CASE NO. 17-16783

In the United States Court of Appeals
For the Ninth Circuit

HIQ LABS, INC.
Plaintiff-Appellee,

v.

LINKEDIN CORPORATION
Defendant-Appellant,

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

APPELLANT'S PETITION FOR REHEARING AND REHEARING EN BANC

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

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

Attorneys for Defendant-Appellant *LinkedIn Corporation*

(additional counsel listed inside cover page)

(additional counsel continued from cover page)

ORRICK, HERRINGTON & SUTCLIFFE LLP

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

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

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

Attorneys for Defendant-Appellant *LinkedIn Corporation*

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

STATE CASES

TABLE OF AUTHORITIES
(Continued)

Page(s)

INTRODUCTION AND RULE 35(b) STATEMENT

The Computer Fraud and Abuse Act ("CFAA") prohibits parties from "intentionally access[ing] a computer without authorization." 18 U.S.C. § 1030(a)(2). It is foundational to the ability of website owners to control access to their computer servers in order to prevent abuse, including the furtive scraping of personal data on a massive scale. The panel's decision fundamentally weakens this protection and will have profound consequences for the Internet and for websites' ability to control access to their servers and guard their users' privacy. It should not stand.

In affirming an injunction forcing LinkedIn to allow hiQ's legion of data-scraping bots to access its servers, the panel held that owners of publicly facing websites—those that can be viewed without a password—cannot invoke the CFAA, regardless of what steps they take to limit someone's access or withdraw authorization. This interpretation conflicts with two prior decisions of this Court: (1) *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), which held that data scrapers need the permission of *both* the owner of the data on the website *and* the owner of the computer that operates the website; and (2) *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016) (*Nosal II*), which held that a password requirement was *not* a prerequisite to CFAA liability. The panel's decision also directly conflicts with the plain text of the statute, its interpretation

by other circuits, and its roots in property law, under which owners of private property have the right to evict bad actors, even if the property is generally open to the public.

These intra-circuit and inter-circuit conflicts make this precisely the kind of case in which reconsideration en banc is warranted. Fed. R. App. Proc. 35(b)(1)(A). But review is urgently needed not just to prevent the disarray that the panel's decision will sow. If left uncorrected, the decision will pose a grave threat to user privacy and the openness of the Internet. The panel concluded that the privacy interests of LinkedIn's 645 million members were not "significant enough to outweigh hiQ's interest in continuing its business" of scraping their personal data and selling it to their employers. Op. 16. In a world shaken by privacy breaches of staggering scope and depth, the panel's ruling is fundamentally at odds with the demands of policymakers and the public that technology companies do *more* to protect personal data entrusted to them, not less. And data aggregators are more aggressive than ever before, collecting and combining more and more personal data to create highly detailed user profiles.

As the Electronic Privacy Information Center (EPIC) stated in its amicus brief, the injunction here "discounted the privacy interests of users and required LinkedIn to make the personal data of LinkedIn users available to data aggregators for whatever purpose they wish. That cannot be correct." EPIC Br. 2. Consider

the following recent, extraordinary examples that demonstrate the need for companies like LinkedIn to prevent automated access to their users' data:

- A company scraped public posts of millions of Instagram users tagged with real-world locations—including posts that users "intended to vanish after 24 hours"—to create a "sophisticated database about Instagram users, their interests, and their movements."[1]

- A data analytics company combined public data from LinkedIn, Facebook, Twitter, and Zillow to "build a three-dimensional picture" on 48 million Americans, with everything from name and physical address to salary, marital status, and net worth.[2]

- An email marketing company amassed 809 million records, containing names, email and physical addresses, gender, date of birth, and phone numbers, all through "publicly available" sources.[3]

If computer owners cannot invoke the CFAA to stem abuse, data scrapers will operate with impunity, profoundly threatening both user privacy and Internet openness. Website operators' recourse would be to withdraw information from the public altogether, allowing access solely through password authentication systems. This would transform the Internet in ways that are inimical to open access and robust economic growth. En banc review is necessary to address these issues of exceptional importance and correct the panel's manifest errors.

---

[1]https://www.businessinsider.nl/startup-hyp3r-saving-instagram-users-stories-tracking-locations-2019-8/.

[2] https://www.zdnet.com/article/data-firm-leaks-48-million-user-profiles-it-scraped-from-facebook-linkedin-others/.

[3]https://www.wired.com/story/email-marketing-company-809-million-records-exposed-online/.

BACKGROUND

I. LINKEDIN

LinkedIn is a professional networking service that allows its members to create, manage, and share their professional identities and interests with people online. 5ER-824. LinkedIn members entrust their personal data to LinkedIn—including work and education history, profile narratives, and headshots—that LinkedIn stores on its computer servers.

LinkedIn does not permit the mass copying of data its members entrust to it. Its User Agreement makes clear that visitors cannot "[u]se bots or other automated methods to access" the website and "scrape" or "otherwise copy profiles." 4ER-775, 783. LinkedIn continuously employs multiple layers of technical barriers to prevent automated bots from scraping member data from its servers. 4ER-759-61. All member profiles—both those that are only viewable with a password, and those that can sometimes be viewed without one—are protected by these measures. *Id.* "In total, LinkedIn blocks approximately 95 million automated attempts to scrape data every day, and has restricted over 11 million accounts suspected of violating its User Agreement, including through scraping." Op. 8.

Because privacy is important to LinkedIn and its members, LinkedIn has a privacy policy that limits what LinkedIn can do with member data, regardless of whether that member sets her profile to allow others to view it with or without a

password. 4ER-787-96. LinkedIn also offers members a menu of privacy choices, so that they can control not only what information is shared, but how it is shared. For example, when a member updates her profile, LinkedIn lets that member choose not to broadcast that change to her connections to protect the member's privacy—a "Do Not Broadcast" option that over 50 million users have selected. 3ER-427; Op. 6. LinkedIn also promises members that if they delete their profiles, LinkedIn will permanently delete their data from its servers within 30 days. 4ER-794.

II. HIQ

hiQ uses a network of anonymous bots to continuously scrape hundreds of thousands of member profiles from LinkedIn's servers without the consent of LinkedIn or its members, and then repackages that data to sell to its clients. 4ER-766. As the district court found, hiQ "circumvent[s] LinkedIn's measures to prevent use of bots and implementation of IP address blocks." 1ER-16. hiQ has no contractual relationship with LinkedIn's members, and asserts that it has the right to scrape and keep any publicly-viewable data it wants, without any notice to or permission from the member. 3ER-516-17.

After scraping data from LinkedIn's servers, hiQ claims that it incorporates the data into analytics products it sells to customers. 5ER-859. hiQ's products specifically defeat the privacy protection LinkedIn offers. Indeed, a *goal* of hiQ's

"Keeper" product is to tell employers when LinkedIn members change their profiles—a common precursor to applying for new jobs—even if members have chosen not to broadcast such changes. *Id*. As the panel recognized, "the fact that a user has set his profile to public does not imply that he wants any third parties to collect and use that data for all purposes." Op. 14. Yet that is exactly what hiQ does.

III. PROCEDURAL HISTORY

As part of LinkedIn's efforts to keep data scrapers off its website, LinkedIn implemented additional technical measures to bar hiQ's access and sent hiQ a cease-and-desist letter demanding that hiQ stop accessing LinkedIn's servers to scrape data. 4ER-742. After receiving the letter, hiQ brought a complaint asserting claims under California tort and constitutional law, and seeking a declaratory judgment that LinkedIn could not invoke the CFAA here. 5ER-992. hiQ also sought and received a preliminary injunction forcing LinkedIn to disable its technical measures and allow hiQ's bots to access its servers. 1ER-1. The district court held that hiQ had shown "serious enough questions" as to its claim under California's Unfair Competition Law, and the court had "serious doubt[s]" whether LinkedIn could invoke the CFAA to preempt hiQ's state-law claims, 1ER-15, 23.

The panel affirmed. Addressing the equitable factors first, the panel held that LinkedIn members' "privacy interests in their information" were not "significant enough to outweigh hiQ's interest in continuing its business, which depends on accessing, analyzing, and communicating information derived from public LinkedIn profiles." Op. 16. As to likelihood of success, the panel affirmed on the alternative ground of hiQ's tortious interference with contract claim, even though the district court made no findings supporting this claim. Op. 24.

The panel next analyzed the CFAA, which prohibits parties from "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] ... information from any protected computer." 18 U.S.C. § 1030(a)(2). The panel recognized that "to scrape LinkedIn data, hiQ must access LinkedIn servers, which are 'protected computer[s]'" under the CFAA, and if hiQ's access is "'without authorization' within the meaning of the CFAA," then hiQ "could have no legal right of access to LinkedIn's data and so could not succeed on any of its state law claims." Op. 25.

The panel held, however, that the CFAA did not apply here. Op. 26-30. In breaking with every court (except for the district court) that had considered the question (*see* Opening Br. 40 (collecting authority)), it held that the CFAA does not govern access to publicly viewable data on websites because, "[w]here the default is free access without authorization, in ordinary parlance one would

characterize selective denial of access as a ban, not as a lack of 'authorization.'" Op. 26. This was the sum of its textual analysis, which the panel itself characterized as "debatable." *Id.* It concluded: "the CFAA's prohibition on accessing a computer 'without authorization' is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer," but a party's accessing "publicly available data will not constitute access without authorization under the CFAA." *Id*. at 33-34.[4]

REASONS FOR GRANTING REHEARING

I. THE PANEL'S DECISION CONFLICTS WITH PRIOR CFAA DECISIONS OF THIS CIRCUIT

The panel's decision conflicts with this Court's prior decisions in *Power Ventures* and *Nosal II*, leaving this Circuit's CFAA jurisprudence in disarray.

