacks merit, hiQ now contends that LinkedIn's actions are a vertical restraint imposed on LinkedIn's members not to deal with a competitor. hiQ never raised this argument below, so it is waived. *Idaho Watersheds Project v. Hahn*, 307 F.3d 815, 830 (9th Cir. 2002).

Nonetheless, hiQ's latest antitrust theory is as meritless as its others. LinkedIn imposes no exclusivity requirement. If members want to share their personal information with hiQ, they are free to do so. LinkedIn's User Agreement provides that members "own the content and information that [they] submit" and "are only granting LinkedIn … [a] non-exclusive license." 5ER-893. Thus, LinkedIn does *nothing* to prevent its members from dealing directly with hiQ. Only LinkedIn itself is choosing not to deal with hiQ. *LiveUniverse, Inc. v. MySpace, Inc.*, 304 F. App'x 554, 557 (9th Cir. 2008) ("All MySpace has done is prevent consumers from accessing vidiLife.com through MySpace.com. Consumers remain free to choose which online social networks to join.").[5]

---

because it "forc[ed] [the defendants] to do business with Authenticom on terms to which they did not agree." *Id*. at 1026. hiQ argues that the defendants there were ordered to "grant Authenticom access to non-public databases and data not available to the public." AB-50 n.17. But *nothing* in the court's analysis turned on that distinction, nor does hiQ explain why the non-public nature of the information is relevant to a *Trinko* analysis when hiQ similarly seeks to force LinkedIn to do business with it on hiQ's preferred terms.

[5] hiQ further errs (AB-49) by suggesting that LinkedIn promised that it would "honor member choices about who can access their content." The User Agreement

Ultimately, hiQ's exclusive dealing theory suffers from the same flaws as its other forsaken theories. Instead of putting in the work to attract information voluntarily, hiQ wants to free-ride. That is why hiQ introduced no evidence that it ever asked LinkedIn's members for their information instead of trying to covertly scrape it from LinkedIn's servers *en masse*. LinkedIn's members are free to give their data to hiQ, but hiQ does not want to invest the time or money to find out if they will.

3. hiQ's failure to define a market or demonstrate market power is fatal to its UCL claim.

LinkedIn explained that hiQ's UCL claim falters at the start because hiQ did not define a relevant market or demonstrate that LinkedIn had market power. AOB-26-29. Unable to correct this shortcoming, hiQ now contends that "[w]hether LinkedIn will obtain a monopoly in any well-defined market for purposes of a hypothetical Sherman Act claim is irrelevant to whether the conduct is 'unfair' under the UCL." AB-47.

---

prohibits using automated software—including "bots"—to access and scrape LinkedIn's computers, 5ER-896; 4ER-761-762 & 4ER-775, and it informs members that LinkedIn "reserves the right to restrict, suspend, or terminate" the access of those who violate these prohibitions, 4ER-763 & 4ER-772. hiQ's response brief ignores that hiQ itself agreed to these conditions and to refrain from deploying data-scraping bots *on multiple occasions*. AOB-8-9. Member choices must be understood in light of these provisions, which provide comfort that LinkedIn will attempt to prevent their information from being scraped by companies like hiQ.

That assertion is baseless. Even if hiQ were correct that UCL reaches some sliver of purportedly anticompetitive conduct beyond conduct that violates the antitrust laws, a court must know *what* the relevant market is to assess whether conduct unfairly affects competition *within* it. The California Supreme Court is crystal clear that "any finding of unfairness" under the UCL must be "tethered to … proof of some actual or threatened impact on competition." *Cel-Tech*, 20 Cal. 4th at 186-87. It "is plaintiff's burden to make the required showing of a substantially adverse effect on competition *in the relevant market*." *Marsh*, 200 Cal. App. 4th at 495 (emphasis added and internal quotation marks omitted). hiQ's failure to define a market or demonstrate market power therefore defeats its claim.

