CASE NO. 17-16783

In the United States Court of Appeals For the Ninth Circuit

HIQ LABS, INC.

Plaintiff-Appellee,

VS.

LINKEDIN CORPORATION

Defendant-Appellant.

Appeal From The United States District Court for the Northern District of California, Case No. 3:17-cv-03301 The Honorable Edward M. Chen, Presiding

PLAINTIFF-APPELLEE HIQ LABS, INC.'S ANSWERING BRIEF

FARELLA BRAUN + MARTEL LLP
C. BRANDON WISOFF
DEEPAK GUPTA
JEFFREY G. LAU
REBECCA H. STEPHENS
235 Montgomery Street, 17th Floor
San Francisco, California 94104
Telephone: (415) 954-4400
Facsimile: (415) 954-4480

KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, PLLC
AARON M. PANNER
GREGORY G. RAPAWY
T. DIETRICH HILL
1615 M Street, N.W.
Suite 400
Washington, DC 20036
Telephone: (202) 326-7900
Facsimile: (202) 326-7999

Attorneys for Plaintiff-Appellee hiQ Labs, Inc.
(additional counsel listed inside cover page)

(additional counsel continued from cover page)

LAURENCE H. TRIBE*
CARL M. LOEB UNIVERSITY PROFESSOR AND PROFESSOR OF CONSTITUTIONAL LAW
HARVARD LAW SCHOOL
1575 Massachusetts Avenue
Cambridge, Massachusetts 02138
(617) 495-1767
**Affiliation noted for identification purposes only*

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Plaintiff-Appellee hiQ Labs, Inc. states that CEB, Inc. owns more than 10% of hiQ's stock. CEB, Inc. is a subsidiary of Gartner, Inc., a publicly-held corporation.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

FEDERAL CASES

STATE CASES

FEDERAL STATUTES

STATE STATUTES

FEDERAL RULES AND REGULATIONS

LEGISLATIVE HISTORY

OTHER AUTHORITIES

INTRODUCTION

hiQ is a data analytics company that creates award-winning human resources tools for Fortune 500 companies. To do so, hiQ analyzes information that LinkedIn's members affirmatively choose to make publicly available to everyone on the Internet (and in which LinkedIn expressly disclaims ownership). For years, LinkedIn has known of hiQ's products and attended hiQ's conferences, even accepting an award from hiQ. Earlier this year, however, after announcing that it would offer competing data analytics products, LinkedIn abruptly blocked hiQ's access to public profile information that is available to everyone else in the world and threatened civil (and even criminal) liability under the Computer Fraud and Abuse Act ("CFAA") for any continued access. After a hearing, the district court found that (1) LinkedIn's CFAA claims were likely meritless; (2) LinkedIn's actions likely violated state law; (3) hiQ would suffer irreparable harm without preliminary relief; and (4) the balance of equities and the public interest strongly favored relief. The district court preliminarily enjoined LinkedIn from blocking hiQ's access to public data and suspended any threat of CFAA liability for that access.

This Court should affirm. LinkedIn does not and cannot offer any serious challenge to the district court's findings on the equitable factors; because those factors weigh heavily in hiQ's favor, hiQ need only raise "serious questions" on

the merits – a relatively modest showing – to support provisional relief. hiQ satisfies that standard because the CFAA does not place the power of criminal sanction behind a website owner's selective denial of access to disfavored individuals to view public information on the Internet. The CFAA prohibits only "obtain[ing] information" by accessing a computer "without authorization." 18 U.S.C. § 1030(a)(2)(C). When information is public, no "authorization" is required to access it. LinkedIn's CFAA interpretation – which would give private parties the power to block disfavored individuals' access to public information – is not only inconsistent with the statutory language but would also raise serious constitutional issues. Furthermore, LinkedIn's actions – which the district court found were likely motivated by a desire to destroy a competitor and not by any legitimate concern about member privacy – are both tortious under common law and "unfair" under California's Unfair Competition Law ("UCL").

Unable to dispute the district court's factual findings, LinkedIn relies on rhetoric disparaging hiQ as a "scraper" and a "free rider" engaging in "surveillance" with "bots." But using software to automate data collection is common, legitimate, and key to the functioning of the modern Internet. Search engines like Google and Bing (owned by LinkedIn's parent Microsoft) "scrape" not only particular websites but large swaths of the Internet millions of times per day. Nor is hiQ a free rider, seeking to duplicate LinkedIn's professional network.

None of the data at issue belongs to LinkedIn; it belongs to members who have designated it public. hiQ collects data from narrow subsets of public profiles and analyzes it to provide predictive insights – a new, value-added service – to its clients. (Clients do not hire hiQ to scrape data; they want hiQ's analysis.) The value those companies see in hiQ's analyses explains why LinkedIn is now entering that market with a competing product.

Contrary to LinkedIn's arguments, hiQ's claim does not conflict with the antitrust principle that a monopolist generally has no duty to deal with a would-be rival. hiQ's business requires no affirmative assistance from LinkedIn because hiQ uses only data belonging to LinkedIn's members who expressly made their profiles public. LinkedIn could have designed a website that prevented its members from posting profile data publicly; indeed, it could change its website's design today, if its users would tolerate that (which it knows very well they would not). What LinkedIn cannot do is prevent hiQ from providing its own service using information that does not belong to LinkedIn and that LinkedIn has no right to control. Nor can LinkedIn acquire that right by repurposing the CFAA to criminalize access to public information. At minimum, these questions should be determined on a more fully developed record. In the meantime, preliminary relief is necessary to ensure that hiQ survives to have its day in court.

JURISDICTIONAL STATEMENT

LinkedIn's jurisdictional statement is complete and correct.

STATEMENT OF THE ISSUES

Whether the district court abused its discretion in granting preliminary relief to hiQ, based on its findings that (1) hiQ raised serious questions about whether (a) 18 U.S.C. § 1030(a)(2)(C) and California Penal Code § 502 empower a website owner to impose liability on disfavored individuals who access information posted to the public Internet, and (b) LinkedIn's actions likely violated the UCL and tortiously interfered with hiQ's contracts and relationships; and (2) the irreparable-injury, balance-of-hardships, and public-interest prongs of the preliminary-injunction standard all militate strongly in hiQ's favor?

STATEMENT OF THE CASE

A. hiQ Labs and Its Services

hiQ is a data analytics start-up that has raised over $14.5 million in multiple rounds of funding since its 2012 inception. It applies predictive data science to provide its Fortune 500 clients "people analytics" – insights into their workforce – by analyzing LinkedIn public profile information. 5ER-988 (¶¶ 3-4).

hiQ provides two services: (a) "Keeper," which identifies employees at greatest risk of being recruited away, and (b) "SkillMapper," which summarizes the breadth and depth of employees' skills. *Id* (¶¶ 4-6). With Keeper, employers can "develop action plans for retaining [their] talent" by offering at-risk employees career

development opportunities or retention bonuses. *Id* (¶ 5). hiQ won "Top HR Product" honors in 2016 for Keeper. 4ER-628. SkillMapper empowers employers to "build succession plans, drive employee engagement, promote internal mobility, and reduce costs associated with external talent acquisition," by, for example, identifying and offering training in areas where employees' skills are lacking. 5ER-988-89 (¶ 6).

To provide these services, hiQ gathers data that its clients' employees have designated as public (*e.g.*, name, job title, skills, work history) on the LinkedIn site. hiQ scientifically analyzes that data and provides statistical insights that fulfill clients' needs and (through opportunities for promotions, bonuses and training) add to the value of a public LinkedIn profile. Each data set analyzed is a tiny subset of LinkedIn's more than 500 million members. Contrary to LinkedIn's assertion, hiQ does not resell or republish the underlying data. The analytics it provides to its clients is a new, transformative product. 5ER-989 (¶ 9).

In early 2017, hiQ had 23 employees, most in San Francisco. Eleven had advanced degrees, including several PhDs. 5ER-988 (¶ 3). After LinkedIn's cease-and-desist letter, employees began to leave. hiQ now has 11 employees.

B. LinkedIn's Professional Network And Member Public Profiles

LinkedIn's core business is an online professional network that aggregates self-published profile information for about 500 million professionals. 5ER-888. The

network's purpose is for professionals "to meet, exchange ideas, learn and find opportunities." 5ER-892 (§ 1.1). User-generated profiles contain resume information including education, skills, publications, and employment history. *See, e.g.*, 5ER-899. LinkedIn is the largest, most up-to-date and authoritative repository of information about the world's professionals. 5ER-888.

LinkedIn is an "intermediary" which takes advantage of the Internet's one-to-many communication infrastructure by giving each member the means of posting a professional billboard. LinkedIn attracts users to post information (which LinkedIn would not otherwise have on its servers) by expressly (1) disavowing any ownership in or claim to the data, (2) agreeing that LinkedIn's right to use the data will be "non-exclusive," and (3) assuring members that they, and not LinkedIn, will decide who can access and use their information. *E.g.*, 5ER-893 (§ 3.1) ("*you own* the content and information that you submit" and "are only granting LinkedIn the following *non-exclusive* license"), 5ER-901 ("You *control the visibility and reach of your LinkedIn profile.*"). To facilitate this control, LinkedIn allows members to specify which profile portions are visible to the general "public" and which are visible only to direct connections, their "network" (those within three degrees of separation), or all LinkedIn members. 5ER-899.

The "public" setting (at issue here) gives access to "everyone," members and non-members alike: "[a]ll LinkedIn members as well as others who find you through

search engines (e.g. Google, Bing) or other services." 5ER-997. Public profiles are accessible without signing in, agreeing to LinkedIn's User Agreement, or obtaining a password. Members value public profiles because they serve as professional billboards and lead to expanded networks and opportunities.

Since its 2002 founding, LinkedIn has created several revenue streams that capitalize on member-generated content. As of hiQ's launch in 2012, LinkedIn's annual revenues approximated $1 billion, increasing to nearly $ 4 billion by the end of 2016. *Compare* 5ER-909 *with* 5ER-912. In late 2016, Microsoft purchased LinkedIn for $26 billion. 5ER-915.

C. hiQ Pioneered The Business That LinkedIn Now Seeks To Enter

hiQ has led the people analytics field since launching in 2012. hiQ even established an "Elevate" conference to bring together thought leaders and those trying to understand this new industry, share insights, and disseminate best practices. 5ER-989 (¶ 12).