A. *Power Ventures*: Permission of the Computer Owner Is Necessary for Authorization

In *Power Ventures*, the defendant, Power, "aggregat[ed] the user's social networking information" through scraping data from Facebook after users granted

[4] The panel noted that a trespass to chattels claim might curb scrapers, but as it acknowledged (Op. 34 n.15), such claims require "actual or threatened interference with the computers' functioning." *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1353 (2003). "Sophisticated scrapers are unlikely to actually crash a data host's server, which makes trespass claims seem increasingly unlikely to succeed." *Symbiotic Relationships: Pragmatic Acceptance of Data Scraping*, 29 Berkeley Tech. L.J. 897, 914 (2014).

Power access to their Facebook accounts. 844 F.3d at 1062. Facebook sent Power a cease-and-desist letter revoking its permission to access Facebook's servers, implemented technical measures to prevent Power from returning, and ultimately sued when Power did not stop accessing Facebook's servers. *Id.* at 1063. In other words, Facebook took exactly the steps LinkedIn took here to deny Power authorization to scrape its servers.

Power therefore violated the CFAA. While Facebook's "users arguably gave Power permission to use Facebook's computers" in the first instance, "Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter." *Id.* at 1067. Critically, "[t]he consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission." *Id.* at 1068. For "Power to continue its campaign using Facebook's computers, it needed authorization *both* from *individual Facebook users* (who controlled their data and personal pages) *and from Facebook (which stored this data on its physical servers)*. Permission from the users alone was not sufficient to constitute authorization after Facebook issued the cease and desist letter." *Id.* (emphases added). *Power Ventures* thus holds that computer owners can deny authorization to access their physical servers within the meaning of the CFAA, even when users have authorized access to data stored on the owner's servers.

This framework—that the user must have authorization from *both* the data owner *and* the computer owner—cannot be reconciled with the panel's result here. Even if it were true that hiQ had implied authorization to access the publicly available portions of LinkedIn's website—and it is clearly not true, given the technical barriers hiQ knew about and circumvented—LinkedIn explicitly revoked any such permission. Instead of following the *Power Ventures* framework, the panel stopped at its first step: it held that because data owners (LinkedIn members) had decided to make their data "presumptively accessible to the general public," Op. 31, the permission of the computer owner (LinkedIn) was irrelevant. But *Power Ventures* holds the opposite. LinkedIn's servers are LinkedIn's property, and the CFAA is a "computer trespass" statute that allows computer owners to regulate access to their property. *Power Ventures*, 844 F.3d at 1065.

The panel sought to distinguish *Power Ventures* on the basis that while Power "was gathering user data that was protected by Facebook's username and password authentication system, the data hiQ was scraping was available to anyone with a web browser." Op. 31. But *Power Ventures* did not turn on *how* a data owner decided to make her data available to third parties—by expressly sharing a password (in *Power Ventures*) or by making it viewable to members of the public (here). Nothing about a data owner's decision to place her data on a website changes *LinkedIn's* independent right to regulate who can access its website

servers. To the contrary, *Power Ventures* acknowledged that "permission" to access websites that are "presumptively open to all comers" could be "revoked expressly" by the website owner. 844 F.3d at 1067 n.2.

The physical world analogy that *Power Ventures* employed underscores the conflict created by the panel decision. *Power Ventures* analogized itself to a scenario in which a person seeks to access a friend's safe-deposit box (with the friend's permission), but does so "while carrying a shotgun," and the bank therefore "ejects the person from its premises and bans his reentry." *Id*. at 1068. The "person needs permission *both* from his friend (who controls access to the safe) *and* from the bank (which controls access to its premises)." *Id.* Like Facebook (and like a bank), LinkedIn may regulate who accesses its premises, just like any owner of private property that is generally open to the public may eject those who break its rules. *Cf*. 75 Am. Jur. 2d Trespass § 40 ("Opening an establishment to transact business with the public is permission to enter" yet "invitation may be revoked"; "[o]nce the proprietor requests that a person leave, that individual has no legal right to remain").

B. ***Nosal II*: There Is No Password Requirement in the CFAA**

The panel also concluded that "we ... look to whether the conduct at issue is analogous to 'breaking and entering'" and thus "authorization is only required for password-protected sites or sites that otherwise prevent the general public from

viewing the information." Op. 27, 29. That flatly conflicts with this Court's decision in *Nosal II*, which expressly rejected a "technological access barrier" requirement under the CFAA. In dismissing the defendant's argument that the district court's jury instruction did not reference the circumvention of technological barriers as part of "without authorization," *Nosal II* held that the CFAA applies regardless of whether "the party circumvents a technological access barrier"—*like* a "password requirement"—because such a requirement is "missing from the statutory language." 844 F.3d at 1038-39.

The *hiQ* panel distinguished *Nosal II* on the basis that there, a former employee had "used current employees' login credentials to access company computers and collect confidential information." Op. 30. But *Nosal II rejected* the defendant's argument that the "CFAA only criminalizes access where the party circumvents a technological access barrier." 844 F.3d at 1038–39. The panel here, thus, "impermissibly graft[ed] onto the statute" a new password "requirement nowhere to be found in the statute's text," which this Court previously had recognized does not exist. *U.S. ex rel. Hartpence v. Kinetic Concepts, Inc.*, 792 F.3d 1121, 1127-28 (9th Cir. 2015) (en banc). And in any event, the district court found that hiQ *was circumventing* LinkedIn's technical barriers to prevent hiQ's access and bot scraping, 1ER-16—its behavior *was* akin to "breaking and entering."

* * *

Until the panel's decision, Ninth Circuit CFAA jurisprudence was stable and coherent: District courts and parties understood that trespassing on private computer property was forbidden, whether the trespasser was prevented from entering (through technical measures) or had been explicitly instructed to keep out (with a cease-and-desist letter). Courts thus understood that the CFAA lacks any "hacking" or "breaking and entering" requirement, and that a computer owner could selectively revoke "authorization" to access public websites. *E.g.*, *Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1169 (C.D. Cal. 2018) ("the word 'hack' does not appear anywhere in the [CFAA's] text.... In fact, courts in the Ninth Circuit have repeatedly recognized violations of the CFAA without characterizing the violations as hacking"); *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 829 (N.D. Cal. 2014) (same); *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1184 (N.D. Cal. 2013) (Breyer, J.) (even though "Craigslist gave the world permission (i.e., 'authorization') to access the public information on its public website," Craigslist "rescinded that permission for 3Taps" by sending a cease-and-desist letter and implementing technical blocks, so "[f]urther access by 3Taps after that rescission was 'without authorization'").

Now, however, district courts will have to choose which of this Court's cases to follow: *Power Ventures* and *Nosal II* (no locked password gate is required

for a CFAA violation) or this one (yes, it is). Only the en banc Court can restore the "uniformity of the court's decisions." Fed. R. App. P. 35(b)(1)(A).

II. THE PANEL'S DECISION CONFLICTS WITH THE CFAA'S PLAIN LANGUAGE

Just as the panel's decision conflicts with this Court's leading CFAA precedents, the decision is also impossible to square with the CFAA's plain text.

The sum of the panel's textual analysis is as follows: Because "authorization is an affirmative notion," where "the default is free access without authorization," there is no "authorization" to revoke. Instead, "in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of 'authorization.'" Op. 26. This analysis is wordplay. Someone banned from a restaurant has lost his authorization to enter. Likewise, a website can "affirmative[ly]" configure its computers to "authorize" access by members of the public, subject to its technical barriers on bot access, and when parties (like hiQ) evade those barriers and the computer owner responds by explicitly "banning" them from accessing the site, any further access is "without authorization." *3Taps,* 964 F. Supp. 2d at 1184 ("where a user is altogether banned from accessing a website," further access is "without authorization"); *Power Ventures*, 844 F.3d at 1068 (analogizing Facebook's actions to a "ban[]"). Nothing in the CFAA's text or the definition of "authorization" that the panel employed—"[o]fficial permission to do something; sanction or warrant," Op. 26—suggests that enabling websites to be publicly

viewable is not "authorization" that can be revoked. Indeed, the legislative history is expressly to the contrary: Congress recognized that individuals may be "*permitted* to access publicly available" computers by the computer owner, "for example, via [a] *World Wide Web site*." S. Rep. No. 104-357, at 8-9 (1996) (emphases added).

The panel's interpretation also ignores a critical distinction between public and nonpublic computers expressly written into the statute. At the same time that Congress added § 1030(a)(2)(C), it added § 1030(a)(3), which added a "nonpublic" modifier for government computers, without adding any such qualification to § 1030(a)(2)(C). In doing so, Congress acknowledged that authorized "access" to a "publicly available" computer under the CFAA could occur via a "World Wide Web site." *Id*. Thus, "Congress apparently knew how to restrict the reach of the CFAA to only certain kinds of information, and it appreciated the public vs. nonpublic distinction—but § 1030(a)(2)(C) contains no such restrictions or modifiers." *3Taps*, 964 F. Supp. 2d at 1182-83; *see SEC v. McCarthy*, 322 F.3d 650, 656 (9th Cir. 2003) ("use of different words or terms within a statute demonstrates that Congress intended to convey a different meaning for those words").[5]

[5] The panel briefly discussed the rule of lenity (Op. 33), but as in *Power Ventures*, "concerns about overreaching or an absence of culpable intent simply do not apply

Similarly, the panel's construction of "without authorization" is undermined by the Stored Communications Act ("SCA"), the very statute the panel relied upon, describing it as "nearly identical to the CFAA provision at issue." Op. 31-33. The panel ignored that unlike § 1030(a)(2), the SCA *expressly carves* out communications "readily accessible to the general public": "[i]t shall not be unlawful" under "chapter 121 [18 U.S.C. §§ 2701 et seq.] for any person—(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g). "No such language appears in the CFAA provision at issue here." *3Taps*, 964 F. Supp. 2d at 1183. The fact that Congress chose in the SCA to carve out "public" communications, but did not include similar language in the CFAA, confirms that the CFAA should *not* be read to include such an exception. *Id.*; *Blangeres v. Burlington N., Inc.*, 872 F.2d 327, 328 (9th Cir. 1989) ("We will not carve out exceptions to [statutes] unless Congress clearly expresses an intent to create an exception.").