Even more to the point, all of hiQ's now-discarded antitrust theories were grounded in the Sherman Act, Compl. ¶¶ 65-69 (5ER-1007-1008); AB-41; the district court relied on those Sherman Act theories, 1ER-21-22; and hiQ's newfangled "exclusive dealing" theory is explicitly premised on the Sherman Act, AB-50. But "[a]n independent claim under California's UCL is … barred so long as [a defendant's] activities are lawful under the antitrust laws." *City of San Jose v. Office of the Comm'r of Baseball*, 776 F.3d 686, 692 (9th Cir. 2015); *LiveUniverse*, 304 F. App'x at 558 ("Because LiveUniverse fails to state a claim under the Sherman Act, it also fails to state a claim under § 17200."). Indeed, the California courts have held that "[i]f the same conduct is alleged to be both an

antitrust violation and an 'unfair' business act or practice for the same reason—because it unreasonably restrains competition and harms consumers—the determination that the conduct is not an unreasonable restraint of trade necessarily implies that the conduct is not 'unfair' toward consumers." *Chavez v. Whirlpool Corp.*, 93 Cal. App. 4th 363, 375 (2001).

These cases describe a commonsense rule: a plaintiff cannot prevail on an "unfair" UCL challenge to conduct that a court would otherwise uphold under the antitrust laws, simply by omitting a Sherman Act claim. hiQ's UCL claim therefore must fail because it would not survive the antitrust analysis that it transparently tried to duck by alleging a Sherman Act claim under a different name.

hiQ seeks to escape the consequences of its failure to define a relevant market or demonstrate market power by arguing that LinkedIn cited no case dismissing a UCL claim on these grounds. But most UCL plaintiffs do not fail to make so fundamental an allegation. Nonetheless, examples exist. *Hacienda Pools, Inc. v. Anthony & Sylvan Pools, Inc.*, No. E028132, 2001 WL 1441431, at *5 (Cal. Ct. App. Nov. 14, 2001) (unpublished); *Sidibe v. Sutter Health*, 4 F. Supp. 3d 1160, 1181 (N.D. Cal. 2013). And this Court has held that the failure to satisfy an element of a Sherman Act claim is sufficient to defeat an "unfair" UCL claim.

LiveUniverse, 304 F. App'x at 557. hiQ offers no reason why this would not apply to other missing elements of antitrust claims.

B. hiQ's Tortious Interference Claim Is Meritless.

Although the district court addressed hiQ's tortious interference claim only in a footnote, hiQ contends that it "provides an independent basis for affirmance." AB-52. This is incorrect: the district court held that the analysis of hiQ's interference claim "simply overlaps with the analysis of the unfair competition claim." 1ER-23 n.14. It did not consider whether hiQ had proved the elements of this claim or any defenses that LinkedIn raised.

In all events, hiQ's tortious interference claim fails for multiple reasons. As an initial matter, only lawful contracts are protected, so any contracts to sell products based on scraped-data are "tainted with illegality," *i.e.*, hiQ's CFAA violation. AOB-32.

Separately, hiQ has not shown any entitlement to relief on its tortious interference claim. *First*, LinkedIn acted with a legitimate business purpose. *Citizens of Humanity, LLC v. Costco Wholesale Corp.*, 171 Cal. App. 4th 1, 11-12 & n.7 (2009) (citing *Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal. 4th 26, 57 (1998)); *Dollar Tree Stores Inc. v. Toyama Partners, LLC*, No. C 10-00325 SI, 2010 WL 1688583, at *4 (N.D. Cal. Apr. 26, 2010). Here, LinkedIn acted legitimately to protect member privacy and to preserve the trust and goodwill of its

members, which are vital to the success of its business. *Infra* p. 28. Contrary to hiQ's argument (AB-55), LinkedIn's privacy concerns are not pretextual because its "Recruiter" product respects members' privacy choices. LinkedIn informs members that it will use their information in other services that LinkedIn provides, and unlike hiQ's products, "Recruiter" respects the "Do Not Broadcast" feature that 50 million LinkedIn members have elected to use. 2ER-59-60.