LinkedIn knew for years that hiQ was relying on public LinkedIn profiles for its business. By October 2015, LinkedIn was actively participating in hiQ's Elevate conferences, where hiQ openly discussed its business and data collection practices. LinkedIn sent at least ten representatives to Elevate, including some who attended multiple times, took on a speaking role, and applied for and received the Elevate "Impact" Award in 2016. In late 2016 and early 2017, hiQ's former CEO held a

series of in-person meetings with LinkedIn personnel discussing hiQ's business. 5ER-989-90 (¶¶11-14); 4ER-756 (¶¶5, 6, 8).[1]

LinkedIn is now building its own people analytics offerings based on public profiles. 5ER-932, 941. In an earnings call three years after hiQ's launch, LinkedIn's CEO announced a plan to "enter a new category" by creating products for other companies which "leverag[e] content and data that members are already sharing publicly." 5ER-932. He explained:

> So by way of example, *our public profile information*, which particularly at larger organizations, you see some of those companies turning to LinkedIn *to look up someone within their own company*, because of how robust that public profile information can prove to be . . . . *[W]e're trying to think about ways in which we can better leverage that to create value within an organization.*

5ER-941 (emphasis added).

On June 21, 2017, LinkedIn's CEO announced the launch of a product that would analyze skills data from member profiles, just as hiQ's SkillMapper does:

> [W]hat LinkedIn would like to do is leverage all this extraordinary data we've been able to collect by virtue of having 500 million people join the site. We have over 10 million jobs that are now listed on the site. 50,000 standardized skills. *For employers, it's an understanding*

[1] LinkedIn did not seriously dispute its long-standing knowledge of hiQ's use of public profiles. It submitted a single declaration from only one of its ten or so Elevate conference attendees, who stated that he "does not recall" being told at one conference (in October 2015) how hiQ obtained its data, though he "learned a bit about hiQ and the product it had." 4ER-756 (¶ 5). He carefully avoided stating what he did learn at that conference, what he knew from other sources and conferences, and when he learned it. hiQ's showing was thus largely unrebutted.

> *of what skills they're gonna need to be able to continue to grow, and where that talent exists.*

4ER-0583 (emphasis added). A few days later, an IT buyer at a blue-chip Wall Street firm who had been evaluating hiQ's technology for purchase revealed that LinkedIn was marketing its SkillMapper-like product head-to-head against hiQ. 3ER-460.

D. LinkedIn Suddenly Purports To Revoke hiQ's Access To Public Information and Implements hiQ-Specific Blocking Measures

On May 23, 2017, without forewarning, LinkedIn's counsel emailed hiQ a letter stating that hiQ was improperly "access[ing] and copy[ing]" LinkedIn public profile information. 5ER-990 (¶ 15); 5ER-920. The letter demanded that hiQ immediately cease and desist accessing LinkedIn's website or any data stored there. 5ER-921. LinkedIn accused hiQ of violating LinkedIn's User Agreement, state trespass law, the CFAA, California Penal Code § 502, and the Digital Millennium Copyright Act, and stated:

> hiQ's company page on LinkedIn has been restricted. Any future access of any kind by hiQ is without permission and without authorization from LinkedIn. Further, LinkedIn has implemented technical measures to prevent hiQ from accessing, and assisting others to access, LinkedIn's site, through systems that detect, monitor, and block scraping activity.

5ER-921.

hiQ, through counsel, contacted LinkedIn to explain that it had a right to access public pages, that its business is synergistic to LinkedIn's (not injurious), and that complying with LinkedIn's letter would devastate hiQ. During that call, LinkedIn's

counsel could not identify any server impairment from hiQ's activities and conceded that LinkedIn allows other commercial enterprises, including Google and Yahoo!, to programmatically analyze the site. 5ER-882 (¶¶ 2-5).

On May 31, 2017, hiQ's counsel again wrote to LinkedIn detailing how LinkedIn's actions were threatening hiQ's business, pending financing round, and customer relationships. 5ER-926. LinkedIn did not respond. 5ER-882 (¶ 6).

Because LinkedIn's letter threatened criminal liability, hiQ ceased accessing LinkedIn's site and promptly filed the underlying action seeking a declaration of its rights and responsibilities and a TRO to preserve hiQ's access until the merits could be decided. hiQ also sought to recover the damages it suffered from LinkedIn's actions.

E. The Proceedings Below

On June 29, 2017, the district court held a hearing on hiQ's TRO request. LinkedIn justified its actions almost exclusively on supposed member privacy concerns, calling hiQ's unfair competition claim a "total red herring." 3ER-464:8-9. The district court expressed skepticism about LinkedIn's broad reading of the CFAA and Penal Code, which could prevent anyone for any reason from merely viewing the site and taking notes. LinkedIn attempted to narrow its claims by arguing that its only concerns were "bots" and "scraping" rather than manual access. 3ER-447-49; 3ER-502. The district court found it "a pretty big pill to

swallow" that manual copying was permissible but copying data "quickly and automatedly" would be a federal crime. 3ER-471. Because most data cannot be aggregated manually in a useful manner, the court observed, even LinkedIn's narrower position would have "pretty serious implications" for "future research, future access, future speech, [and] the way that information is collected and exchanged in our society." 3ER-503. The court also noted that LinkedIn's CFAA invocation introduced "a state action element" for constitutional purposes: "Once you invoke the imprimatur of the state, I think it changes the analysis." 3ER-0477:12-16; 3ER-0478:1-2. After the hearing, the parties stipulated to extend a negotiated standstill permitting hiQ's continued access and to convert the TRO motion into a preliminary injunction motion. SER-1-6.

At the preliminary injunction hearing, LinkedIn again disputed that its purpose was to block a competitor, claiming it was acting only to preserve member privacy. LinkedIn contended that hiQ's activities undermine the "Do Not Broadcast" feature which allegedly prevents a member's network from receiving updates of that member's profile changes. 2ER-87. hiQ countered that its technology does not track and disclose every profile update, instead providing a composite score based on numerous variables signaling "pull risk." 2ER-98. hiQ noted that LinkedIn, on the other hand, touts its "Update Me" feature to purchasers

of LinkedIn's Recruiter product as offering the precise profile change updates that LinkedIn falsely accused hiQ of providing:

> From now on, when they update their profile or celebrate a work anniversary, you'll receive an update on your homepage….*And don't worry — they don't know you're following them.*

2ER-100 (emphasis added); 2ER-69. The district court thus dismissed LinkedIn's privacy argument, stating, "Frankly, I don't find that convincing." 2ER-111.

The district court then granted hiQ's requested preliminary injunction. 1ER-1. It found that the potential consequences to hiQ without injunctive relief – breaching customer agreements, laying off employees, and shuttering its operations – were "sufficient to constitute irreparable harm." 1ER-4-5. The court determined that the balance of hardships tipped "sharply in hiQ's favor" because LinkedIn's asserted harms were "tied to its users' expectations of privacy" and "uncertain at best." 1ER-7.

Applying this Court's sliding-scale preliminary injunction standard, the court found that hiQ raised "serious questions going to the merits" on its substantive claims. 1ER-8. The court expressed "serious doubt" whether LinkedIn's purported revocation of permission to access public pages of its site rendered hiQ's access "without authorization" under the CFAA. 1ER-8-15. The court also found that hiQ raised serious questions regarding whether LinkedIn was motivated by an anticompetitive purpose in violation of the UCL, 1ER-21-23, and

that hiQ's tortious-interference claim "overlapped" with the UCL analysis. 1ER-23 n.14. Finally, the court found that the public interest favored hiQ because LinkedIn's use of government-backed CFAA sanctions to block particular users from accessing public information "could pose an ominous threat to public discourse and the free flow of information promised by the Internet." 1ER-0024. The district court's order thus (1) suspended any legal effect of LinkedIn's cease-and-desist letter and (2) enjoined LinkedIn from blocking hiQ's access to public profiles.

SUMMARY OF THE ARGUMENT

Under this Court's sliding-scale preliminary injunction standard, hiQ's showing that the balance of equities tips sharply in its favor means that hiQ need only show "serious questions" about the merits of its claims. The court acted well within its discretion in concluding that hiQ had made such a showing.

I. LinkedIn is wrong that the CFAA criminalizes efforts to read or use public information on the Internet whenever the owner of the computer hosting the information purports to block access by disfavored individuals. The CFAA prohibits "obtain[ing] information" from protected computers "without authorization," but no authorization is required to access or obtain information displayed publicly on a website. Under LinkedIn's flawed interpretation, a website owner could selectively make a criminal of anyone who views information that

anyone else in the world may readily view. LinkedIn's CFAA interpretation also raises serious constitutional questions: it would put the power of state sanction behind a website owner's decision to bar disfavored individuals from viewing public information, even when that decision is based on anticompetitive motives, racial or religious animus, or political disagreement. Nothing in the CFAA's history or purpose supports such a radical interpretation, and the canon of constitutional avoidance precludes it. The court's finding that hiQ raised substantial issues with respect to its CFAA declaratory relief claim independently supports the portion of the order suspending potential liability for continued access, irrespective of hiQ's affirmative state-law claims.

II. hiQ has also raised serious questions about whether LinkedIn's actions violate California law. LinkedIn's attempt to diminish competition in the people analytics market to ease its own entry threatens harm to competition and falls within the wide range of conduct prohibited by the UCL. The district court's finding that LinkedIn's "privacy" justifications are suspect is well-supported by the record and strengthens the inference that LinkedIn is acting with improper (anticompetitive) motives. LinkedIn cannot defend its conduct by contending that hiQ has not proven a market definition under the Sherman Act; hiQ did not bring a Sherman Act claim, and the UCL requires no market definition. Nor can LinkedIn rely on the principle that a firm has no duty to deal with a competitor. hiQ does

not need "to deal" with LinkedIn; it needs LinkedIn to stop selectively blocking its access to public profile information owned by LinkedIn's members. Indeed, LinkedIn's emphasis on appeal – that it can "refuse to deal" with a "competitor" – highlights the pretextual nature of the privacy justifications it relied on below. LinkedIn's actions also fulfill every element of tortious interference with hiQ's contractual and business relations. The burden will be on LinkedIn to prove at trial some legitimate purpose for its conduct.

III. The district court's determination that the equitable factors favor hiQ was well within its discretion. The existential threat to hiQ's business absent injunctive relief constitutes irreparable harm. The balancing of hardships favors hiQ, because LinkedIn could identify no concrete countervailing harms, and any theoretical injuries are "uncertain, at best." The public interest also favors hiQ because of the potential harm to public discourse posed by LinkedIn's actions. The district court thus properly granted a preliminary injunction. This Court should affirm.

STANDARD OF REVIEW

A preliminary injunction order is reviewed for abuse of discretion. *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011). The Court employs a two-part test: (1) whether the district court identified the correct legal standard to apply to the relief requested; and (2) whether the court's application of

that standard was "illogical," "implausible," or "without support in inferences that may be drawn from the facts in the record." *Pimentel v. Dreyfus*, 670 F.3d 1096, 1105 (9th Cir. 2012) (internal citations omitted). The district court's factual findings are reviewed for clear error. *Wild Rockies*, 632 F.3d at 1131.