---

here, where an individualized cease-and-desist letter is a far cry from the permission skirmishes that ordinary Internet users may face." 844 F.3d at 1069.

III. THE PANEL'S CONCLUSION CONFLICTS WITH OTHER CIRCUITS' PRECEDENT

The panel's construction of "authorization" also conflicts directly with the treatment of this same question by other circuits.

The First Circuit has rejected a "'presumption' of open access to Internet information," as "[t]he CFAA, after all, is primarily a statute imposing limits on access and enhancing control by information providers." *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003). Thus, a "public website provider can easily spell out explicitly what is forbidden" and if it "wants to ban scrapers," it may do so. *Id*. (enjoining scraper of public website).

Other circuits similarly have held that making a website publicly accessible is an affirmative grant of "authorization" to the public by the owner, which in turn may be withdrawn. *See Pulte Homes, Inc. v. Laborers' Int'l Union*, 648 F.3d 295, 304 (6th Cir. 2011) (where "an unprotected website [is] open to the public" a party is "authorized to use'" it); *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (same).

IV. THE PANEL'S OPINION RAISES ISSUES OF EXCEPTIONAL IMPORTANCE

The privacy implications of the panel's opinion are enormous. Although "the premise of [§ 1030(a)(2)] is privacy protection," S. Rep. No. 104-357, at 7 (cited at Op. 29), the panel held that "hiQ's interest in continuing its business" was

more important than the privacy interests of LinkedIn members in their personal data. Op. 16. This has seismic implications for user privacy on the Internet.

Instead of recognizing that LinkedIn members share their information on LinkedIn with the expectation that it will be viewed by a particular audience (human beings) in a particular way (by visiting their pages)—and that it will be subject to LinkedIn's sophisticated technical measures designed to block automated requests—the panel assumed that LinkedIn members expect that their data will be "accessed by others, including for commercial purposes," even purposes antithetical to their privacy setting selections. Op. 17. That conclusion is fundamentally wrong. LinkedIn members have privacy rights—and LinkedIn has corresponding obligations, pursuant to its privacy policy—regarding what happens to personal data members post to LinkedIn.

By contrast, hiQ has no contractual relationship with LinkedIn's members limiting how it can share their data or requiring its deletion if a member so requests. No contract prevents hiQ from selling member data to the highest bidder, or combining it with other data to create sophisticated profiles to facilitate identity theft or other unwanted behavior. hiQ flagrantly disregards the expectation "that the personal data [LinkedIn's members] provide [to LinkedIn] will be used to advance their careers, not acquired by an unaccountable third party." EPIC Br. 2. Like the owner of any business open to the public, LinkedIn is entitled—and best-

positioned—to protect its members from harm that bad actors would cause on its premises. Website owners' ability to protect Internet users is an issue of monumental importance, and the panel decision's severely limits that ability.

The panel's decision thus threatens the open nature of the Internet. Without the CFAA, website owners' recourse would be to withdraw information from public view altogether to prevent unwanted data scraping. If password walls are the only things that can stop bots, then more data will end up behind walls. This would transform the Internet in ways that are contrary to open access and robust economic growth.

CONCLUSION

For these reasons, the Court should grant the petition.

Respectfully submitted,

Dated: October 11, 2019

/s/ Donald B. Verrilli, Jr.

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

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

Attorneys for Defendant-Appellant
LinkedIn Corporation

ORRICK, HERRINGTON & SUTCLIFFE LLP

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

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

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

Attorneys for Defendant-Appellant
LinkedIn Corporation

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 11. Certificate of Compliance for Petitions for Rehearing or Answers

Instructions for this form: http://www.ca9.uscourts.gov/forms/form11instructions.pdf

9th Cir. Case Number(s) 17-16783

I am the attorney or self-represented party.

I certify that pursuant to Circuit Rule 35-4 or 40-1, the attached petition for panel rehearing/petition for rehearing en banc/answer to petition is (*select one*):

◉ Prepared in a format, typeface, and type style that complies with Fed. R. App. P. 32(a)(4)-(6) and **contains the following number of words**: 4,198.

(Petitions and answers must not exceed 4,200 words)

OR

○ In compliance with Fed. R. App. P. 32(a)(4)-(6) and does not exceed 15 pages.

Signature /s/ Donald B. Verrilli, Jr. **Date** 10/11/2019

*(use "*s/[typed name]*" to sign electronically-filed documents)*

Addendum A
Panel Opinion

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

HIQ LABS, INC., *Plaintiff-Appellee*, v. LINKEDIN CORPORATION, *Defendant-Appellant.*	No. 17-16783 D.C. No. 3:17-cv-03301-EMC OPINION

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

Argued and Submitted March 15, 2018
San Francisco, California

Filed September 9, 2019

Before: J. Clifford Wallace and Marsha S. Berzon, Circuit Judges, and Terrence Berg,* District Judge.

Opinion by Judge Berzon;
Concurrence by Judge Wallace

* The Honorable Terrence Berg, United States District Judge for the Eastern District of Michigan, sitting by designation.

SUMMARY**

Preliminary Injunction / Computer Fraud and Abuse Act

The panel affirmed the district court's preliminary injunction forbidding the professional networking website LinkedIn Corp. from denying plaintiff hiQ, a data analytics company, access to publicly available LinkedIn member profiles.

Using automated bots, hiQ scrapes information that LinkedIn users have included on public LinkedIn profiles. LinkedIn sent hiQ a cause-and-desist letter, demanding that hiQ stop accessing and copying data from LinkedIn's server. HiQ filed suit, seeking injunctive relief based on California law and a declaratory judgment that LinkedIn could not lawfully invoke the Computer Fraud and Abuse Act ("CFAA"), the Digital Millennium Copyright Act, California Penal Code § 502(c), or the common law of trespass against it.

Affirming the district court's grant of the preliminary injunction in favor of hiQ, the panel concluded that hiQ established a likelihood of irreparable harm because the survival of its business was threatened. The panel held that the district court did not abuse its discretion in balancing the equities and concluding that, even if some LinkedIn users retain some privacy interests in their information notwithstanding their decision to make their profiles public,

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

those interests did not outweigh hiQ's interest in continuing its business. Thus, the balance of hardships tipped decidedly in favor of hiQ.

The panel further held that hiQ raised serious questions going to (1) the merits of its claim for tortious interference with contract, alleging that LinkedIn intentionally interfered with its contracts with third parties, and (2) the merits of LinkedIn's legitimate business purpose defense. HiQ also raised a serious question as to whether its state law causes of action were preempted by the CFAA, which prohibits intentionally accessing a computer without authorization, or exceeding authorized access, and thereby obtaining information from any protected computer. LinkedIn argued that, once hiQ received its cause-and-desist letter, any further scraping and use of LinkedIn's data was without authorization within the meaning of the CFAA. The panel concluded that hiQ had raised a serious question as to whether the CFAA's reference to access "without authorization" limits the scope of statutory coverage to computer information for which authorization or access permission, such as password authentication, is generally required.

Finally, the panel held that the district court's conclusion that the public interest favored granting the preliminary injunction was appropriate.

Specially concurring, Judge Wallace wrote that he concurred in the majority opinion. He wrote separately to express his concern about appealing from a preliminary injunction to obtain an appellate court's view of the merits.

COUNSEL

Donald B. Verrilli Jr. (argued) and Chad I. Golder, Munger Tolles & Olson LLP, Washington, D.C.; Jonathan H. Blavin, Rosemarie T. Ring, Nicholas D. Fram, and Elia Herrera, Munger Tolles & Olson LLP, San Francisco, California; E. Joshua Rosenkranz, Orrick Herrington & Sutcliffe LLP, New York, New York; Eric A. Shumsky, Orrick Herrington & Sutcliffe LLP, Washington, D.C.; Brian P. Goldman, Orrick Herrington & Sutcliffe LLP, San Francisco, California; for Defendant-Appellant.

C. Brandon Wisoff (argued), Deepak Gupta, Jeffrey G. Lau, and Rebecca H. Stephens, Farella Braun & Martel LLP, San Francisco, California; Aaron M. Panner, Gregory G. Rapawy, and T. Dietrich Hill, Kellogg Hansen Todd Figel & Frederick PLLC, Washington, D.C.; Laurence H. Tribe, Cambridge, Massachusetts; for Plaintiff-Appellee.

Nicholas J. Boyle, John S. Williams, and Eric J. Hamilton, Williams & Connolly LLP, Washington, D.C., for Amicus Curiae CoStar Group Inc.

Perry J. Viscounty, Latham & Watkins LLP, San Francisco, California; Gregory G. Garre, Latham & Watkins LLP, Washington, D.C.; for Amicus Curiae Craigslist Inc.

Marc Rotenberg and Alan Butler, Electronic Privacy Information Center, Washington, D.C., for Amicus Curiae Electronic Privacy Information Center.

Thomas V. Christopher, Law Offices of Thomas V. Christopher, San Francisco, California, for Amicus Curiae 3taps Inc.