Second, LinkedIn revoked hiQ's access because hiQ was violating its User Agreement. Enforcing a contract cannot possibly be an improper purpose. *Richardson v. La Rancherita La Jolla, Inc.*, 98 Cal. App. 3d 73, 81 (1979) (where a party has "a prior contract of [its] own … [it] is privileged to prevent performance of the contract of another which threatens it"). hiQ cites *Quelimane*, 19 Cal. 4th 26, for its contention that enforcing legal rights cannot qualify as a "proper purpose," but hiQ nowhere explains how *Quelimane* supports its assertion, *Quelimane* stands for no such thing, and courts have held otherwise, *Pacific Gas & Electric Co. v. Bear Stearns & Co.*, 50 Cal. 3d 1118, 1137 (1990); *Sweeley v. Gordon*, 47 Cal. App. 2d 385, 386 (1941). hiQ also makes the extraordinary argument that asserting LinkedIn's legal rights advances no socially valuable objective and is not a "business" purpose. AB-56. Under any definition of those terms, enforcing contractual rights qualifies. At the most basic level, it is legitimate for LinkedIn to protect itself from free-riders like hiQ.

Third, hiQ presented no evidence that LinkedIn *intended* to disrupt hiQ's contracts. LinkedIn acted to protect its servers from data-scraping bots—not to interfere with hiQ's contracts. Even if LinkedIn was aware that its actions would affect hiQ's contracts, that consequence was "'so far removed from … [LinkedIn's] objective that … the interference may be found to be not improper.'" *Quelimane*, 19 Cal. 4th at 56 (quoting Restatement (Second) Torts § 766 cmt. J at p. 12).

C. hiQ's Deployment of Data-Scraping Bots to Access LinkedIn's Servers Following Revocation Violates the CFAA.

hiQ's failure to establish any valid state-law cause of action justifies vacatur of the preliminary injunction without any further consideration of the CFAA. But if the Court does reach the CFAA, it should reject hiQ's flawed argument that LinkedIn cannot exclude hiQ from its property, simply because LinkedIn's servers host "publicly-viewable" websites.

hiQ was not viewing data on LinkedIn's website like any human could do. hiQ was using a sophisticated legion of bots to extract data from hundreds of thousands of aggregated profiles stored on LinkedIn's *servers*. AOB-8-10. But those servers are *not* "open to the public" for any and all purposes. LinkedIn is not a public park, a public street, or any other public place. LinkedIn's servers are private property. Just like other property owners, LinkedIn may condition access to its servers, including by imposing rules prohibiting access through automated

scraping. In the digital realm, as in the physical, the decision to bar someone is likely to be motivated by violations of a property owner's rules ("No shirt, no shoes, no service"). And when entities violate those rules and are ejected, LinkedIn may deny access in the future.[6]

After hiQ blatantly violated LinkedIn's rules prohibiting automated scraping, LinkedIn revoked any further access by following the approach prescribed in *Power Ventures*. LinkedIn sent hiQ a targeted cease-and-desist letter and implemented technical measures making it unmistakable that continued access "of any kind" would be unauthorized. 4ER-743. Under the text, structure, and history of the CFAA, as well as this Court's decisions, LinkedIn's revocation means that future access by hiQ's bots is "without authorization."

1. hiQ is incorrect that LinkedIn could not revoke its authorization to access its computers.

As hiQ acknowledges, this Court has held that "without authorization" is "'an unambiguous, non-technical term.'" AB-19 (quoting *United States v. Nosal*, 844 F.3d 1024, 1028 (9th Cir. 2016) (*Nosal II*)). As hiQ further recognizes (AB-22), this Court has held that "a defendant can run afoul of the CFAA when he or

[6] LinkedIn contends only that hiQ's access to its servers would be "without authorization" *after* LinkedIn revoked that access following hiQ's misconduct. Accordingly, this case does *not* raise the issue resolved in *Nosal I*—whether a party accessing a website in violation of its terms of use "exceeds authorized access" under the CFAA. While terms-of-use violations are not enforceable through the CFAA, *Power Ventures* holds that "revocation[s] of access" *are* enforceable, once a party is "clearly notified" of the revocation. 844 F.3d at 1069.

she has no permission to access a computer or when such permission has been revoked explicitly." *Power Ventures*, 844 F.3d at 1067.

hiQ nonetheless contends that LinkedIn "does not grant permission to access its public content because those pages are, by definition, open for all to see and use," and that there is thus "no 'authorization' for LinkedIn to revoke." AB-19-20, 22-24. But whether something is "open … to see" at one point in time tells you nothing about whether permission can be revoked. Retail stores typically are "open for all," but visitors can be evicted if they break the proprietor's rules.