The Supreme Court articulated a four-part preliminary injunction test in *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008) (likelihood of success on the merits; irreparable harm absent relief; balance of equities tips in movant's favor; injunction is in the public interest). This Court applies a sliding-scale approach allowing for a preliminary injunction where "serious questions going to the merits [are] raised and the balance of hardships tips sharply in [plaintiff's] favor." *Wild Rockies*, 632 F.3d at 1131.

LinkedIn's argument that hiQ "faces an especially high hurdle" because the district court supposedly entered a "mandatory" injunction, Dkt. 6 at 29, is incorrect because the injunction was prohibitory, not mandatory. The order "prohibits [LinkedIn] from taking action and 'preserves the status quo pending a determination of the action on the merits.'" *Marlyn Nutraceuticals, Inc. v. Mucos Pharma GmbH & Co.*, 571 F.3d 873, 879 (9th Cir. 2009) (citation omitted); *see Heckler v. Lopez*, 463 U.S. 1328, 1333 (1983) (prohibitory injunction "freezes the positions of the parties until the court can hear the case on the merits").

The order's requirement that LinkedIn withdraw its cease-and-desist letter and remove measures it recently implemented to block hiQ does not make the injunction mandatory. Those requirements merely return the parties to "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) (citation omitted). The "last uncontested status" before this case was that hiQ had the same ability to access public LinkedIn profiles as any other member of the public. hiQ need not meet any special burden.

ARGUMENT

I. HIQ IS LIKELY TO SUCCEED ON ITS CLAIM THAT THE CFAA DOES NOT PROHIBIT ACCESS TO PUBLIC WEBPAGES

The CFAA, a statute enacted to combat hacking and protect digital privacy, does not prohibit any user from accessing public web content, even against the website owner's wishes. Public webpages are, by definition, available worldwide and without restriction. No one needs "authorization" to access them. A website owner cannot revoke a user's authorization to view public pages because there is no authorization to revoke.

The district court drew an apt analogy:

> [I]f a business displayed a sign in its storefront window visible to all on a public street and sidewalk, it could not ban an individual from looking at the sign and subject such person to trespass for violating such a ban. LinkedIn, here, essentially seeks to prohibit hiQ from viewing a sign publicly visible to all.

1ER-15. The viewer in this analogy stands in a public space and views material that the shopkeeper has displayed to the public. It offends common ideas of trespass (and common sense) to think that by purporting to "revoke access," the shopkeeper could prevent passersby from opening their eyes. It is similarly offensive to think that having plugged its servers into the open Internet and configured them to respond automatically to requests for webpages, LinkedIn can, by sending a letter purporting to "revoke access," make a criminal of someone who types a URL into their own browser or clicks on a search result.[2]

LinkedIn's interpretation misreads the CFAA's authorization requirement, creates potential civil and criminal liability for all manner of innocent web browsing, and does nothing to further the statute's purpose, all while creating a host of constitutional problems. Section 1030(a)(2)(C)'s "authorization" requirement reaches only those users who access a computer for which authorization is required in the first place.

A. Access to Public Web Content Is Not "Without Authorization" Under the CFAA

The CFAA creates criminal and civil liability for any person who "intentionally accesses a computer without authorization … and thereby obtains …

[2] LinkedIn's counter-analogy of hiQ surreptitiously recording job fair attendees is off-base. Because members have expressly designated their information public, hiQ's access is expected, not surreptitious. Indeed, it is impossible for *anyone* to view a member's "public" profile without capturing (recording) a copy of it in their computer's random access memory.

information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Although the CFAA does not define "without authorization," this Court has held that it "is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission." *United States v. Nosal* ("*Nosal II*"), 844 F.3d 1024, 1028 (9th Cir. 2016).

The CFAA does not distinguish among various means of access (manual or automated), but rather whether the person accessing information has received the necessary authority to do so. *See United States v. Nosal* ("*Nosal I*"), 676 F.3d 854, 857-59 (9th Cir. 2012) (distinguishing between unauthorized access to and use of data). Accordingly, to understand whether a user acted without CFAA authorization, courts look to the granting authority and the scope of the permission. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009) (in employment context, "'authorization' depends on actions taken by the employer," from the grant of authorization, to access limits, to revocation of authorization); *Nosal II*, 844 F.3d at 1029 (employee who continued to access confidential information on company computers after company revoked his credentials acted "without authorization" under the CFAA).

LinkedIn does not grant permission to access its public content because those pages are, by definition, open for all to see and use. hiQ, like any other Internet user, simply requests LinkedIn's public pages, and LinkedIn's servers

automatically provide them. No one, including hiQ, needs "authorization" to access those pages, and LinkedIn does not check for "authorization" before providing them. There is no "authorization" for LinkedIn to revoke. Reading the statute in accordance with the language's ordinary significance, "without authorization" refers to circumstances where authorization is a prerequisite to access.

The district court credited the argument of leading CFAA scholar Professor Orin Kerr that "authorization" necessarily implies the existence of an "authentication requirement," or some other mechanism "to create the necessary barrier that divides open spaces from closed spaces on the Web." 1ER-14, citing Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1161 (2016). The court noted that this approach "would square with the results in both *Nosal II* and *Power Ventures*, [in which] the defendants had bypassed a password authentication system" to access "private data." 1ER-14, citing *Nosal II*, 844 F.3d 1024; *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. 3d 1058 (9th Cir. 2016). It would also square with the overwhelming weight of appellate authority applying the CFAA to password-protected or otherwise private computers.[3] Indeed, the

[3] *See, e.g.*, *Musacchio v. United States*, 136 S. Ct. 709, 713 (2016) (affirming CFAA conviction where former employees continued accessing former employer's computers using a password without permission); *Nosal II*, 844 F.3d at 1029 (affirming CFAA conviction where "former employee whose computer access credentials ha[d] been rescinded … disregarded the revocation, [and] accesse[d]

statute itself points to "passwords" in its *only* express example of the meaning of "without authorization." 18 U.S.C. §1030(a)(6).

Other federal statutory and regulatory schemes define "authorization" similarly. Under the Health Insurance Portability and Accountability Act ("HIPAA"), a health care provider "may not use or disclose protected health information without a [valid] authorization." 45 C.F.R. § 164.508(a)(1). Protected health information ("PHI") includes "individually identifiable information, including demographic information," that relates to the individual's "past, present, or future . . . health . . . and identifies the individual." *Id.* § 160.103. But publicly available demographic information does not qualify as PHI even if it meets the other requirements: "[i]dentifying information alone . . . would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI."[4] A health care provider would not need authorization (and a patient

---

the computer by other means"); *EF Cultural Travel BV v. Zefer Corp.* 318 F.3d 58, 64 (1st Cir. 2003) (affirming CFAA violation because even though the pages involved were putatively "public," the accessor, a former employee, violated an NDA by decoding secret and proprietary code portions based on confidential knowledge he obtained as an employee).

[4] Dep't of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (Nov. 6, 2015), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected.

could not revoke authorization) to disclose publicly available demographic information – even though the health care provider obtained the information from the patient and not from some other source.

B. The CFAA Does Not Provide For LinkedIn's Purported "Revocation of Authorization" to Access Public Pages

Contrary to LinkedIn's suggestion, this Court has never held or implied that a website owner has authority under the CFAA to revoke authorization that was never needed in the first place to selectively bar particular members of the public from accessing information readily accessible to anyone else in the world. 1ER-15. Further, nothing in the CFAA addresses when authorization can be "revoked"; neither the phrases "revocation of access," "revoke access," nor anything like them appear in the statute. Instead, courts have discussed authorization revocation in situations where someone who was originally granted access to *privately* stored information continued to access the information after leaving employment or otherwise being told to stop. *See supra* at 20-21 n. 3. Those cases thus stand merely for the proposition that when authorization is required to access a non-public computer, the owner may revoke authorization once granted.

In its *en banc* decision in *Nosal I*, this Court emphasized the CFAA's dual civil-criminal application and disavowed any construction that would "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime," 676 F. 3d at 859, or "allow[] private parties to

manipulate" their website policies "so as to turn these relationships [with internet users] into ones policed by the criminal law." *Id.* at 860. The Court was clear that prosecutorial discretion does not affect statutory construction: "[W]e shouldn't have to live at the mercy of our local prosecutor." *Id*. at 861. Instead, this Court applied the rule of lenity, opining that "'penal laws [must] be construed strictly,'" and rejected any interpretation that "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id*. at 857, 863 (internal quotation omitted). LinkedIn's interpretation goes even further by transforming routine access to public information into a federal crime at private website owners' discretion.

Nosal II and *Power Ventures* do not support LinkedIn because both cases involved unauthorized access to *private* computer spaces. In *Nosal II*, this Court held that a former employee accessed his former employer's private computers without authorization when he used current employees' credentials to access confidential information. 844 F.3d at 1028-29, 1038. Similarly, *Power Ventures* involved unauthorized entry into Facebook's password-protected zones. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1028 (N.D. Cal. 2012) ("undisputed fact" that Facebook users "register with a unique username and

password"), *rev'd in part*, 844 F.3d 1058.[5] At the same time, this Court *expressly reserved* the question presented here: whether the CFAA could apply to websites that are "open to all comers." 844 F.3d at 1067 n.2. ("[W]ebsites are the cyber-equivalent of an open public square in the physical world." (quoting Kerr, 116 Colum. L. Rev. at 1163).[6]

Craigslist, Inc. v. 3Taps, Inc., 964 F. Supp. 2d 1178 (N.D. Cal. 2013), is wrongly decided. It rested on the faulty premise that users are inherently "authorized" to view public content, and that owners of that content can revoke this general permission as to specific users. But neither the CFAA nor any other federal statute creates an authorization scheme for public web browsing, and the *3Taps* court erred by reading into the statute a requirement that is unsupported by the text and impracticable in the context of the modern Internet.[7]

---

[5] The cease-and-desist letter mattered in *Power Ventures* because the defendant could reasonably believe (notwithstanding contrary User Agreement language) that using another Facebook user's login credentials was "authorization" to satisfy the statute. Facebook's cease-and-desist letter clarified that using another user's credentials – like a former employee's use of a current employee's credentials – was not permitted. *Cf.* 18 U.S.C. § 1030(a)(6) (making it a crime, in defined circumstances, to "traffic[] . . . in any password . . . through which a computer may be accessed without authorization").

[6] LinkedIn's argument that this Court did not mention passwords in its *Power Ventures* decision is unavailing. The Court had no reason to make a distinction that was not at issue in that case and it is undisputed that the case involved access to password-protected pages. 844 F. Supp. 2d at 1028. The Court's holding cannot go beyond the actual facts and issues presented.