Jamie Williams, Corynne McSherry, Cindy Cohn, and Nathan Cardozo, Electronic Frontier Foundation, San Francisco, California, for Amici Curiae Electronic Frontier Foundation, DuckDuckGo, and Internet Archive.

Kenneth L. Wilton and James M. Harris, Seyfarth Shaw LLP, Los Angeles, California; Carrie P. Price, Seyfarth Shaw LLP, San Francisco, California; for Amicus Curiae Scraping Hub Ltd.

OPINION

BERZON, Circuit Judge:

May LinkedIn, the professional networking website, prevent a competitor, hiQ, from collecting and using information that LinkedIn users have shared on their public profiles, available for viewing by anyone with a web browser? HiQ, a data analytics company, obtained a preliminary injunction forbidding LinkedIn from denying hiQ access to publicly available LinkedIn member profiles. At this preliminary injunction stage, we do not resolve the companies' legal dispute definitively, nor do we address all the claims and defenses they have pleaded in the district court. Instead, we focus on whether hiQ has raised serious questions on the merits of the factual and legal issues presented to us, as well as on the other requisites for preliminary relief.

I.

Founded in 2002, LinkedIn is a professional networking website with over 500 million members. Members post resumes and job listings and build professional "connections" with other members. LinkedIn specifically

disclaims ownership of the information users post to their personal profiles: according to LinkedIn's User Agreement, members own the content and information they submit or post to LinkedIn and grant LinkedIn only a non-exclusive license to "use, copy, modify, distribute, publish, and process" that information.

LinkedIn allows its members to choose among various privacy settings. Members can specify which portions of their profile are visible to the general public (that is, to both LinkedIn members and nonmembers), and which portions are visible only to direct connections, to the member's "network" (consisting of LinkedIn members within three degrees of connectivity), or to all LinkedIn members.[1] This case deals only with profiles made visible to the general public.

LinkedIn also offers all members—whatever their profile privacy settings—a "Do Not Broadcast" option with respect to every change they make to their profiles. If a LinkedIn member selects this option, her connections will not be notified when she updates her profile information, although the updated information will still appear on her profile page (and thus be visible to anyone permitted to view her profile under her general privacy setting). More than 50

[1] Direct connections (or first-degree connections) are people to whom a LinkedIn member is connected by virtue of having invited them to connect and had the invitation accepted, or of having accepted their invitation to connect. Second-degree connections are people connected to a member's first-degree connections. Third-degree connections are people connected to a member's second-degree connections. A LinkedIn member's network consists of the member's first-degree, second-degree, and third-degree connections, as well as fellow members of the same LinkedIn Groups (groups of members in the same industry or with similar interests that any member can request to join).

million LinkedIn members have, at some point, elected to employ the "Do Not Broadcast" feature, and approximately 20 percent of all active users who updated their profiles between July 2016 and July 2017—whatever their privacy setting—employed the "Do Not Broadcast" setting.

LinkedIn has taken steps to protect the data on its website from what it perceives as misuse or misappropriation. The instructions in LinkedIn's "robots.txt" file—a text file used by website owners to communicate with search engine crawlers and other web robots—prohibit access to LinkedIn servers via automated bots, except that certain entities, like the Google search engine, have express permission from LinkedIn for bot access.[2] LinkedIn also employs several technological systems to detect suspicious activity and

[2] A web robot (or "bot") is an application that performs automated tasks such as retrieving and analyzing information. *See Definition of "bot,"* Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/bot (last visited July 12, 2019). A web crawler is one common type of bot that systematically searches the Internet and downloads copies of web pages, which can then be indexed by a search engine. *See Assoc. Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 544 (S.D.N.Y. 2013); *Definition of "web crawler,"* Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/web%20crawler (last visited July 12, 2019). A robots.txt file, also known as the robots exclusion protocol, is a widely used standard for stating the rules that a web server has adopted to govern a bot's behavior on that server. *See About /robots.txt*, http://www.robotstxt.org/robotstxt.html (last visited July 12, 2019). For example, a robots.txt file might instruct specified robots to ignore certain files when crawling a site, so that the files do not appear in search engine results. Adherence to the rules in a robots.txt file is voluntary; malicious bots may deliberately choose not to honor robots.txt rules and may in turn be punished with a denial of access to the website in question. *See Can I Block Just Bad Robots?*, http://www.robotstxt.org/faq/blockjustbad.html (last visited July 12, 2019); *cf. Assoc. Press*, 931 F. Supp. 2d at 563 (S.D.N.Y. 2013).

restrict automated scraping.[3] For example, LinkedIn's Quicksand system detects non-human activity indicative of scraping; its Sentinel system throttles (slows or limits) or even blocks activity from suspicious IP addresses;[4] and its Org Block system generates a list of known "bad" IP addresses serving as large-scale scrapers. In total, LinkedIn blocks approximately 95 million automated attempts to scrape data every day, and has restricted over 11 million accounts suspected of violating its User Agreement,[5] including through scraping.

HiQ is a data analytics company founded in 2012. Using automated bots, it scrapes information that LinkedIn users

---

[3] Scraping involves extracting data from a website and copying it into a structured format, allowing for data manipulation or analysis. *See, e.g.*, *What Is a Screen Scraper?*, WiseGeek, http://www.wisegeek.com/what-is-a-screen-scraper.htm (last visited July 12, 2019). Scraping can be done manually, but as in this case, it is typically done by a web robot or "bot." *See supra* note 2.

[4] "IP address" is an abbreviation for Internet protocol address, which is a numerical identifier for each computer or network connected to the Internet. *See Definition of "IP Address,"* Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/IP%20address (last visited July 12, 2019).

[5] Section 8.2 of the LinkedIn User Agreement to which hiQ agreed states that users agree not to "[s]crape or copy profiles and information of others through any means (including crawlers, browser plugins and add-ons, and any other technology or manual work)," "[c]opy or use the information, content or data on LinkedIn in connection with a competitive service (as determined by LinkedIn)," "[u]se manual or automated software, devices, scripts robots, other means or processes to access, 'scrape,' 'crawl' or 'spider' the Services or any related data or information," or "[u]se bots or other automated methods to access the Services." HiQ is no longer bound by the User Agreement, as LinkedIn has terminated hiQ's user status.

have included on public LinkedIn profiles, including name, job title, work history, and skills. It then uses that information, along with a proprietary predictive algorithm, to yield "people analytics," which it sells to business clients.

HiQ offers two such analytics. The first, Keeper, purports to identify employees at the greatest risk of being recruited away. According to hiQ, the product enables employers to offer career development opportunities, retention bonuses, or other perks to retain valuable employees. The second, Skill Mapper, summarizes employees' skills in the aggregate. Among other things, the tool is supposed to help employers identify skill gaps in their workforces so that they can offer internal training in those areas, promoting internal mobility and reducing the expense of external recruitment.

HiQ regularly organizes "Elevate" conferences, during which participants discuss hiQ's business model and share best practices in the people analytics field. LinkedIn representatives participated in Elevate conferences beginning in October 2015. At least ten LinkedIn representatives attended the conferences. LinkedIn employees have also spoken at Elevate conferences. In 2016, a LinkedIn employee was awarded the Elevate "Impact Award." LinkedIn employees thus had an opportunity to learn about hiQ's products, including "that [one of] hiQ's product[s] used data from a variety of sources—internal and external—to predict employee attrition" and that hiQ "collected skills data from public professional profiles in order to provide hiQ's customers information about their employees' skill sets."

In recent years, LinkedIn has explored ways to capitalize on the vast amounts of data contained in LinkedIn profiles by marketing new products. In June 2017, LinkedIn's Chief

Executive Officer ("CEO"), Jeff Weiner, appearing on CBS, explained that LinkedIn hoped to "leverage all this extraordinary data we've been able to collect by virtue of having 500 million people join the site." Weiner mentioned as possibilities providing employers with data-driven insights about what skills they will need to grow and where they can find employees with those skills. Since then, LinkedIn has announced a new product, Talent Insights, which analyzes LinkedIn data to provide companies with such data-driven information.[6]

In May 2017, LinkedIn sent hiQ a cease-and-desist letter, asserting that hiQ was in violation of LinkedIn's User Agreement and demanding that hiQ stop accessing and copying data from LinkedIn's server. The letter stated that if hiQ accessed LinkedIn's data in the future, it would be violating state and federal law, including the Computer Fraud and Abuse Act ("CFAA"), the Digital Millennium Copyright Act ("DMCA"), California Penal Code § 502(c), and the California common law of trespass. The letter further stated that LinkedIn had "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."

[6] The record does not specifically name Talent Insights, but at a district court hearing on June 29, 2017, counsel for hiQ referenced Mr. Weiner's statements on CBS and stated that "in the past 24 hours we've received word . . . that LinkedIn is launching a product that is essentially the same or very similar to [hiQ's] Skill Mapper, and trying to market it head-to-head against us." LinkedIn has since launched Talent Insights, which, among other things, promises to help employers "understand the . . . skills that are growing fastest at your company." *See* https://business.linkedin.com/talent-solutions/blog/product-updates/2018/linkedin-talent-insights-now-available (last visited July 12, 2019).

HiQ's response was to demand that LinkedIn recognize hiQ's right to access LinkedIn's public pages and to threaten to seek an injunction if LinkedIn refused. A week later, hiQ filed suit, seeking injunctive relief based on California law and a declaratory judgment that LinkedIn could not lawfully invoke the CFAA, the DMCA, California Penal Code § 502(c), or the common law of trespass against it. HiQ also filed a request for a temporary restraining order, which the parties subsequently agreed to convert into a motion for a preliminary injunction.