Power Ventures recognizes this principle and thereby forecloses hiQ's argument. This Court assumed that entities *could* violate the CFAA *even if* websites are "presumptively open to all comers," so long as "permission [to access them] is revoked expressly." 844 F.3d at 1067 n.2. hiQ's assertion (AB-23-24) that *Power Ventures* defined revocation only in the context of "private" websites is therefore incorrect.

Even if this Court had not already addressed the issue in *Power Ventures*, hiQ's focus on "public" content on webpages still would have no purchase. hiQ ignores that bots access and extract "data on … [LinkedIn's] physical servers." 844 F.3d at 1068. And the CFAA regulates access to *physical* computer servers, not simply the information that resides on them. *Power Ventures* made clear that "[p]ermission from the users alone was not sufficient to constitute authorization

after Facebook issued the cease and desist letter," *id*., even though the information itself belonged to the users, not Facebook. Like Facebook, LinkedIn "store[s member] data on its physical servers." *Id*. Thus, authorization from LinkedIn—the server's *owner*—is "needed" to avoid CFAA liability, regardless of whether those servers also host data that LinkedIn generally makes available on its website. *Id*.[7] hiQ lacked that required "authorization" once LinkedIn sent hiQ its cease-and-desist letter and implemented additional technological barriers restricting bot access.[8]

---

[7] hiQ's reference (AB-21) to a separate statute—the Health Insurance Portability and Accountability Act—demonstrates how insubstantial its CFAA arguments are. No definition of "protected health information" in HIPAA's text—let alone the agency regulations that hiQ cites—purports to inform the meaning of "without authorization" under the CFAA.

[8] Contrary to hiQ's assertion (AB-19-20, 37), LinkedIn's servers do not "automatically provide" LinkedIn pages, and LinkedIn's countermeasures are not limited to IP address blocking; they include a range of sophisticated authentication and security protections that block *95 million bot-attempts every day*. AOB-7-8. hiQ's own chief technology officer recently stated that LinkedIn has been "aggressively complaining about what they considered unfair scraping practices for quite some time," and that LinkedIn goes "through a lot of trouble technically to make it difficult to collate that data." Drake Bennett, *The Brutal Fight to Mine Your Data and Sell It to Your Boss* (Nov. 15, 2017), https://www.bloomberg.com/news/features/2017-11-15/the-brutal-fight-to-mine-your-data-and-sell-it-to-your-boss. hiQ also wrongly describes LinkedIn's technical measures as "not actually 'barriers' to access." AB-37. This Court has rejected the argument that the CFAA only bars "access where the party circumvents a technological access barrier," *Nosal II*, 844 F.3d at 1038, and *Power Ventures* found a CFAA violation where the defendant "circumvented IP barriers" (and ignored a cease-and-desist letter), 844 F.3d at 1068.

There is nothing unusual about an owner whose property is generally open to the public enforcing standards that condition access to that property. For example, a bookstore may bar visitors who copy books or act rowdily. Further access by these rule-breakers would be trespass. The CFAA embodies the same principles: it "prohibits acts of computer trespass by those who are not authorized users." *Id.* at 1065; *id.* at 1068 (analogizing the CFAA to "the physical world" and explaining that once a "bank ejects [a] person from its premises and bans his reentry" because he was "carrying a shotgun," that visitor "could not then reenter the bank").