[7] Indeed, in an earlier ruling, the *3Taps* court acknowledged this problem:

C. Construing the CFAA to Criminalize Access To Public Webpages Would Cast Serious Doubt on Its Constitutionality

The CFAA was never meant to help a website owner to put a competitor out of business after copying its business model and latest product. But LinkedIn's CFAA interpretation goes well beyond shielding anti-competitive tactics, enabling any website owner to block disfavored individuals from viewing otherwise publicly-available content, suppressing the flow of information protected by the First Amendment. That power could be used to discriminate based on race or gender, to bar political rivals or journalists from campaign websites, or to prevent competitors or consumers from learning about products or pricing. 1ER-11-12. The district court's correct reading of the CFAA is thus reinforced by the doctrine of constitutional avoidance. *See Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is

---

> Applying the CFAA to publicly available website information presents uncomfortable possibilities. Any corporation could subject its competitors to civil and criminal liability for visiting its otherwise publicly available home page; in theory, a major news outlet could seek criminal charges against competing journalists for reading articles on its website.

Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 970 n.8 (N.D. Cal. 2013).

plainly contrary to the intent of Congress"); *see* 1ER-17 n.12 (acknowledging this argument but finding it unnecessary to rely on it).

1. LinkedIn's CFAA Interpretation Violates the First Amendment

According to LinkedIn, the CFAA authorizes it to prohibit hiQ from viewing information available to the public and gives that prohibition the force of law. If that were so, the CFAA as applied here would be unconstitutional. The government could no more enact such a statute than it could authorize someone delivering a speech on the sidewalk to select which passersby could pause to listen, or give a billboard owner to the power to decide who could read a message posted in plain view.

The First Amendment protects access to information as well as expressive activity. *See Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 756-57 (1976) ("[T]he protection afforded is to the communication, to its source and to its recipients both . . . . [T]his Court has referred to a First Amendment right to receive information and ideas, and that freedom of speech necessarily protects the right to receive.") (citations, internal quotation marks omitted). The First Amendment also protects the right to access the Internet generally and social media in particular, as the Supreme Court recently held in *Packingham v. North Carolina* when striking down a statute categorically banning sex offenders from social media. 137 S. Ct. 1730, 1735, 1737 (2017) (such websites, expressly

mentioning LinkedIn, "for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge"). Accordingly, the district court correctly concluded that "the act of viewing a publicly accessible website is likely protected by the First Amendment." *See* 1ER-0017, n.12.

Under LinkedIn's interpretation, the CFAA substantially burdens the right to access information on the Internet; indeed, it would prohibit hiQ from engaging in the protected activity of gathering publicly available information. Even the least problematic burdens on speech – time, place, and manner restrictions – "must be narrowly tailored to serve a significant governmental interest, and must leave open ample alternatives for communication." *Forsyth Cty., Ga. v. Nationalist Movement*, 505 U.S. 123, 130 (1992). If the CFAA authorizes LinkedIn to prohibit access to public information, that leaves no alternatives for communication; and the statute serves no significant governmental interest as applied in this instance.

It is no answer that LinkedIn is, itself, not a government body. The First Amendment prevents the government from enacting or enforcing laws prohibiting protected activity, even if a private party uses that law in a civil lawsuit to suppress speech. "[T]he need to encourage debate on public issues that concerned the Court in the governmental-restriction cases is of concern in a similar manner in this case

involving a private suit for damages." *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767, 777 (1986). Thus, the Supreme Court has repeatedly held that the First Amendment protects speech from government suppression at the behest of private parties in civil cases. *E.g.*, *New York Times Co. v. Sullivan*, 376 U.S. 254, 265 (1964) (defamation); *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 916 n.51 (1982) (malicious interference with business); *Philadelphia Newspapers, Inc.*, 475 U.S. at 777 (defamation); *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 630-32, 639-41 (1994) (cable statute that delegated to private broadcasters the power to demand carriage on a cable system); *Snyder v. Phelps*, 562 U.S. 443, 460 (2011) (intentional infliction of emotional distress).

Further, delegation of authority to a private party to prohibit protected activity is particularly problematic under the First Amendment when the party's discretion is unlimited. "A government regulation that allows arbitrary application" violates the First Amendment "because such discretion has the potential for becoming a means of suppressing a particular point of view." *Forsyth Cty., Ga. v. Nationalist Movement*, 505 U.S. 123, 130-31 (1992) (internal quotation marks omitted). That danger only increases when a private party with no public interest or political accountability has complete discretion to trigger legal sanctions.

LinkedIn would read the CFAA to confer on every website owner unfettered

discretion to ban anyone from reading that website. If it were not already evident that such selective censorship power would inevitably be abused, this case – in which LinkedIn seeks to prohibit hiQ's information-gathering for anticompetitive purposes – is a perfect example. Putting the power of state sanction behind LinkedIn's effort to prohibit hiQ from engaging in protected activity for no legitimate purpose would violate the First Amendment.

Contrary to LinkedIn's argument, it makes no difference whether hiQ accesses information using bots, as supposedly distinct from "living, breathing human[s]." Dkt. 6 at 58. The Supreme Court has never drawn arbitrary distinctions based on the technology used by speakers and listeners. *See Citizens United v. Fed. Election Comm'n.*, 558 U.S. 310, 326 (2010) ("declin[ing] to draw, and then redraw, constitutional lines based on the particular media or technology used"); *Brown v. Entm't Merchs. Ass'n*, 564 U.S. 786, 790 (2011)(citation omitted) ("'[T]he basic principles of freedom of speech and the press, like the First Amendment's command, do not vary' when a new and different medium for communication appears."). Indeed, the Supreme Court has *expressly* upheld data miners' First Amendment right to access large amounts of information for analytics: "Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011). And the Court has consistently recognized the right to use

technology to improve communication's effectiveness or efficiency. *See Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue*, 460 U.S. 575 (1983) (printing press); *FCC v. League of Women Voters*, 468 U.S. 364 (1984) (electromagnetic spectrum); *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622 (1994) (coaxial and fiber optic cables); *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (the Internet). LinkedIn cannot invoke the CFAA to suppress hiQ's protected activity, whether hiQ is manually reviewing public information or programming software to do so.

The issue here is not whether a private actor must allow individuals to join a private network. What matters is that LinkedIn and its members have chosen to make the information at issue available to anyone with a computer. The government may not give a private actor the power to block disfavored individuals from accessing information that is otherwise open for all to see.[8]

2. The CFAA's Dual Civil-Criminal Application Strengthens the Case for Constitutional Scrutiny

LinkedIn's CFAA interpretation also raises significant constitutional issues because it is both a civil and criminal statute. *See Nosal I*, 676 F.3d at 859-61. As

[8] This case likewise does not implicate the question whether there may be limits placed on a private actor's *use* of information obtained from the public Internet pursuant to generally applicable business tort law. (Duplicating another party's website, for example, might implicate copyright, unfair competition or Lanham Act concerns.) But LinkedIn has not claimed that hiQ's use of the information is tortious; it claims that hiQ violates federal (and state) law simply by accessing it.

the district court noted, "even if the First Amendment were not directly implicated" in a civil lawsuit, the "same interpretation of the statute would apply uniformly to both civil and criminal actions, . . . and a criminal prosecution under the CFAA would undoubtedly constitute state action." 1ER-17 n.12; *see Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (where a statute "has both criminal and noncriminal applications," courts should interpret the statute consistently in both contexts).

Under LinkedIn's view, a private party's attempts to block an individual's access to public pages would create the specter of criminal prosecution, essentially placing in private hands unbridled discretion to determine the scope of CFAA criminal liability. By itself, that possibility represents the kind of "credible threat of prosecution," *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2342 (2014) (internal quotation marks and citation omitted), that warrants judicial relief. In the First Amendment context, the risk of chilling protected activities (including by parties not before the court) means that "harm . . . can be realized even without an actual prosecution." *Virginia v. Am. Booksellers Ass'n*, 484 U.S. 383, 393 (1988). Even if LinkedIn never brought a civil suit to enforce the CFAA, its ability to define the boundaries of criminal conduct creates an additional First Amendment problem and a separate reason that the CFAA, under LinkedIn's interpretation, would be unconstitutional as applied.

As noted, a private party's use of government-sanctioned law to prohibit protected activity raises constitutional concerns even where the enforcement mechanism is limited to a private suit for damages. That problem is only compounded when the law gives a private party the power to determine what conduct is prohibited. In *Larkin v. Grendel's Den, Inc.*, 459 U.S. 116 (1982), the Supreme Court invalidated a statute allowing churches and schools to veto applications for liquor licenses for nearby businesses as an impermissible delegation of government authority to a private party. By the same token, LinkedIn's CFAA interpretation would delegate to website operators an effective veto enforced by the government. Here, invocation of that veto power would deny access to public information, rather than liquor licenses, making this an even stronger case for application of the principle at stake. Moreover, LinkedIn's asserted veto over First-Amendment-protected activity is absolute, standardless, and backed by criminal sanctions. Even if the CFAA's language could bear the meaning LinkedIn ascribes to it, this Court should avoid that interpretation given the serious constitutional problems it would create.

D. LinkedIn's CFAA Interpretation Contradicts the CFAA's Legislative History

The CFAA's legislative history confirms that its purpose has always been to protect private material, not to fence off public information. Congress passed the

CFAA in 1986 to address "computer crime" such as "hacking" or "trespass." H.R. Rep. No. 98-894, 1984 U.S.C.C.A.N. 3689, 3691-92, 3695-97 (1984) ("H. Rep. 98-894"); S. Rep. No. 99-432, 1986 U.S.C.C.A.N. 2479, 2480 (1986) ("S. Rep. 99-432"). The original "premise" of 18 U.S.C. § 1030(a)(2) was "privacy protections" and prohibiting unauthorized access to government-controlled "classified information." S. Rep. 99-432 at 2484; H. Rep. 98-894 at 3706-07. Congress reaffirmed this purpose by amending the CFAA in 1996 to fill in "significant gaps" in "privacy protection coverage." S. Rep. 104-357, 1996 WL 492169 (Leg. Hist.), at *4. The subsection at issue here (1030(a)(2)), was amended specifically to "increase protection for the *privacy and confidentiality* of computer information." *Id.*, at *7 (emphasis added). The CFAA's legislative history, including the 1996 amendments, shows its purpose has always been to protect private information.[9]

[9] The district court correctly recognized the CFAA's overlap with Cal. Penal Code § 502, concluding that hiQ raised serious questions regarding whether the Penal Code "criminalize[s] viewing public portions of a website." 1ER-17-18 n.13. The Penal Code's legislative history supports hiQ's position as well. It was amended in 2014 to introduce the concept of user "profiles," which it treats *differently* from "data," "computers," and "computer networks." Cal. Penal Code § 502(b)(15)(B). The statute was simultaneously amended to prohibit *only certain* use of such profiles: "knowingly and without permission" using someone else's profile to send "one or more electronic mail messages or posts and thereby damage[ing] or caus[ing] damage to a computer, computer data, computer system, or computer network." *Id*. § 502(c)(9). The amendment's prohibition of only email spamming activity related to profile pages corroborates that in its *original* form the statute did not apply to such pages.