The district court granted hiQ's motion. It ordered LinkedIn to withdraw its cease-and-desist letter, to remove any existing technical barriers to hiQ's access to public profiles, and to refrain from putting in place any legal or technical measures with the effect of blocking hiQ's access to public profiles. LinkedIn timely appealed.

II.

"A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). All four elements must be satisfied. *See, e.g.*, *Am. Trucking Ass'n v. City of Los Angeles*, 559 F.3d 1046, 1057 (9th Cir. 2009). We use a "sliding scale" approach to these factors, according to which "a stronger showing of one element may offset a weaker showing of another." *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011). So, when the balance of hardships tips sharply in the plaintiff's favor, the plaintiff need demonstrate only "serious questions going to the merits." *Id.* at 1135.

Applying that sliding scale approach, the district court granted hiQ a preliminary injunction, concluding that the balance of hardships tips sharply in hiQ's favor and that hiQ raised serious questions on the merits. We review the district court's decision to grant a preliminary injunction for abuse of discretion. The grant of a preliminary injunction constitutes an abuse of discretion if the district court's evaluation or balancing of the pertinent factors is "illogical, implausible, or without support in the record." *Doe v. Kelly*, 878 F.3d 710, 713 (9th Cir. 2017).

A. Irreparable Harm

We begin with the likelihood of irreparable injury to hiQ if preliminary relief were not granted.

"[M]onetary injury is not normally considered irreparable." *Los Angeles Mem'l Coliseum Comm'n v. Nat'l Football League*, 634 F.2d 1197, 1202 (9th Cir. 1980). Nonetheless, "[t]he threat of being driven out of business is sufficient to establish irreparable harm." *Am. Passage Media Corp. v. Cass Commc'ns, Inc.*, 750 F.2d 1470, 1474 (9th Cir. 1985). As the Second Circuit has explained, "[t]he loss of . . . an ongoing business representing many years of effort and the livelihood of its . . . owners, constitutes irreparable harm. What plaintiff stands to lose cannot be fully compensated by subsequent monetary damages." *Roso Lino Beverage Distributors, Inc. v. Coca Cola Bottling Co. of New York, Inc.*, 749 F.2d 124, 125–26 (2d Cir. 1984) (per curiam). Thus, showing a threat of "extinction" is enough to establish irreparable harm, even when damages may be available and the amount of direct financial harm is ascertainable. *Am. Passage Media Corp.*, 750 F.2d at 1474.

The district court found credible hiQ's assertion that the survival of its business is threatened absent a preliminary

injunction. The record provides ample support for that finding.

According to hiQ's CEO, "hiQ's entire business depends on being able to access public LinkedIn member profiles," as "there is no current viable alternative to LinkedIn's member database to obtain data for hiQ's Keeper and Skill Mapper services." Without access to LinkedIn public profile data, the CEO averred, hiQ will likely be forced to breach its existing contracts with clients such as eBay, Capital One, and GoDaddy, and to pass up pending deals with prospective clients. The harm hiQ faces absent a preliminary injunction is not purely hypothetical. HiQ was in the middle of a financing round when it received LinkedIn's cease-and-desist letter. The CEO reported that, in light of the uncertainty about the future viability of hiQ's business, that financing round stalled, and several employees left the company. If LinkedIn prevails, hiQ's CEO further asserted, hiQ would have to "lay off most if not all its employees, and shutter its operations."

LinkedIn maintains that hiQ's business model does not depend on access to LinkedIn data. It insists that alternatives to LinkedIn data exist, and points in particular to the professional data some users post on Facebook. But hiQ's model depends on access to publicly available data from people who choose to share their information with the world. Facebook data, by contrast, is not generally accessible, *see infra* p. 31, and therefore is not an equivalent alternative source of data.

LinkedIn also urges that even if there is no adequate alternative database, hiQ could collect its own data through employee surveys. But hiQ is a data analytics company, not a data collection company. Suggesting that hiQ could fundamentally change the nature of its business, not simply

the manner in which it conducts its current business, is a recognition that hiQ's current business could not survive without access to LinkedIn public profile data. Creating a data collection system would undoubtedly require a considerable amount of time and expense. That hiQ could feasibly remain in business with no products to sell while raising the required capital and devising and implementing an entirely new data collection system is at least highly dubious.

In short, the district court did not abuse its discretion in concluding on the preliminary injunction record that hiQ currently has no viable way to remain in business other than using LinkedIn public profile data for its Keeper and Skill Mapper services, and that HiQ therefore has demonstrated a likelihood of irreparable harm absent a preliminary injunction.

B. Balance of the Equities

Next, the district court "balance[d] the interests of all parties and weigh[ed] the damage to each in determining the balance of the equities." *CTIA-The Wireless Ass'n v. City of Berkeley, Calif.*, 928 F.3d 832, 852 (9th Cir. 2019) (internal quotation marks and citation omitted). Again, it did not abuse its discretion in doing so.

On one side of the scale is the harm to hiQ just discussed: the likelihood that, without an injunction, it will go out of business. On the other side, LinkedIn asserts that the injunction threatens its members' privacy and therefore puts at risk the goodwill LinkedIn has developed with its members. As the district court observed, "the fact that a user has set his profile to public does not imply that he wants any third parties to collect and use that data for all purposes." LinkedIn points in particular to the more than 50 million

members who have used the "Do Not Broadcast" feature to ensure that other users are not notified when the member makes a profile change. According to LinkedIn, the popularity of the "Do Not Broadcast" feature indicates that many members—including members who choose to share their information publicly—do not want their employers to know they may be searching for a new job. An employer who learns that an employee may be planning to leave will not necessarily reward that employee with a retention bonus. Instead, the employer could decide to limit the employee's access to sensitive information or even to terminate the employee.

There is support in the record for the district court's connected conclusions that (1) LinkedIn's assertions have some merit; and (2) there are reasons to discount them to some extent. First, there is little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly, and it is doubtful that they do. LinkedIn's privacy policy clearly states that "[a]ny information you put on your profile and any content you post on LinkedIn may be seen by others" and instructs users not to "post or add personal data to your profile that you would not want to be public."

Second, there is no evidence in the record to suggest that most people who select the "Do Not Broadcast" option do so to prevent their employers from being alerted to profile changes made in anticipation of a job search. As the district court noted, there are other reasons why users may choose that option—most notably, many users may simply wish to avoid sending their connections annoying notifications each time there is a profile change. In any event, employers can always directly consult the profiles of users who chose to

make their profiles public to see if any recent changes have been made. Employees intent on keeping such information from their employers can do so by rejecting public exposure of their profiles and eliminating their employers as contacts.

Finally, LinkedIn's own actions undercut its argument that users have an expectation of privacy in public profiles. LinkedIn's "Recruiter" product enables recruiters to "follow" prospects, get "alert[ed] when prospects make changes to their profiles," and "use those [alerts] as signals to reach out at just the right moment," without the prospect's knowledge.[7] And subscribers to LinkedIn's "talent recruiting, marketing and sales solutions" can export data from members' public profiles, such as "name, headline, current company, current title, and location."

In short, even if some users retain some privacy interests in their information notwithstanding their decision to make their profiles public, we cannot, on the record before us, conclude that those interests—or more specifically, LinkedIn's interest in preventing hiQ from scraping those profiles—are significant enough to outweigh hiQ's interest in continuing its business, which depends on accessing, analyzing, and communicating information derived from public LinkedIn profiles.

Nor do the other harms asserted by LinkedIn tip the balance of harms with regard to preliminary relief. LinkedIn invokes an interest in preventing "free riders" from using profiles posted on its platform. But LinkedIn has no protected property interest in the data contributed by its users, as the users retain ownership over their profiles. And

[7] Recruiter does not provide alerts about profile changes made by LinkedIn members who select the "Do Not Broadcast" setting.

as to the publicly available profiles, the users quite evidently intend them to be accessed by others, including for commercial purposes—for example, by employers seeking to hire individuals with certain credentials. Of course, LinkedIn could satisfy its "free rider" concern by eliminating the public access option, albeit at a cost to the preferences of many users and, possibly, to its own bottom line.

We conclude that the district court's determination that the balance of hardships tips sharply in hiQ's favor is not "illogical, implausible, or without support in the record." *Kelly*, 878 F.3d at 713.

C. Likelihood of Success

Because hiQ has established that the balance of hardships tips decidedly in its favor, the likelihood-of-success prong of the preliminary injunction inquiry focuses on whether hiQ has raised "serious questions going to the merits." *Alliance for the Wild Rockies*, 632 F.3d at 1131. It has.

As usual, we consider only the claims and defenses that the parties press on appeal. We recognize that the companies have invoked additional claims and defenses in the district court, and we express no opinion as to whether any of those claims or defenses might ultimately prove meritorious. Thus, while hiQ advanced several affirmative claims in support of its request for preliminary injunctive relief, here we consider only whether hiQ has raised serious questions on the merits of its claims either for intentional interference with contract or unfair competition, under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* Likewise, while LinkedIn has asserted that it has "claims under the Digital Millennium Copyright Act and under trespass and misappropriation doctrines," it has chosen for

present purposes to focus on a defense based on the CFAA, so that is the sole defense to hiQ's claims that we address here.