Accordingly, every court to reach the issue—except the district court here—has held that a computer owner may revoke access to servers that host data available on a publicly-viewable website when a party violates the rules of access, including through automated scraping. AOB-39-40. hiQ largely ignores these decisions, arguing only that *3Taps* was "wrongly decided." AB-24. But in hiQ's view, any company whose business model depends on a publicly-viewable website is at the mercy of bots deployed by free-riding competitors, malefactors launching denial of service attacks, and other cyber-wrongdoers.[9]

[9] Contrary to hiQ's argument (AB-19), *Nosal I* did not address methods of access. It held that "CFAA does not extend to violations of use restrictions." *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (*Nosal I*). As LinkedIn explained (AOB-48 n.5), however, the statute's "without authorization" prong, modifies the term "access," and well-established precedent holds that the CFAA permits

hiQ's emphasis on "public" websites also cannot be reconciled with the CFAA's structure and legislative history. hiQ has no response to the argument (AOB-42) that "Congress might have written § 1030(a)(2) to protect only 'nonpublic' information. A neighboring CFAA provision includes that very modifier, and prohibits access without authorization to 'nonpublic' government computers. *See* 18 U.S.C. § 1030(a)(3)." *Craigslist Inc. v. 3Taps*, 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013). This structure demonstrates that Congress "appreciated the public vs. nonpublic distinction—but § 1030(a)(2)(C) contains no such restrictions or modifiers." *Id*. at 1182-83. Similarly, hiQ's discussion of legislative history (AB-32-33) does not grapple with the fact that § 1030(a)(2)(C) "was added to the CFAA in *1996*"—after the spread of the Internet—not 1984, and was done so as part of the same set of amendments that added the "nonpublic" modifier in § 1030(a)(3) for the specific purpose of carving out CFAA liability for access to public government *websites*. AOB-43.

hiQ concludes its CFAA discussion with tag-along policy arguments. Putting aside that hiQ nowhere defines the source of its "Federal Policy of an Open Internet," these arguments are for Congress, not this Court. Anyhow, hiQ has it backwards. hiQ's rule will make the Internet *less* open. AOB-53-54. Companies

---

computer owners to revoke permission for certain types of prohibited "access" (*e.g.*, by bots), just like "a restaurant can prohibit a person entering on horseback but not on foot." hiQ does not respond.

with publicly-available portions of their websites will be exposed to invasive bots deployed by free-riders unless they move those websites behind password barriers. Many will likely do so in order to protect their businesses, thereby reducing the amount of information available to the public. hiQ does not dispute these consequences.

2. hiQ's constitutional avoidance arguments fail.

hiQ did not assert a free-standing First Amendment claim, nor could it: "LinkedIn is not a … governmental agency," and the absence of "state action presents a serious hurdle to any direct First Amendment claim against LinkedIn in this case." 1ER-16-17 n.12.

Nonetheless, hiQ attempts to shoehorn its constitutional arguments into the doctrine of constitutional avoidance. AB-25. But where, as here, the "statutory language" is "not ambiguous, the doctrine of constitutional avoidance is inapplicable." *United States v. Shill*, 740 F.3d 1347, 1355 (9th Cir. 2014). At any rate, hiQ raises no "serious" constitutional questions, let alone the "'grave doubts'" that the doctrine requires. *Ileto v. Glock, Inc.*, 565 F.3d 1126, 1144 (9th Cir. 2009).

hiQ errs in contending that LinkedIn's CFAA interpretation might violate the First Amendment. Private parties may not "claim special protection from governmental regulations of general applicability simply by virtue of their First

Amendment protected activities." *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 705 (1986). Thus, laws protecting private property against unauthorized intrusion may be enforced without raising any First Amendment concern. The Supreme Court "has never held that a trespasser or an uninvited guest may exercise general rights of free speech on property privately owned and used nondiscriminatorily for private purposes only." *Lloyd Corp. v. Tanner*, 407 U.S. 551, 568 (1972); *Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971) ("First Amendment is not a license to trespass, to steal, or to intrude by electronic means").