E. Extending the CFAA to Restrict Access to Public Websites Violates the Federal Policy of an Open Internet

The CFAA's definition of "without authorization" must fit into the context of how the Internet – which was barely born when the CFAA was enacted – works. The CFAA is intended to prevent computer trespass. Any sensible concept of "trespass," whether oriented to the physical or digital world, must be premised on protection of a space that is somehow private. Public social media profiles are available to anyone with an Internet connection. An Internet user has no expectation of privacy in content affirmatively placed in public view on the Internet.[10] Accessing such pages purely to obtain information—in the absence of any injury or impairment to computer servers—should not create CFAA liability.[11]

---

[10] *See Pappas v. Naked Juice Co. of Glendora, Inc.*, No. CV-11-8276-JAK (PLAx), 2012 WL 12885109, at *4 (C.D. Cal. Dec. 5, 2012) ("online statements that are available to the public at large are not protected by the right to privacy.") (citing *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1130 (2009)); *Moreno*, 172 Cal. App. 4th at 1130 (affirmative act of posting on a "hugely popular internet site" made information "available to any person with a computer and thus opened it to the public eye"; "no reasonable person would have had an expectation of privacy regarding the published material"); *see* 2ER-220-21 n.1 for additional authority.

[11] *See, e.g., United States v. Gines-Perez*, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) ("A person who places information on the information superhighway clearly subjects said information to being accessed by every conceivable interested party."); *CollegeSource, Inc. v. AcademyOne, Inc.*, 597 F. App'x 116, 129 (3d Cir. 2015) (user did not act "without authorization" by accessing and redistributing "materials [that] were available without precondition to any member of the general public who clicked the link").

The type of access at issue here—automated data collection, or "scraping"—is ubiquitous and necessary to the functioning of the Internet, and nowhere does the CFAA prohibit it. Contrary to LinkedIn's characterization, automated data collection is not a form of hacking, but rather the use of "bots" to analyze the public web. "[A] 'bot' request is still ultimately a request from a person. It is merely an automated request, with the person who used the software still responsible." Kerr, 116 Colum. L. Rev. at 1170.

Numerous businesses, institutions and researchers engage in data scraping, and scraping software is openly sold by lawful businesses. It has been a standard web practice since Alta Vista and Excite in the mid-nineties, through Google and Bing (which, like LinkedIn, is owned by Microsoft), and the new breed of vertically-focused services, such as Intelius and DocketNavigator, today. Indeed, no search engine can work without scraping. Recognizing this, courts routinely uphold the work of so-called "scrapers" as fair use in the analogous realm of copyright. *See, e.g.*, *Authors Guild v. Google, Inc.*, 804 F.3d 202 (2d Cir. 2015) (accessing and copying books to create a "search function"—even without authorization—is a "transformative" fair use") (citation omitted); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1165 (9th Cir. 2007); *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 819 (9th Cir. 2003). LinkedIn here seeks to go even further by preventing access to data in which it has no copyright or other proprietary

interest and which resides on its website only because of its promise of non-exclusivity and public access.

Thus, the district court correctly found that members who opt for LinkedIn's public profile setting likely "expect their public profile will be subject to searches, data mining, aggregation, and analysis." 1ER-24. Criminalizing this practice would have serious implications for content owners and Internet users alike and make it impossible to harness and extract meaning from the information embedded in the Internet's billions of webpages.

LinkedIn argues in passing that its IP address limiters create a technical authentication requirement, so hiQ's circumvention of those measures gives rise to CFAA liability. But LinkedIn's attempt to block certain disfavored individuals does not make the public portion of its site – or the information on it – private. LinkedIn may have the technical wherewithal to disable hiQ's software, but it has not withdrawn the information in question from the public sphere.

Indeed, IP limiters do not create a private space for CFAA purposes, because they are typically designed to regulate the *rate* of access. They are like speedbumps or metering lights, not police barricades. Kerr, 116 Colum. L. Rev. at 1167-69; *Power Ventures*, 844 F.3d at 1063. Even if LinkedIn completely blocked

hiQ's IP addresses, this would not prevent anyone else from accessing the site.[12] Even as to a particular IP address, service providers like Comcast and Amazon Web Services lease out rotating IP addresses, and the use of diverse and ever-changing IP addresses is standard. In this context, any "IP block" is more gap than block. *See Power Ventures*, 844 F.3d at 1068 n.5.[13] The measures LinkedIn claims hiQ "circumvented" are not actually "barriers" to access.

LinkedIn asks this Court to interpret its rate-limiting measures and cease-and-desist letter as reflecting LinkedIn's *intent* to block hiQ. But the CFAA is designed to prevent actual security breaches like the misuse of passwords, not transform a company's business decisions into criminal liability. *See Nosal I*, 676 F.3d at 860. LinkedIn has no authentication requirement in place for restricting access to its public webpages. Without one, it cannot invoke the CFAA to prevent hiQ from viewing public content.[14]

---

[12] LinkedIn also complains that hiQ evades IP blocks by maintaining "anonymity." LinkedIn's point is unclear, because accessing public profiles does not require a membership sign-in. Robots.txt is also not a barrier to accessing a computer, because that protocol *depends* on access to a file entitled "robots.txt" on a host computer: one must access the computer to practice the protocol, so it is no barrier per the CFAA.

[13] The district court found that LinkedIn's use of hiQ-specific blocks raised serious questions of an unlawful anti-competitive practice. *See* Section II, *infra*. Certainly any unlawful blocks cannot justify LinkedIn's CFAA claim.

[14] Nothing in the district court's order requires LinkedIn to disable its general security or anti-hacking measures and LinkedIn cannot credibly claim it has done so. And as the court noted, LinkedIn has technical and legal recourse against

F. Even If the CFAA Applies to Public Websites, It Does Not Pre-empt hiQ's State Law Claims

Even if the CFAA could apply to public pages, it would not, as LinkedIn argues, pre-empt hiQ's state-law claims. Federal courts "have long presumed that Congress does not cavalierly pre-empt state-law causes of action," and must "start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress." *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996) (internal quotation marks omitted). Nothing – let alone "clear and manifest" language – suggests that Congress intended the CFAA to displace all other law, including state unfair competition and tort law.

Without any express or implied conflict between federal and state law, preemption under the Supremacy Clause does not into come into play. *See, e.g.*, Laurence Tribe, American Constitutional Law (3d ed. 2000), §§ 6-28 through 6-31, pp. 1172-1212. "The [CFAA] was . . . designed to target hackers who accessed

---

actual nefarious actors. *See* 1ER-16 ("Finding the CFAA inapplicable to hiQ's actions does not remove all arrows from LinkedIn's legal quiver against malicious attacks."), n.11 (collecting authority). *See also* 18 U.S.C. § 1030(a)(5), (8) (protecting computers from unauthorized "damage" broadly defined to include "impairment"); 17 U.S.C. § 103 (protecting copyrights in a compilation); 17 U.S.C. § 1201 (prohibiting "circumvention of technical measures" to obtain copyrighted material); Cal. Bus. & Prof. Code § 17200 (protecting against actual free-riders); *eBay, Inc. v. Bidder's Edge*, 100 F Supp. 2d 1058, 1069-72 (N.D. Cal. 2000) (trespass to chattels doctrine protects against computer damage). LinkedIn has not argued that it has a claim under *any* of these sundry theories.

computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives.'" *LVRC Holdings*, 581 F.3d at 1130-31. This purpose does not conflict with unfair competition law or common law governing interference with contract or economic advantage.

Indeed, the CFAA's prohibition on access "without authorization" can readily co-exist with generally-applicable state laws that may preclude a website owner from unlawfully blocking access to public web pages. *See Florida Lime & Avocado Growers, Inc. v. Paul*, 373 U.S. 132, 142 (1963) ("federal regulation of a field of commerce should not be deemed preemptive of state regulatory power in the absence of persuasive reasons – either that the nature of the regulated subject matter permits no other conclusion, or that the Congress has unmistakably so ordained"). Even if the CFAA applied to public pages and LinkedIn could selectively "withdraw" authorization from certain members of the public, nothing immunizes LinkedIn from liability if, in doing so, it violated state law.

II. HIQ HAS RAISED SERIOUS QUESTIONS AND IS LIKELY TO SUCCEED ON ITS STATE LAW CLAIMS

The district court correctly held that hiQ made a sufficient showing on its state-law claims to support preliminary relief. LinkedIn knew that hiQ was building its people-analytics business – and entering into contractual relationships

– based on LinkedIn public profile data, and for years it did not object. LinkedIn's effort to destroy hiQ's business by affirmatively interfering with hiQ's use of public data – to clear the field for LinkedIn's own competing offering – runs afoul of the UCL, because, at minimum, it violates the spirit of the antitrust laws or otherwise harms competition. *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 186 (1999). That conduct likewise constitutes tortious interference with hiQ's customer contracts.

LinkedIn's primary defense to these claims – that hiQ's use of public data violates the CFAA – is incorrect for the reasons explained above. LinkedIn's arguments that hiQ's UCL claims depend on market definition and market power allegations sufficient to sustain a Sherman Act claim or that those claims run afoul of limitations on affirmative duties to deal under the Sherman Act likewise fail for two basic reasons. *First*, hiQ's claim is under the UCL – not the Sherman Act – and no formal market definition or market power allegations are required. *Second*, hiQ seeks to impose no affirmative duty to deal, but instead to prevent LinkedIn's interference with hiQ's lawful, legitimate, and pro-competitive activities. LinkedIn's reliance on its terms of service to stop anyone from copying or using public profile information demonstrates LinkedIn's intent to target not just hiQ but any potential competitor. This impacts competition generally, not just hiQ. Given

the breadth of the UCL, hiQ's showing is sufficient to support its claim at this preliminary, pre-discovery stage.

Furthermore, hiQ's tortious interference claim is independently sufficient to support injunctive relief. LinkedIn does not (and cannot) contest that hiQ established every element of a tortious interference with contract claim. It claims to have a legitimate business reason to prevent certain uses of its members' public information, but the district court rejected that argument as a factual matter. LinkedIn does not seriously argue that its challenge to that finding can satisfy the applicable demanding standard of review.