1. Tortious Interference with Contract

HiQ alleges that LinkedIn intentionally interfered with hiQ's contracts with third parties. "The elements which a plaintiff must plead to state the cause of action for intentional interference with contractual relations 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).[8]

HiQ has shown a sufficient likelihood of establishing each of these elements. First, LinkedIn does not contest

[8] Under California law, tortious interference with contract claims are not limited to circumstances in which the defendant has caused the third party with whom the plaintiff has contracted to breach the agreement. "The most general application of the rule is to cases where the party with whom the plaintiff has entered into an agreement has been induced to breach it, but the rule is also applicable where the plaintiff's performance has been prevented or rendered more expensive or burdensome and where he has been induced to breach the contract by conduct of the defendant, such as threats of economic reprisals." *Lipman v. Brisbane Elementary Sch. Dist.*, 55 Cal. 2d 224, 232 (1961), *abrogated on other grounds by Brown v. Kelly Broadcasting Co.*, 48 Cal. 3d 711, 753 n.37 (1989); *see also Pac. Gas & Elec. Co.*, 50 Cal. 3d at 1129 ("We have recognized that interference with the plaintiff's performance may give rise to a claim for interference with contractual relations if plaintiff's performance is made more costly or more burdensome.").

hiQ's evidence that contracts exist between hiQ and some customers, including eBay, Capital One, and GoDaddy.

Second, hiQ will likely be able to establish that LinkedIn knew of hiQ's scraping activity and products for some time. LinkedIn began sending representatives to hiQ's Elevate conferences in October 2015. At those conferences, hiQ discussed its business model, including its use of data from external sources to predict employee attrition. LinkedIn's director of business operations and analytics, who attended several Elevate conferences, specifically "recall[s] someone from hiQ stating [at the April 2017 conference] that they collected skills data from public professional profiles in order to provide hiQ's customers information about their employees' skill sets." Additionally, LinkedIn acknowledged in its cease-and-desist letter that "hiQ has stated during marketing presentations that its Skill Mapper product is built on profile data from LinkedIn." Finally, at a minimum, LinkedIn knew of hiQ's contracts as of May 31, 2017, when hiQ responded to LinkedIn's cease-and-desist letter and identified both current and prospective hiQ clients.

Third, LinkedIn's threats to invoke the CFAA and implementation of technical measures selectively to ban hiQ bots could well constitute "intentional acts designed to induce a breach or disruption" of hiQ's contractual relationships with third parties. *Pac. Gas & Elec. Co.*, 50 Cal. 3d at 1126; *cf. Winchester Mystery House, LLC v. Global Asylum, Inc.*, 210 Cal. App. 4th 579, 597 (2012) (indicating that "cease-and-desist letters . . . refer[ring] to a[] contractual or other economic relationship between plaintiff and any third party" could "establish . . . the . . . intent element[] of the interference claim[]").

Fourth, the contractual relationships between hiQ and third parties have been disrupted and "now hang[] in the

balance." Without access to LinkedIn data, hiQ will likely be unable to deliver its services to its existing customers as promised.

Last, hiQ is harmed by the disruption to its existing contracts and interference with its pending contracts. Without the revenue from sale of its products, hiQ will likely go out of business. *See supra* pp. 12–14.

LinkedIn does not specifically challenge hiQ's ability to make out any of these elements of a tortious interference claim. Instead, LinkedIn maintains that it has a "legitimate business purpose" defense to any such claim. *Cf. Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal. 4th 26, 57 (1998), *as modified* (Sept. 23, 1998). That contention is an affirmative justification defense for which LinkedIn bears the burden of proof. *See id.*

Under California law, a legitimate business purpose can indeed justify interference with contract, but not just any such purpose suffices. *See id.* at 55–56. Where a contractual relationship exists, the societal interest in "contractual stability is generally accepted as of greater importance than competitive freedom." *Imperial Ice Co. v. Rossier*, 18 Cal. 2d 33, 36 (1941). Emphasizing the "distinction between claims for the tortious disruption of an existing contract and claims that a prospective contractual or economic relationship has been interfered with by the defendant," the California Supreme Court instructs that we must "bring[] a greater solicitude to those relationships that have ripened into agreements." *Della Penna v. Toyota Motor Sales, U.S.A., Inc.*, 11 Cal. 4th 376, 392 (1995). Thus, interference with an existing contract is not justified simply because a competitor "seeks to further his own economic advantage at the expense of another." *Imperial Ice*, 18 Cal. 2d at 36; *see id.* at 37 ("A party may not . . . under the guise of

competition . . . induce the breach of a competitor's contract in order to secure an economic advantage."). Rather, interference with contract is justified only when the party alleged to have interfered acted "to protect an interest that has greater social value than insuring the stability of the contract" interfered with. *Id.* at 35.

Accordingly, California courts apply a balancing test to determine whether the interests advanced by interference with contract outweigh the societal interest in contractual stability:

> Whether an intentional interference by a third party is justifiable 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). Considerations include whether "the means of interference involve no more than recognized trade practices," *Buxbom v. Smith*, 23 Cal. 2d 535, 546 (1944), and whether the conduct is "within the realm of fair competition," *Inst. of Veterinary Pathology, Inc. v. Cal. Health Labs., Inc.*, 116 Cal. App. 3d 111, 127 (Cal. Ct. App. 1981). The "determinative question" is whether the business interest is pretextual or "asserted in good faith." *Richardson v. La Rancherita*, 98 Cal. App. 3d 73, 81 (Cal. Ct. App. 1979).

Balancing the interest in contractual stability and the specific interests interfered with against the interests advanced by the interference, we agree with the district court

that hiQ has at least raised a serious question on the merits of LinkedIn's affirmative justification defense. First, hiQ has a strong commercial interest in fulfilling its contractual obligations to large clients like eBay and Capital One. Those companies benefit from hiQ's ability to access, aggregate, and analyze data from LinkedIn profiles.

Second, LinkedIn's means of interference is likely not a "recognized trade practice" as California courts have understood that term. "Recognized trade practices" include such activities as "advertising," "price-cutting," and "hir[ing] the employees of another for use in the hirer's business," *Buxbom*, 23 Cal. 2d at 546–47—all practices which may indirectly interfere with a competitor's contracts but do not fundamentally undermine a competitor's basic business model. LinkedIn's proactive technical measures to selectively block hiQ's access to the data on its site are not similar to trade practices heretofore recognized as acceptable justifications for contract interference.

Further, LinkedIn's conduct may well not be "within the realm of fair competition." *Inst. of Veterinary Pathology*, 116 Cal. App. 3d at 127. HiQ has raised serious questions about whether LinkedIn's actions to ban hiQ's bots were taken in furtherance of LinkedIn's own plans to introduce a competing professional data analytics tool. There is evidence from which it can be inferred that LinkedIn knew about hiQ and its reliance on external data for several years before the present controversy. Its decision to send a cease-and-desist letter occurred within a month of the announcement by LinkedIn's CEO that LinkedIn planned to leverage the data on its platform to create a new product for employers with some similarities to hiQ's Skill Mapper product. If companies like LinkedIn, whose servers hold vast amounts of public data, are permitted selectively to ban only potential

competitors from accessing and using that otherwise public data, the result—complete exclusion of the original innovator in aggregating and analyzing the public information—may well be considered unfair competition under California law.[9]

Finally, LinkedIn's asserted private business interests—"protecting its members' data and the investment made in developing its platform" and "enforcing its User Agreements' prohibitions on automated scraping"—are relatively weak. LinkedIn has only a non-exclusive license to the data shared on its platform, not an ownership interest. Its core business model—providing a platform to share professional information—does not require prohibiting hiQ's use of that information, as evidenced by the fact that hiQ used LinkedIn data for some time before LinkedIn sent its cease-and-desist letter. As to its members' interests in their data, for the reasons already explained, *see supra* pp. 15–16, we agree with the district court that members' privacy expectations regarding information they have shared in their public profiles are "uncertain at best." Further, there is evidence that LinkedIn has itself developed a data analytics tool similar to HiQ's products, undermining LinkedIn's claim that it has its members' privacy interests in mind. Finally, LinkedIn has not explained how it can enforce its user agreement against hiQ now that its user status has been terminated.

[9] The district court determined that LinkedIn's legitimate business purpose defense overlapped with hiQ's claim under California's Unfair Competition Law ("UCL"), which the district court found raised serious questions on the merits: "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, and thus potentially 'violates [the UCL].'"

For all these reasons, LinkedIn may well not be able to demonstrate a "legitimate business purpose" that could justify the intentional inducement of a contract breach, at least on the record now before us. We therefore conclude that hiQ has raised at least serious questions going to the merits of its tortious interference with contract claim. As that showing on the tortious interference claim is sufficient to support an injunction prohibiting LinkedIn from selectively blocking hiQ's access to public member profiles, we do not reach hiQ's unfair competition claim.[10]

2. Computer Fraud and Abuse Act (CFAA)

Our inquiry does not end, however, with the state law tortious interference claim. LinkedIn argues that even if hiQ can show a likelihood of success on any of its state law causes of action, all those causes of action are preempted by the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, which LinkedIn asserts that hiQ violated.

The CFAA states that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds

[10] LinkedIn also advances a business interest in "asserting its rights under federal and state law." That interest depends upon the scope of LinkedIn's rights under the CFAA and California's CFAA analogue, California Penal Code § 502. Similarly, LinkedIn argues that there can be no tortious interference because hiQ's contracts are premised on unauthorized access to LinkedIn data and are therefore illegal. Under California law, "[i]f the central purpose of the contract is tainted with illegality, then the contract as a whole cannot be enforced." *Marathon Entm't, Inc. v. Blasi*, 42 Cal. 4th 974, 996 (2008), *as modified* (Mar. 12, 2008); *see also* Cal. Civ. Code § 1598 ("Where a contract has but a single object, and such object is unlawful, whether in whole or in part, or wholly impossible of performance . . . the entire contract is void."). As we explain next, however, hiQ has raised at least serious questions in support of its position that its activities are lawful under the CFAA.

authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished" by fine or imprisonment. 18 U.S.C. § 1030(a)(2)(C). Further, "[a]ny person who suffers damage or loss by reason of a violation" of that provision may bring a civil suit "against the violator to obtain compensatory damages and injunctive relief or other equitable relief," subject to certain conditions not relevant here. 18 U.S.C. § 1030(g). The term "protected computer" refers to any computer "used in or affecting interstate or foreign commerce or communication," 18 U.S.C. § 1030(e)(2)(B)—effectively any computer connected to the Internet, *see United States v. Nosal (Nosal II)*, 844 F.3d 1024, 1050 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 314 (2017)—including servers, computers that manage network resources and provide data to other computers. LinkedIn's computer servers store the data members share on LinkedIn's platform and provide that data to users who request to visit its website. Thus, to scrape LinkedIn data, hiQ must access LinkedIn servers, which are "protected computer[s]." *See Nosal II*, 844 F.3d at 1050.