The CFAA is a law of general applicability that regulates conduct independently of whether it has any connection to expressive activity. It prohibits unauthorized access to computer systems without regard to speech or speaker. Its bar on unauthorized intrusion by hiQ's bots therefore raises no First Amendment concern. *3Taps*, 964 F. Supp. 2d at 1186 n.8.[10]

hiQ nonetheless asserts a broad "right to access" information on LinkedIn's servers. AB-26. In support, hiQ cites several unrelated cases involving

[10] hiQ wrongly reads *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017), as providing a general right to Internet access. AB-26-27. As LinkedIn explained (AOB-45-46), *Packingham* addressed *the scope* of the state law at issue, which allowed North Carolina to ban *all* access to certain websites regardless of whether the website-owners would permit access. It said nothing to limit a website operator from limiting who may access its property, and it held that "the First Amendment permits a State to enact specific, narrowly tailored laws" restricting access to websites. 137 S. Ct. at 1737. hiQ offers no response.

communications mediums. AB-30. But those cases did not announce any "right to access." They merely applied the First Amendment to various evolving technologies.

hiQ cites *no case* holding that the First Amendment guarantees one private party the right to gain access to information held by another private party. The closest hiQ comes—and it is not close—is *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011). But *Sorrell* merely invalidated a content- and viewpoint-based restriction on certain "information's use by some speakers and for some purposes." *Id*. at 580. The CFAA, by contrast, is content- and viewpoint-neutral.

Sorrell also is inapposite because the information-provider was willing to share its data, and the right to receive information "presupposes a willing speaker." *Virginia State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 756 (1976); *Bond v. Utreras*, 585 F.3d 1061, 1078 (7th Cir. 2009). Where parties do not wish for their speech to be accessed in a particular form, they are not "willing speakers." *Gregg v. Barrett*, 771 F.2d 539, 547-48 (D.C. Cir. 1985).

hiQ offered no evidence that LinkedIn or its members are "willing speakers" in the sense that they wish to make their profile data available for scraping by hiQ's bots. As noted, LinkedIn's User Agreement bars the use of data-scraping bots, and members know that when joining. More than 50 million LinkedIn members have chosen to limit the public availability of their activity. 3ER-427-

430. And LinkedIn has received numerous complaints from members who discovered their scraped information on other sites. 3ER-431-432, 3ER-434-439.

Even if there were a sweeping "right to receive" information held by private parties, hiQ has no right to receive information in the manner it demands. hiQ argues that "it makes no difference whether hiQ accesses information using bots, as supposedly distinct from 'living, breathing human[s].'" AB-29. But there is no First Amendment right to access information in a specific form. *Houchins v. KQED, Inc.*, 438 U.S. 1, 15 (1978) (First Amendment did not require state to provide access to information "as conveniently as [recipient] might prefer."); *Putnam Pit, Inc. v. City of Cookeville, Tenn.*, 221 F.3d 834, 840-41 (6th Cir. 2000); *Belo Broad. Corp. v. Clark*, 654 F.2d 423, 426-27 (5th Cir. 1981). While hiQ may find it "'good,' 'desirable,' or 'expedient'" to scrape LinkedIn's data through bots, this is not "constitutionally commanded." *Houchins*, 8 U.S. at 13.

Left without any First Amendment-based avoidance argument, hiQ hypothesizes a risk of discriminatory enforcement. AB-25. But hiQ does not cite *a single real-world instance* where that has occurred in the decades since the CFAA was enacted. hiQ also disregards that this is, in part, because CFAA violations must cause loss "aggregating at least $5,000 in value," 18 U.S.C. § 1030(c)(4)(A)(i)(I), so it is unlikely that the CFAA could be arbitrarily enforced against individuals. AOB-57. And hiQ ignores that courts may bar discriminatory

"selective enforcement" of the CFAA by private plaintiffs in the same ways as they could bar such enforcement by the government. AOB-57-58.

hiQ's reliance on *Larkin v. Grendel's Den, Inc.*, 459 U.S. 116 (1982)—an Establishment Clause case—is misplaced. A law does not raise constitutional concerns under *Larkin* simply because it delegates to a private party some authority to "determine what conduct is prohibited." AB-32. What was delegated there was the right to control who could obtain a liquor license, which is within the province of the state. By contrast, the power to determine who can enter one's private property has always been up to the property owner. *E.g.*, Cal. Penal Code § 602(l) (trespass includes entering private lands where no-trespassing signs are posted). hiQ's rule would topple centuries of property law that underlies the CFAA—the federal "computer trespass" statute. *Power Ventures*, 844 F.3d at 1065.