A. LinkedIn's Conduct Falls Within the UCL's Broad Scope

1. Affirmative Interference With a Rival's Efforts To Provide Competing Services Implicates the UCL

The district court properly found that hiQ raised serious questions regarding whether LinkedIn's conduct runs afoul of the UCL, which bars "any unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. LinkedIn's efforts to interfere with hiQ's legitimate business activities harm competition by eliminating a rival without any pro-competitive justification. The UCL captures a wide variety of unfair and anticompetitive practices: "the section was intentionally framed in its broad, sweeping language, precisely to enable judicial tribunals to deal with the 'innumerable new schemes which the fertility of

man's invention would contrive.'" *Barquis v. Merchs. Collection Ass'n*, 7 Cal. 3d 94, 112 (1972) (citation omitted).

LinkedIn's conduct is "unfair" within the UCL's meaning because of its anticompetitive impact. The UCL's "unfair" prong is broad, covering:

> conduct that 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, 20 Cal. 4th at 187 (emphasis added). The California Supreme Court's use of the disjunctive "or" means that each theory is a distinct alternative. *PeopleBrowsr, Inc. v. Twitter, Inc.*, No. C-12-6120 EMC, 2013 WL 843032, at *4 (N.D. Cal. Mar. 6, 2013). Although LinkedIn had long been aware that hiQ was analyzing LinkedIn users' public profiles, *see* 5ER-989-90, only when it became apparent that LinkedIn's new product would compete with hiQ's did LinkedIn attempt to prevent hiQ from accessing information which is available to any other member of the public.

The district court properly inferred – a fact-finding that is entitled to deference – that, rather than compete with hiQ on the merits, LinkedIn took affirmative steps to eliminate a competitor. *See* 1ER-23 ("hiQ has presented some evidence supporting its assertion that LinkedIn's decision to revoke hiQ's access to its data was made for the purpose of eliminating hiQ as a competitor in the data analytics field."). LinkedIn's attempt to minimize competition by interfering with

a competitor's independent efforts to utilize public information violates the spirit of the antitrust laws, which seek to promote competition on the merits. *See Allied Orthopedic Appliances Inc. v. Tyco Health Care Grp. LP*, 592 F.3d 991, 1000 (9th Cir. 2010) ("[T]he very purpose of the antitrust laws . . . [is] to foster and ensure competition on the merits.") (internal quotation marks omitted); *Clayworth v. Pfizer, Inc.*, 49 Cal. 4th 758, 783 (2010) ("[T]he Cartwright Act has always been focused on the punishment of violators for the larger purpose of promoting free competition"). This conduct likewise harms competition by immediately decreasing industry output, eliminating a viable competitor, and increasing the likelihood that LinkedIn will dominate the market. *See, e.g., Broad. Music, Inc. v. Columbia Broad. Sys., Inc.*, 441 U.S. 1, 19-20 (1979) (condemning practices that "threaten the proper operation of our predominantly free-market economy" because they "tend to restrict competition and decrease output").

To be sure, the UCL is not intended to reach vigorous competition that may place rivals at a disadvantage: while such conduct may cause "[i]njury to a competitor" it does not constitute "injury to competition." *Cel-Tech*, 20 Cal. 4th at 186. But in this case, LinkedIn seeks to drive hiQ from the market not by offering a superior service, but by blocking hiQ's independent competitive efforts. Such conduct harms competition and is appropriately addressed under the UCL. Although hiQ does not assert an antitrust claim, eliminating one competitor at a

time can constitute harm to competition under California law even for purposes of an antitrust violation. *Flagship Theaters of Palm Desert, LLC v. Century Theaters, Inc.*, 198 Cal. App. 4th 1366, 1379-80 (2011) (citation omitted). While there has been no discovery at this early stage, nothing suggests that LinkedIn's actions are solely aimed at hiQ. LinkedIn claims its terms of service justify blocking anyone who copies public profile information and readily admits it is pursuing others besides hiQ. Dkt. 6 at 18-19. Its concession to the district court that it would permit manual copying (not commercially feasible, but which would similarly impact any supposed privacy concerns) further evidences an effort to harm competition generally. 3ER-500:15-21 ("We're talking about access through automated bots and scraping technologies. … It's not about manual copying.").[15]

2. hiQ's UCL Claim Requires No Showing of Market Power

LinkedIn's assertion that hiQ's UCL claim should fail because hiQ has not established a Sherman Act violation (15 U.S.C. § 2) ignores the differences between the two statutes. Each of the UCL's three prongs – unlawful, unfair, and

[15] Contrary to LinkedIn's suggestion, there is no meaningful difference between an employer reading each employee's profile (one at a time) and hiQ's reading each employee's profile (also one at a time but more quickly with automation) and providing analysis to the employer. If hiQ hired thousands of employees to manually read and copy public data, the implications for LinkedIn's supposed privacy justifications would be the same. LinkedIn obviously seeks to make use of the data commercially unfeasible for anyone but LinkedIn. LinkedIn has never provided a persuasive reason for this differentiation or any basis to conclude that automated reading of public profiles causes the platform any harm.

fraudulent – "is a separate and distinct theory of liability." *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). The "unlawful" prong covers practices violating "[v]irtually any state, federal, or local law," *Friedman v. AARP, Inc.*, 855 F.3d 1047, 1052 (9th Cir. 2017), including state and federal antitrust laws, *see, e.g.*, *Catch Curve, Inc. v. Venali, Inc.*, 519 F. Supp. 2d 1028, 1040 (C.D. Cal. 2007); *Sunbelt Television, Inc. v. Jones Intercable, Inc.*, 795 F. Supp. 333, 338 (C.D. Cal. 1992). By contrast, the "unfair" prong of the UCL reaches conduct that is *not otherwise unlawful*; it prohibits practices that are "deemed unfair even if not specifically proscribed by some other law." *Cel-Tech*, 20 Cal. 4th at 180. "Even absent a violation of law, a plaintiff may prevail on a UCL claim if the defendant engaged in unfair practices." *EchoStar Satellite Corp. v. NDS Grp. PLC*, No. SACV-03-0950DOCJTLX, 2008 WL 4596644, at *5 (C.D. Cal. Oct. 15, 2008). To require hiQ to prove every element of a § 2 claim would read "unfair" out of the statute and contradict *Cel-Tech*.

Thus, LinkedIn's argument that hiQ failed to allege a distinct antitrust market or establish monopoly power in such a market attacks a straw man; hiQ's UCL claim requires no such showing and LinkedIn cites no authority for that proposition. It cites *Cel-Tech*, which stands for the opposite proposition: conduct that might *not* violate the antitrust laws may *nevertheless* be "unfair" under the UCL because it prevents independent competition.

The *Cel-Tech* plaintiff alleged that the defendant – one of two wireless service providers in Los Angeles – sold wireless phones below cost, thereby foreclosing competition by independent equipment vendors. 20 Cal. 4th at 169. In holding that these allegations created a triable issue under the UCL, the court did not require the plaintiff to establish a Sherman Act predatory pricing claim – it hardly referred to Sherman Act standards at all. Furthermore, because there were vigorous competitors in the wireless service market, there was no risk of the defendant gaining a monopoly or recouping losses from below-cost sales by charging monopoly prices later. *Cf. Brooke Grp. Ltd. v. Brown & Williamson Tobacco Corp.*, 509 U.S. 209, 224 (1993). The court nevertheless recognized that the conduct could violate the UCL precisely because the UCL "does more than just borrow" from other sources of law – it imposes liability for unfair practices that threaten competition.

LinkedIn cites no case – from any court, state or federal – dismissing an unfair competition claim for failure to define a relevant market or to demonstrate sufficient power in the market.[16] By contrast, the district court here correctly

[16] LinkedIn relies on two cases dismissing UCL claims under the "unfair" prong, but in those cases the plaintiffs lacked "any allegations" that the defendants' "conduct threatens harm to competition." *Oracle Am., Inc. v. Hewlett Packard Enter. Co.*, No. 16-CV-01393-JST, 2016 WL 3951653, at *8 (N.D. Cal. July 22, 2016); *see Total Recall Techs. v. Luckey*, No. C 15-02281 WHA, 2016 WL 1070656, at *5 (N.D. Cal. Mar. 18, 2016) ("If anything, [defendant's] conduct helped competition by bringing a new competitor into the market."). Here, the

found that "LinkedIn enjoys a position as the dominant power in the market of professional networking," and that it seeks to "'leverage all this extraordinary data [it's] been able to collect by virtue of having 500 million people join the site'" to foreclose competitors like hiQ. 1ER-22. Whether 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.

3. hiQ Seeks To Impose No Affirmative Duty To Deal

LinkedIn's argument that hiQ's claim violates the principle that even a monopolist has no duty to deal with a would-be competitor fails because hiQ seeks to impose no such duty. Notably, this argument is an about-face from its argument in the district court that hiQ's unfair competition claim was a "total red herring," further supporting the inference that LinkedIn's privacy justifications were always pretext. 3ER-464:8-9. But more fundamentally, hiQ seeks to use information belonging to LinkedIn's members – not to LinkedIn – that members have chosen to make publicly available to anyone who chooses to view it over the Internet. LinkedIn admits it has taken affirmative "technical and legal measures" to block

---

threatened harm to competition is clear; LinkedIn seeks to decrease industry output by eliminating a competitor, not bring a new competitor into the market. Nor was failure to define a market determinative in the cases LinkedIn cites, *Creative Mobile Techs., LLC v. Flywheel Software, Inc.*, No. 16-CV-02560-SI, 2017 WL 679496 (N.D. Cal. Feb. 21, 2017), and *Synopsis, Inc. v. ATopTech, Inc.*, No. C 13-2965 MMC, 2015 WL 4719048 (N.D. Cal. Aug. 7, 2015).

hiQ's use of that data. Dkt. 6 at 16. hiQ does not want to deal with LinkedIn – it wants LinkedIn to stop trying to destroy it.

Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398 (2004), bears no resemblance to this case. There, the Supreme Court held that, though an incumbent telephone company may have regulatory duties to share certain elements of its telephone network with competing phone companies, it has no antitrust duty to do so. 540 U.S. at 410-12. The Court invoked the century-old case of *United States v. Colgate & Co.*, 250 U.S. 300 (1919), which upheld the right of a "trader or manufacturer engaged in an entirely private business, freely to exercise his own independent discretion as to parties with whom he will deal." *Id.* at 307.