The pivotal CFAA question here is whether once hiQ received LinkedIn's cease-and-desist letter, any further scraping and use of LinkedIn's data was "without authorization" within the meaning of the CFAA and thus a violation of the statute. 18 U.S.C. § 1030(a)(2). If so, hiQ could have no legal right of access to LinkedIn's data and so could not succeed on any of its state law claims, including the tortious interference with contract claim we have held otherwise sufficient for preliminary injunction purposes.

We have held in another context that the phrase "'without authorization' is a non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission." *Nosal II*, 844 F.3d at 1028.

Nosal II involved an employee accessing without permission an employer's private computer for which access permissions in the form of user accounts were required. *Id.* at 1028–29. *Nosal II* did not address whether access can be "without authorization" under the CFAA where, as here, prior authorization is not generally required, but a particular person—or bot—is refused access. HiQ's position is that *Nosal II* is consistent with the conclusion that where access is open to the general public, the CFAA "without authorization" concept is inapplicable. At the very least, we conclude, hiQ has raised a serious question as to this issue.

First, the wording of the statute, forbidding "access[] . . . without authorization," 18 U.S.C. § 1030(a)(2), suggests a baseline in which access is not generally available and so permission is ordinarily required. "Authorization" is an affirmative notion, indicating that access is restricted to those specially recognized or admitted. *See, e.g.*, Black's Law Dictionary (10th ed. 2014) (defining "authorization" as "[o]fficial permission to do something; sanction or warrant"). Where the default is free access without authorization, in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of "authorization." *Cf. Blankenhorn v. City of Orange*, 485 F.3d 463, 472 (9th Cir. 2007) (characterizing the exclusion of the plaintiff in particular from a shopping mall as "bann[ing]").

Second, even if this interpretation is debatable, the legislative history of the statute confirms our understanding. "If [a] statute's terms are ambiguous, we may use . . . legislative history[] and the statute's overall purpose to illuminate Congress's intent." *Jonah R. v. Carmona*, 446 F.3d 1000, 1005 (9th Cir. 2006).

The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking. *See United States v. Nosal (Nosal I)*, 676 F.3d 854, 858 (9th Cir. 2012) (citing S. Rep. No. 99-432, at 9 (1986) (Conf. Rep.)).

The 1984 House Report on the CFAA explicitly analogized the conduct prohibited by section 1030 to forced entry: "It is noteworthy that section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' . . . ." H.R. Rep. No. 98-894, at 20 (1984); *see also id.* at 10 (describing the problem of "'hackers' who have been able to access (trespass into) both private and public computer systems"). Senator Jeremiah Denton similarly characterized the CFAA as a statute designed to prevent unlawful intrusion into otherwise inaccessible computers, observing that "[t]he bill makes it clear that unauthorized access to a Government computer is a trespass offense, as surely as if the offender had entered a restricted Government compound without proper authorization."[11] 132 Cong. Rec. 27639 (1986) (emphasis added). And when considering amendments to the CFAA two years later, the House again linked computer intrusion to breaking and entering. *See* H.R. Rep. No. 99-612, at 5–6 (1986) (describing "the expanding group of electronic trespassers," who trespass "just as much as if they broke a window and crawled into a home while the occupants were away").

In recognizing that the CFAA is best understood as an anti-intrusion statute and not as a "misappropriation statute,"

[11] The CFAA originally prohibited only unauthorized access to government computers.

Nosal I, 676 F.3d at 857–58, we rejected the contract-based interpretation of the CFAA's "without authorization" provision adopted by some of our sister circuits. *Compare Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 313 (2017) ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA."); *Nosal I*, 676 F.3d at 862 ("We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty."), *with EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583–84 (1st Cir. 2001) (holding that violations of a confidentiality agreement or other contractual restraints could give rise to a claim for unauthorized access under the CFAA); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that a defendant "exceeds authorized access" when violating policies governing authorized use of databases).

We therefore look to whether the conduct at issue is analogous to "breaking and entering." H.R. Rep. No. 98-894, at 20. Significantly, the version of the CFAA initially enacted in 1984 was limited to a narrow range of computers—namely, those containing national security information or financial data and those operated by or on behalf of the government. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102, 98 Stat. 2190, 2190–91. None of the computers to which the CFAA initially applied were accessible to the general public; affirmative authorization of some kind was presumptively required.

When section 1030(a)(2)(c) was added in 1996 to extend the prohibition on unauthorized access to any "protected computer," the Senate Judiciary Committee explained that

the amendment was designed to "to increase protection for the privacy and confidentiality of computer information." S. Rep. No. 104-357, at 7 (emphasis added). The legislative history of section 1030 thus makes clear that the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort. As one prominent commentator has put it, "an authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web." Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1161 (2016). Moreover, elsewhere in the statute, password fraud is cited as a means by which a computer may be accessed without authorization, *see* 18 U.S.C. § 1030(a)(6),[12] bolstering the idea that authorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information.

We therefore conclude that hiQ has raised a serious question as to whether the reference to access "without authorization" limits the scope of the statutory coverage to computer information for which authorization or access permission, such as password authentication, is generally required. Put differently, the CFAA contemplates the existence of three kinds of computer information: (1) information for which access is open to the general public and permission is not required, (2) information for

[12] 18 U.S.C. § 1030(a)(6) provides: "Whoever . . . knowingly and with intent to defraud traffics . . . in any password or similar information through which a computer may be accessed without authorization, if—(A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States; . . . shall be punished as provided in subsection (c) of this section."

which authorization is required and has been given, and (3) information for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed). Public LinkedIn profiles, available to anyone with an Internet connection, fall into the first category. With regard to such information, the "breaking and entering" analogue invoked so frequently during congressional consideration has no application, and the concept of "without authorization" is inapt.

Neither of the cases LinkedIn principally relies upon is to the contrary. LinkedIn first cites *Nosal II*, 844 F.3d 1024 (9th Cir. 2016). As we have already stated, *Nosal II* held that a former employee who used current employees' login credentials to access company computers and collect confidential information had acted "'without authorization' in violation of the CFAA." *Nosal II*, 844 F.3d at 1038. The computer information the defendant accessed in *Nosal II* was thus plainly one which no one could access without authorization.

So too with regard to the system at issue in *Power Ventures*, 844 F.3d 1058 (9th Cir. 2016), the other precedent upon which LinkedIn relies. In that case, Facebook sued Power Ventures, a social networking website that aggregated social networking information from multiple platforms, for accessing Facebook users' data and using that data to send mass messages as part of a promotional campaign. *Id.* at 1062–63. After Facebook sent a cease-and-desist letter, Power Ventures continued to circumvent IP barriers and gain access to password-protected Facebook member profiles. *Id.* at 1063. We held that after receiving an individualized cease-and-desist letter, Power Ventures had accessed Facebook computers "without authorization" and was therefore liable

under the CFAA. *Id.* at 1067–68. But we specifically recognized that "Facebook has tried to limit and control access to its website" as to the purposes for which Power Ventures sought to use it. *Id.* at 1063. Indeed, Facebook requires its users to register with a unique username and password, and Power Ventures required that Facebook users provide their Facebook username and password to access their Facebook data on Power Ventures' platform. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1028 (N.D. Cal. 2012). While Power Ventures was gathering user data that was protected by Facebook's username and password authentication system, the data hiQ was scraping was available to anyone with a web browser.

In sum, *Nosal II* and *Power Ventures* control situations in which authorization generally is required and has either never been given or has been revoked. As *Power Ventures* indicated, the two cases do not control the situation present here, in which information is "presumptively open to all comers." *Power Ventures*, 844 F.3d at 1067 n.2.

Our understanding that the CFAA is premised on a distinction between information presumptively accessible to the general public and information for which authorization is generally required is consistent with our interpretation of a provision of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*,[13] nearly identical to the CFAA provision at issue. *Compare* 18 U.S.C. § 2701(a) ("[W]hoever—(1) intentionally accesses without

[13] The Stored Communications Act, enacted as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, provides privacy protections for e-mail and other electronic communications by limiting the ability of the government to compel disclosure by internet service providers.

authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . unauthorized access to a wire or electronic communication . . . shall be punished . . . .") *with* 18 U.S.C. § 1030(a)(2)(C) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished . . . ."). "The similarity of language in [the SCA and the CFAA] is a strong indication that [they] should be interpreted *pari passu*." *Northcross v. Bd. of Educ. of Memphis City Schools*, 412 U.S. 427, 428 (1973); *see also United States v. Sioux*, 362 F.3d 1241, 1246 (9th Cir. 2004).