3. hiQ's CFAA violation preempts its claim for injunctive relief.

hiQ argues that the CFAA would not preempt its state-law claims because it "does not conflict with unfair competition law or common law governing interference with contract or economic advantage." AB-39. But the CFAA permits a computer-owner to bar access "without authorization." When the CFAA applies, there is a right to exclude. A state-law cause of action that would grant an affirmative right of access therefore conflicts with the CFAA, and hiQ's requested

"injunction would stand as an obstacle to the accomplishment of the full purposes and objectives of federal" law. *Brown v. Kerr-McGee Chem. Corp.*, 767 F.2d 1234, 1242 (7th Cir. 1985). Thus, as the district court acknowledged, "the CFAA would preempt all state and local laws that might" force LinkedIn to provide a "right of access" to hiQ. 1ER-12.

hiQ contends that there is no preemption because the CFAA was "designed to target hackers." AB-38-39. But that is not a preemption argument; it is a re-hash of hiQ's erroneous CFAA interpretation. The preemption question arises only if LinkedIn is correct as to the CFAA and hiQ is correct as to its state law claims. In that event, there is a conflict between the CFAA and the preliminary injunction. The CFAA must prevail.

II. THE REMAINING PRELIMINARY INJUNCTION FACTORS FAVOR LINKEDIN

hiQ does not dispute that the remaining preliminary injunction factors are irrelevant where, as here, a movant fails to establish any chance of success on the merits. Even so, hiQ cannot establish irreparable harm based on its inability to engage in proscribed conduct. AOB-58-59. In addition, hiQ wrongly insists that its CEO's declaration stating that hiQ will go out of business absent an injunction establishes irreparable harm. His conclusory and speculative statements are not "grounded in evidence." *Pom Wonderful, LLC v. Hubbard*, 775 F. 3d 1118, 1133 (9th Cir. 2014). This record stands in contrast to *Disney Enterprises, Inc. v.*

VidAngel, Inc., 869 F.3d 848, 865-66 (9th Cir. 2017), where the plaintiffs "provided uncontroverted evidence" beyond a single conclusory declaration. Finally, without offering any evidence, hiQ merely parrots (AB-57) the district court's unsupported conclusion that changing its business model is "comparable" to "going out of business." Other courts have rightly held otherwise. *E.g.*, *Complete Entm't Res. LLC v. Live Nation Entm't, Inc.*, No. CV 15-9814 DSF (AGRx), 2016 WL 3457178, at *3 (C.D. Cal. May 11, 2006).

The balance of hardships and the public interest similarly favor LinkedIn. hiQ belittles LinkedIn's privacy concerns as "[in]direct economic harm," AB-58, but fails to appreciate the relationship between privacy protection and consumer goodwill. *Gonzalez v. Google, Inc.*, 234 F.R.D. 674, 684 (N.D. Cal. 2006). Harm to LinkedIn's goodwill is as irreparable as any of hiQ's asserted harms. *Stuhlbarg Int'l Sales, Co. v. John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001).

hiQ's data-scraping is "not only contrary to the interests of individual LinkedIn users, it is contrary to the public interest." EPIC Br. 16. The public has a strong interest in ensuring "the ability of individuals to control the collection and use of their personal data held by others." *Id.* hiQ also has no answer to LinkedIn's argument that hiQ's position threatens an open Internet. AOB-60. Nor does hiQ deny that the public has a powerful interest in ensuring that computers are protected from unauthorized intrusions.

CONCLUSION

For the foregoing reasons, the preliminary injunction should be vacated.

Respectfully submitted,

Dated: December 11, 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

CERTIFICATE OF COMPLIANCE

I certify pursuant to Federal Rules of Appellate Procedure 32(a)(7)(C) and Circuit Rule 32-1 that the attached brief is proportionately spaced, has a typeface of 14 points, and, according to the word count feature of the word processing system used to prepare the brief (Microsoft Word 2010), contains 6,998 words.

Dated: December 11, 2017

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

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on December 11, 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: December 11, 2017

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