Trinko explains that a monopolist does not have to provide "services . . . not otherwise marketed or available to the public," and products that were "offered not to consumers but to rivals, and at considerable expense and effort." 540 U.S. at 410. A defendant's failure to adequately "design and implement" a new system cannot support a claim because there is no antitrust duty to design and implement new systems for a competitor's benefit. *Id.* The Court also reaffirmed that in some cases, a monopolist could be required to sell to a competitor, as in *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 601 (1985). In that case, the defendant withdrew from its previous cooperative venture and refused to sell its

products to its competitor even on the same terms upon which its products were available to the general public, an "unwillingness" that "revealed a distinctly anticompetitive bent." *Trinko*, 540 U.S. at 409. Under those circumstances, § 2 liability was appropriate.

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. hiQ asked nothing of LinkedIn; certainly, hiQ is not asking LinkedIn to "design[] and implement[]" "[n]ew systems." *Id.* at 410. On the contrary, it is LinkedIn that designed and implemented new technological blocks specifically to put hiQ out of business by limiting its ability to view public profiles on the same terms as other members of the public (including commercial services like Google and Bing that use automation). *E.g.*, 4ER-599. Nothing suggests such conduct is privileged.

This case is also unlike *Trinko* and *Aspen Skiing* (and other duty-to-deal cases, such as *Pacific Bell Telephone Co. v. Linkline Communications, Inc.*, 555 U.S. 438 (2009)) because the information for which LinkedIn has blocked hiQ's access is not only publicly accessible, but does not belong to LinkedIn in the first place. LinkedIn only obtained the data on it servers by promising members that LinkedIn's use would be non-exclusive and that LinkedIn would honor member choices about who can access their content. Members chose to make the data at issue public, accessible to *everyone* including non-LinkedIn members who access

the site through search engines. Along with employers and other commercial enterprises, hiQ is a member of that public. LinkedIn seeks improperly to selectively wall off for its own purposes who can view the information and how they can use it.[17]

To the extent an analogy to federal antitrust law is helpful, LinkedIn's actions are best compared not to a refusal to deal, but to vertical restraints imposed by a seller with substantial market power requiring buyers (here, members) not to deal with a competitor. Vertical exclusivity requirements, though not *per se* illegal, may violate both state and federal antitrust law when imposed by a dominant actor like LinkedIn. *See, e.g.*, *Clear Connection Corp. v. Comcast Cable Commc'ns Mgmt., LLC*, 149 F. Supp. 3d 1188, 1197 (E.D. Cal. 2015); *ZF Meritor, LLC v. Eaton Corp.*, 696 F.3d 254, 270 (3d Cir. 2012) ("[D]e facto exclusive dealing claims are cognizable under the antitrust laws."). And "an aggregation of multiple exclusive agreements" can violate § 2 of the Sherman Act if used "to

[17] This distinguishes this case from *Authenticom, Inc. v. CDK Global, LLC*, No. 17-2540, 2541, 2017 WL 5112979, at *5 (7th Cir. Nov. 6, 2017). In that case, the court reversed an injunction – although it did not disturb the district court's finding that the requirements for a preliminary injunction were satisfied – because the injunction required the defendants to grant Authenticom access to non-public databases and data not available to the public. Accordingly, the court found, the injunction required the "defendants to enter into an entirely new arrangement with Authenticom" which "forc[ed] them to do business with Authenticom on terms to which they did not agree." Whatever the merits of the court's reasoning in that case, it has no application here.

choke off competition in a way that is not legally sanctioned." *Pecover v. Elecs. Arts Inc.*, 633 F. Supp. 2d 976, 984 (N.D. Cal. 2009); *see also, e.g.*, *United States v. Microsoft Corp.*, 253 F.3d 34, 71 (D.C. Cir. 2001) (aggregated exclusive deals violated § 2).

The platform and technology are new, but LinkedIn preventing members from making profile information available to its competitors is like a newspaper's requirement that its advertisers not do business with the local radio station, with the aim of driving the station out of business. *See Lorain Journal Co. v. United States*, 342 U.S. 143, 152 (1951) (finding attempted monopolization in violation of § 2). The fact that LinkedIn is imposing its exclusivity requirement on members without their consent makes its conduct even more anticompetitive. Even if LinkedIn may "refuse to deal" with whomever it wants, it cannot require that *members* refuse to provide their data to its competitors.[18]

[18] Antitrust commentators have already warned that efforts to monopolize consumer data will be the new battleground of antitrust law. *See* 3ER-418-423. These very concerns were also raised when Microsoft proposed to acquire LinkedIn. *See* April Glaser, "Marc Benioff Says Companies Buy Each Other For the Data, and the Government Isn't Doing Anything About It," https://www.recode.net/2016/11/15/13631938/benioff-salesforce-data-government-federal-trade-commission-ftc-linkedin-microsoft (accessed Nov. 17, 2017). That the scheme is new and without much precedent does not remove it from the UCL's ambit; to the contrary, it is precisely the type of "new scheme[] which the fertility of man's invention would contrive" that the UCL was designed to address. *Barquis*, 7 Cal. 3d at 112.

B. hiQ's Tortious Interference Claim Independently Justifies Injunctive Relief

As with the UCL claim, the district court found that hiQ's tortious interference claim supports preliminary relief if, as the record supports, "LinkedIn acted for an improper anticompetitive purpose" rather than "out of legitimate concern for member privacy." 1ER-23 n. 14. hiQ's tortious interference claim thus provides an independent basis for affirmance.

1. hiQ is Likely to Succeed on its Tortious Interference Claim

hiQ has established the requisite likelihood of success on the merits of its claim for tortious interference with contract. The elements of the tort are:

> (1) a valid contract between plaintiff and a third party; (2) defendant's knowledge of this contract; (3) defendant's intentional acts designed to induce a breach or disruption of the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5) resulting damage.

Pac. Gas & Elec. Co. v. Bear Stearns & Co., 50 Cal. 3d 1118, 1126 (1990). Unlike proving tortious interference with prospective economic advantage, "it is not necessary that the defendant's conduct be wrongful apart from the interference with the contract itself."[19] *Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal. 4th

[19] hiQ is also likely to succeed on its separate claim for tortious interference with prospective economic advantage. hiQ established the elements of a tortious interference with contract claim, and LinkedIn's UCL violation satisfies the additional element of an independently wrongful act. *CRST Van Expedited, Inc. v. Werner Enters., Inc.*, 479 F.3d 1099, 1110 (9th Cir. 2007); *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1158 (2003).

26, 55 (1998) (citation omitted), *as modified* (Sept. 23, 1998). The torts are "distinct, and California law 'draw[s] and enforce[s] a sharpened distinction' between the two." *United Nat. Maint., Inc. v. San Diego Convention Ctr., Inc.*, 766 F.3d 1002, 1007 (9th Cir. 2014) (quoting *Della Penna v. Toyota Motor Sales, U.S.A., Inc.*, 11 Cal. 4th 376, 392 (1995)). Further, although the plaintiff must prove the defendant's knowledge of the contract and an "intentional" act, the tort "does not require that the actor's primary purpose be disruption of the contract." *Quelimane Co.*, 19 Cal. 4th at 56.

There is no dispute that every element of the claim is present here. *See* Dkt. 6 at 32 (contesting hiQ's tortious interference claim solely on the basis of alleged affirmative defenses). LinkedIn has known of hiQ's customer contracts since at least 2015, when LinkedIn began participating in hiQ's Elevate conference. 5ER-989. LinkedIn's decision to cut off hiQ's access to public profiles was intentional, and LinkedIn knew that it would disrupt hiQ's existing contracts because hiQ's business model relies on that access. 5ER-991. If there was any doubt, hiQ informed LinkedIn, in its May 31, 2017 letter, that LinkedIn's conduct would cause "millions of dollars' worth" of damage to hiQ, including by disrupting hiQ's current contracts with customers like eBay, Capital One, and GoDaddy. 5ER-926 n.1. Nevertheless, with full awareness of the likely consequences, LinkedIn has

made clear that, unless the preliminary injunction is left in place, it will block hiQ's access to public profiles and disrupt hiQ's contractual relationships.[20]

2. LinkedIn Has Not Established the "Legitimate Business Purpose" Affirmative Defense

LinkedIn's argument that "it acted with 'legitimate business purpose[s],'" (quoting *Quelimane*, 19 Cal. 4th at 57) fails because the district court made contrary factual findings that are supported by evidence. LinkedIn identifies the following justifications: "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. . . ." Dkt. 6 at 43-44.

First, it is LinkedIn's burden to "establish that it had a legitimate business purpose which justified its actions," which is generally "a matter for trial." *Quelimane Co.*, 19 Cal. 4th at 57. A legitimate business purpose is an "affirmative defense" that "depends upon a balancing of the importance, social and private, of the objective advanced by the interference against the importance of the interest interfered with, considering all circumstances including the nature of the actor's conduct and the relationship between the parties." *Herron v. State Farm Mut. Ins. Co.*, 56 Cal. 2d 202, 206 (1961) (citation omitted). LinkedIn cannot meet its

[20] LinkedIn argues that hiQ cannot sustain a tortious interference claim because its contracts are "'tainted with illegality,'" by which LinkedIn means hiQ's purported violations of the CFAA. As explained, hiQ's access to public information on the Internet does not violate the CFAA, so this affirmative defense is unavailing.

burden to show that its affirmative defense is so plainly meritorious that there can be no serious question about hiQ's tortious interference claim.

On the contrary, as the district court found, LinkedIn's supposed concerns about member privacy and its User Agreement's prohibition on automated data collection appear pretextual. LinkedIn's advertisement for its "Recruiter" product "seems to afford little deference to the very privacy concerns it professes to be protecting in this case" – it allows recruiters to pay for secret access not only to LinkedIn users' *public* data, but also to their *private* data. 1ER-7. And LinkedIn has argued to a different Northern District judge that its users have no privacy interest in information that they "chose to make public." 3ER-320. As for the User Agreement, the district court found that LinkedIn had terminated hiQ's status as a LinkedIn member, and that hiQ's access to public profiles is unrelated to hiQ's own use of LinkedIn under the User Agreement. 1ER-7 n.4. Further, as LinkedIn has admitted, other commercial enterprises are permitted to use automated software to access the LinkedIn site. 5ER-882 ¶ 4.

LinkedIn's concern about the value of its investment does not provide a justification for its tortious conduct, because "a competitor's stake in advancing his own economic interest will not justify the intentional inducement of a contract breach." *Envtl. Planning & Info. Council v. Super. Ct.*, 36 Cal. 3d 188, 194

(1984). That LinkedIn believed it advantageous to disrupt hiQ's contractual relationships is no defense at all.

Lastly, LinkedIn offers the defense that it is "asserting its rights under federal and state law." But an assertion of rights is not a "business purpose" in itself, *Quelimane Co.*, 19 Cal. 4th at 56, and no socially valuable "objective" is being "advanced" by LinkedIn's sudden decision to assert its purported rights, *Herron*, 56 Cal.2d at 206; *see also Los Angeles Airways, Inc. v. Davis*, 687 F.2d 321, 325 (9th Cir. 1982) ("The existence and scope of the privilege to induce a breach of contract must be determined by reference to the societal interests which it is designed to protect"). Nor does LinkedIn provide any legal support for the argument that asserting legal rights immunizes an otherwise unlawful interference with a contract from liability.

The district court's factual findings were not clearly erroroneous, and its determination that hiQ had raised serious questions about whether LinkedIn had any legitimate business purpose to interfere with hiQ's contracts was no abuse of discretion.

III. THE DISTRICT COURT DID NOT ABUSE ITS DISCRETION IN RULING THAT THE EQUITIES TIP SHARPLY IN HIQ'S FAVOR

LinkedIn cannot seriously dispute the district court's findings that hiQ established irreparable harm, that the balance of the hardships favors hiQ, or that the public interest also weighs strongly in hiQ's favor.

A. hiQ Would Face Irreparable Harm Absent Relief

The district court did not abuse its discretion in finding that hiQ would suffer irreparable harm absent a preliminary injunction. Relying on the "undisputed fact that hiQ's entire business depends on its access to LinkedIn's public profile data," the court found credible hiQ's assertions that it would go out of business absent injunctive relief. 1ER-4. These factual findings are supported by the declaration of hiQ's CEO, Mark Weidick (*id.*; 5ER-0991). *See Disney Enters., Inc. v. VidAngel, Inc.*, 869 F.3d 848, 865-66 (9th Cir. 2017) (no abuse of discretion in finding irreparable harm based on uncontroverted declaration from company's senior vice president).

Further, the court cited Ninth Circuit and Supreme Court precedent holding that the threat of being driven out of business, a substantial loss of business, and loss of customers or goodwill establish irreparable harm. 1ER-5. It logically rejected LinkedIn's argument that hiQ should come up with a new business model or use data from other websites, because this would be "comparable to simply going out of business" and under LinkedIn's legal interpretation, nothing would stop other platforms "from barring hiQ in the same way LinkedIn has." *Id.* at n.1.

B. The Balance of Hardships Favors hiQ

The court did not abuse its discretion in finding that the balance of hardships favors hiQ given that LinkedIn had "presented no evidence of harm, financial or

otherwise resulting from hiQ's activities." 1ER-8. Unable to show any direct economic harm, LinkedIn argued that its members' privacy interests were harmed by hiQ's actions, asserting falsely – with no record support – that hiQ alerts employers to changes in member profiles. The court discounted these arguments for the reasons cited above and properly concluded that LinkedIn's claims of injury were "uncertain at best." 1ER-7.

C. The Public Interest Favors hiQ

The district court did not abuse its discretion in holding that the public interest favored hiQ. The court logically noted that while LinkedIn's privacy arguments were "at best uncertain," adopting LinkedIn's position could pose an "ominous threat to public discourse and the free flow of information." 1ER-0024. The district court thus permissibly concluded, at least for purposes of preliminary relief, that hiQ's position was most consistent with the public interest in the free flow of ideas. And given that both hiQ and LinkedIn agree that these issues are important to the future of the Internet, it is in the public interest to have them carefully vetted on a developed record and not decided by default because LinkedIn is able to destroy hiQ before the merits can even be considered.

CONCLUSION

The Court should affirm the district court's grant of preliminary injunctive relief on both the CFAA declaratory judgment claims and the state-law affirmative relief claims.

Dated: November 20, 2017

FARELLA BRAUN + MARTEL LLP

By: */s/ C. Brandon Wisoff*

C. Brandon Wisoff
Deepak Gupta
Jeffrey G. Lau
Rebecca H. Stephens
235 Montgomery Street, 17th Floor
San Francisco, California 94104
Telephone: (415) 954-4400
Facsimile: (415) 954-4480

KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, PLLC
Aaron M. Panner
Gregory G. Rapawy
T. Dietrich Hill
1615 M Street, N.W.
Suite 400
Washington, DC 20036
Telephone: (202) 326-7900
Facsimile: (202) 326-7999

Laurence H. Tribe*
Carl M. Loeb University Professor and
Professor of Constitutional Law
Harvard Law School
1575 Massachusetts Avenue
Cambridge, Massachusetts 02138
(617) 495-1767
**Affiliation noted for identification purposes only*

Attorneys for Plaintiff-Appellee hiQ Labs, Inc.

STATEMENT OF RELATED CASES

hiQ is not aware of any related cases pursuant to Ninth Circuit Rule 28-2.6.

CERTIFICATE OF COMPLIANCE

I certify pursuant to Federal Rule of Appellate Procedure 32 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 13,985 words.

Dated: November 20, 2017 FARELLA BRAUN + MARTEL LLP

By: */s/ C. Brandon Wisoff*

C. Brandon Wisoff
Deepak Gupta
Jeffrey G. Lau
Rebecca H. Stephens
235 Montgomery Street, 17th Floor
San Francisco, California 94104
Telephone: (415) 954-4400
Facsimile: (415) 954-4480

STATUTORY ADDENDUM

Except for the following, all applicable statutes are contained in the brief or addendum of Defendant-Appellant LinkedIn Corporation.

Cal. Penal Code § 502

§ 502. Unauthorized access to computers, computer systems and computer data

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

> **(1)** "Access" means to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.
>
> **(2)** "Computer network" means any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities.
>
> **(3)** "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form,

cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, Internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Government computer system" means any computer system, or part thereof, that is owned, operated, or used by any federal, state, or local governmental entity.

(7) "Public safety infrastructure computer system" means any computer system, or part thereof, that is necessary for the health and safety of the public including computer systems owned, operated, or used by drinking water and wastewater treatment facilities, hospitals, emergency service providers, telecommunication companies, and gas and electric utility companies.

(8) "Data" means a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(9) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(10) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.

(11) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(12) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(13) "Internet domain name" means a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(14) "Electronic mail" means an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable of receiving electronic messages, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval.

(15) "Profile" means either of the following:

(A) A configuration of user data required by a computer so that the user may access programs or services and have the desired functionality on that computer.

(B) An Internet Web site user's personal page or section of a page that is made up of data, in text or graphical form, that displays significant, unique, or identifying information, including, but not limited to, listing acquaintances, interests, associations, activities, or personal statements.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network.

(10) Knowingly and without permission disrupts or causes the disruption of government computer services or denies or causes the denial of government

computer services to an authorized user of a government computer, computer system, or computer network.

(11) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.

(12) Knowingly and without permission disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network.

(13) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section.

(14) Knowingly introduces any computer contaminant into any public safety infrastructure computer system computer, computer system, or computer network.

(d)(1) Any person who violates any of the provisions of paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision (c) is guilty of a felony, punishable by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years and a fine not exceeding ten thousand dollars ($10,000), or a misdemeanor, punishable by imprisonment in a county jail not exceeding one year, by a fine not exceeding five thousand dollars ($5,000), or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed nine hundred fifty dollars ($950), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value

of the computer services used exceeds nine hundred fifty dollars ($950), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6), (7), or (13) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000).

(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(4) Any person who violates paragraph (8) or (14) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both that fine and imprisonment.

(5) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000).

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(e)(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, the court may additionally award punitive or exemplary damages.

(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h)(1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

(2) Paragraph (3) of subdivision (c) does not apply to penalize any acts committed by a person acting outside of his or her lawful employment, provided that the employee's activities do not cause an injury, to the employer or another, or provided that the value of supplies or computer services which are used does not exceed an accumulated total of two hundred fifty dollars ($250).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

45 C.F.R. § 164.508

§ 164.508 Uses and disclosures for which an authorization is required.

(a) Standard: Authorizations for uses and disclosures

(1) Authorization required: General rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) Authorization required: Psychotherapy notes. Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(B) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) Authorization required: Marketing.

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

(4) Authorization required: Sale of protected health information.

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart. (ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.

(b) Implementation specifications: general requirements—

(1) Valid authorizations.

(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

(2) Defective authorizations. An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

(3) Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does

not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

(4) Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

(5) Revocation of authorizations. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(6) Documentation. A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

(c) Implementation specifications: Core elements and requirements—

(1) Core elements. A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

(iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

(2) Required statements. In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b) (4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

(3) Plain language requirement. The authorization must be written in plain language.

(4) Copy to the individual. If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

45 C.F.R. § 160.103

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.

Administrative simplification provision means any requirement or prohibition established by:

(1) 42 U.S.C. 1320d–1320d–4, 1320d–7, 1320d–8, and 1320d–9;

(2) Section 264 of Pub.L. 104–191;

(3) Sections 13400–13424 of Public Law 111–5; or

(4) This subchapter.

ALJ means Administrative Law Judge.

ANSI stands for the American National Standards Institute.

Business associate:

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the

covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A Health Information Organization, E–prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Civil money penalty or penalty means the amount determined under § 160.404 of this part and includes the plural of these terms.

CMS stands for Centers for Medicare & Medicaid Services within the Department of Health and Human Services.

Compliance date means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one of the following:

(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.

(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.

Electronic media means:

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section.

Employer is defined as it is in 26 U.S.C. 3401(d).

Family member means, with respect to an individual:

(1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or

(2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins. Genetic information means:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and

(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual.

Genetic services means:

(1) A genetic test;

(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

(3) Genetic education.

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Group health plan (also see definition of health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg–91(a)(2)), including items and services paid for as

medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan. HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg–91(b)(2) and used in the definition of health plan in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg–91(b)(3) and used in the definition of health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(1) Health plan includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

(vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w–101 through 1395w–152.

(vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

(ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(x) The health care program for uniformed services under title 10 of the United States Code.

(xi) The veterans health care program under 38 U.S.C. chapter 17.

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.

(xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(2) Health plan excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)–(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

Implementation specification means specific requirements or instructions for implementing a standard.

Individual means the person who is the subject of protected health information.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Manifestation or manifested means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

Modify or modification refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Person means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.

Respondent means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Small health plan means a health plan with annual receipts of $5 million or less.
Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services, or practices:

(i) Classification of components;

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of protected health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

Subcontractor means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Health care electronic funds transfers (EFT) and remittance advice.

(12) Other transactions that the Secretary may prescribe by regulation.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Violation or violate means, as the context may require, failure to comply with an administrative simplification provision.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

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 are registered CM/ECF users and will be served by the appellate CM/ECF system.

Dated: November 20, 2017 FARELLA BRAUN + MARTEL LLP

By: */s/ C. Brandon Wisoff*

C. Brandon Wisoff
Deepak Gupta
Jeffrey G. Lau
Rebecca H. Stephens
235 Montgomery Street, 17th Floor
San Francisco, California 94104
Telephone: (415) 954-4400
Facsimile: (415) 954-4480