Addressing the "without authorization" provision of the SCA, we have distinguished between public websites and non-public or "restricted" websites, such as websites that "are password-protected . . . or require the user to purchase access by entering a credit card number." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002); *see also id.* at 879 n.8. As we explained in *Konop*, in enacting the SCA, "Congress wanted to protect electronic communications that are configured to be private" and are "'not intended to be available to the public.'" *Id.* at 875 (quoting S. Rep. No. 99-541, at 35–36 (1986)). The House Committee on the Judiciary stated, with respect to the section of the SCA at issue, section 2701, that "[a] person may reasonably conclude that a communication is readily accessible to the general public if the . . . means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy." H.R. Rep. No. 99-647, at 62 (1986). The Committee further explained that "electronic communications which the

service provider attempts to keep confidential would be protected, while the statute would impose no liability for access to features configured to be readily accessible to the general public." *Id.* at 63.

Both the legislative history of section 1030 of the CFAA and the legislative history of section 2701 of the SCA, with its similar "without authorization" provision, then, support the district court's distinction between "private" computer networks and websites, protected by a password authentication system and "not visible to the public," and websites that are accessible to the general public.

Finally, the rule of lenity favors our narrow interpretation of the "without authorization" provision in the CFAA. The statutory prohibition on unauthorized access applies both to civil actions and to criminal prosecutions—indeed, "§ 1030 is primarily a criminal statute." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009). "Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies." *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). As we explained in *Nosal I*, we therefore favor a narrow interpretation of the CFAA's "without authorization" provision so as not to turn a criminal hacking statute into a "sweeping Internet-policing mandate." *Nosal I*, 676 F.3d at 858; *see also id.* at 863.

For all these reasons, it appears that the CFAA's prohibition on accessing a computer "without authorization" is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer. It is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without

authorization under the CFAA. The data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using such an authorization system. HiQ has therefore raised serious questions about whether LinkedIn may invoke the CFAA to preempt hiQ's possibly meritorious tortious interference claim.[14]

We note that entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply: state law trespass to chattels claims may still be available.[15] And other causes of action, such as copyright

[14] LinkedIn asserts that the illegality of hiQ's actions under the CFAA is also grounds for holding (1) that hiQ's injuries are not cognizable as irreparable harm, (2) that hiQ's contracts are illegal and so their breach cannot give rise to a cognizable tortious interference with contract claim, and (3) that LinkedIn has a legitimate business interest in asserting its rights under federal law that justifies its interference with hiQ's contracts. *See supra* n.10. These contentions are insufficient at this stage for the same reasons LinkedIn's CFAA preemption position does not preclude preliminary injunctive relief.

[15] LinkedIn's cease-and-desist letter also asserted a state common law claim of trespass to chattels. Although we do not decide the question, *see supra* pp. 17–18, it may be that web scraping exceeding the scope of the website owner's consent gives rise to a common law tort claim for trespass to chattels, at least when it causes demonstrable harm. *Compare eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) (finding that eBay had established a likelihood of success on its trespass claim against the auction-aggregating site Bidder's Edge because, although eBay's "site is publicly accessible," "eBay's servers are private property, conditional access to which eBay grants the public," and Bidder's Edge had exceeded the scope of any consent, even if it did not cause physical harm); *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 437–38 (2d Cir. 2004) (holding that a company that scraped a competitor's website to obtain data for marketing purposes likely committed trespass to chattels, because scraping could—although it did not yet—cause physical harm to the plaintiff's computer servers); *Sw. Airlines Co. v. FareChase, Inc.*, 318 F. Supp. 2d 435, 442 (N.D. Tex.

infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy, may also lie. *See, e.g.*, *Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 561 (S.D.N.Y. 2013) (holding that a software company's conduct in scraping and aggregating copyrighted news articles was not protected by fair use).

D. Public Interest

Finally, we must consider the public interest in granting or denying the preliminary injunction. Whereas the balance of equities focuses on the parties, "[t]he public interest inquiry primarily addresses impact on non-parties rather than parties," and takes into consideration "the public consequences in employing the extraordinary remedy of injunction." *Bernhardt v. Los Angeles Cty.*, 339 F.3d 920, 931–32 (9th Cir. 2003) (citations omitted).

As the district court observed, each side asserts that its own position would benefit the public interest by maximizing the free flow of information on the Internet. HiQ points out that data scraping is a common method of gathering information, used by search engines, academic researchers, and many others. According to hiQ, letting

---

2004) (holding that the use of a scraper to glean flight information was unauthorized as it interfered with Southwest's use and possession of its site, even if the scraping did not cause physical harm or deprivation), *with Ticketmaster Corp. v. Tickets.Com, Inc.*, No. 2:99-cv-07654-HLH-VBK, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003) (holding that the use of a web crawler to gather information from a public website, without more, is insufficient to fulfill the harm requirement of a trespass action); *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1364 (2003) (holding that "trespass to chattels is not actionable if it does not involve actual or threatened injury" to property and the defendant's actions did not damage or interfere with the operation of the computer systems at issue).

established entities that already have accumulated large user data sets decide who can scrape that data from otherwise public websites gives those entities outsized control over how such data may be put to use.

For its part, LinkedIn argues that the preliminary injunction is against the public interest because it will invite malicious actors to access LinkedIn's computers and attack its servers. As a result, the argument goes, LinkedIn and other companies with public websites will be forced to choose between leaving their servers open to such attacks or protecting their websites with passwords, thereby cutting them off from public view.

Although there are significant public interests on both sides, the district court properly determined that, on balance, the public interest favors hiQ's position. We agree with the district court that giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest.

Internet companies and the public do have a substantial interest in thwarting denial-of-service attacks[16] and blocking abusive users, identity thieves, and other ill-intentioned actors. But we do not view the district court's injunction as opening the door to such malicious activity. The district

[16] In a denial-of-service (DoS) attack, an attacker seeks to prevent legitimate users from accessing a targeted computer or network, typically by flooding the target with requests and thereby overloading the server.

court made clear that the injunction does not preclude LinkedIn from continuing to engage in "technological self-help" against bad actors—for example, by employing "anti-bot measures to prevent, *e.g.*, harmful intrusions or attacks on its server." Although an injunction preventing a company from securing even the public parts of its website from malicious actors would raise serious concerns, such concerns are not present here.[17]

The district court's conclusion that the public interest favors granting the preliminary injunction was appropriate.

CONCLUSION

We **AFFIRM** the district court's determination that hiQ has established the elements required for a preliminary injunction and remand for further proceedings.

WALLACE, Circuit Judge, specially concurring:

I concur in the majority opinion. I write separately to express my concern that "in some cases, parties appeal orders granting or denying motions for preliminary injunctions in order to ascertain the views of the appellate court on the merits of the litigation." *Sports Form, Inc. v. United Press Int'l, Inc.*, 686 F.2d 750, 753 (9th Cir. 1982); *see also California v. Azar*, 911 F.3d 558, 583–84 (9th Cir. 2018). For example, here LinkedIn's counsel suggested that we should address the CFAA question in this appeal for

---

[17] We note that LinkedIn has not specifically challenged the scope of the injunction.

"pragmatic reason[s]" because it "is going to be a significant issue on remand no matter what happens to this injunction."

I emphasize that appealing from a preliminary injunction to obtain an appellate court's view of the merits often leads to "unnecessary delay to the parties and inefficient use of judicial resources." *Sports Form*, 686 F.2d at 753. These appeals generally provide "little guidance" because "of the limited scope of our review of the law" and "because the fully developed factual record may be materially different from that initially before the district court." *Id.*

The district court here also stayed any effort to prepare the case for trial pending the appeal of the preliminary injunction. We have repeatedly admonished district courts not to delay trial preparation to await an interim ruling on a preliminary injunction. *See, e.g.*, *California*, 911 F.3d at 583–84. This case could have well proceeded to a disposition on the merits without the delay in processing the interlocutory appeal. Given the purported urgency of the case's resolution, the parties might "have been better served to pursue aggressively" its claims in the district court, "rather than apparently awaiting the outcome of this appeal" for nearly two years. *Id.* at 584 (citation omitted).

Addendum B
Statutory Addendum

KeyCite Yellow Flag - Negative Treatment
Proposed Legislation

United States Code Annotated
Title 18. Crimes and Criminal Procedure (Refs & Annos)
Part I. Crimes (Refs & Annos)
Chapter 47. Fraud and False Statements (Refs & Annos)

18 U.S.C.A. § 1030

§ 1030. Fraud and related activity in connection with computers

Effective: November 16, 2018
Currentness

(a) Whoever--

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

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

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

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

(C) information from any protected computer;

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

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

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

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

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss. [1]

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

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

(B) such computer is used by or for the Government of the United States; [2]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),[3] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

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

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

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

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

(III) physical injury to any person;

(IV) a threat to public health or safety;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(e) As used in this section--

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

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

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

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

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

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

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

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

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

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

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

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

(G) the Securities Investor Protection Corporation;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

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

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

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

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section [5]

CREDIT(S)

(Added Pub.L. 98-473, Title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190; amended Pub.L. 99-474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub.L. 100-690, Title VII, § 7065, Nov. 18, 1988, 102 Stat. 4404; Pub.L. 101-73, Title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub.L. 101-647, Title XII, § 1205(e), Title XXV, § 2597(j), Title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub.L. 103-322, Title XXIX, § 290001(b) to (f), Sept. 13, 1994, 108 Stat. 2097-2099; Pub.L. 104-294, Title II, § 201, Title VI, § 604(b)(36), Oct. 11, 1996, 110 Stat. 3491, 3508; Pub.L. 107-56, Title V, § 506(a), Title VIII, § 814(a)-(e), Oct. 26, 2001, 115 Stat. 366, 382-384; Pub.L. 107-273, div. B, Title IV, §§ 4002(b)(1), (12), 4005(a)(3), (d)(3), Nov. 2, 2002, 116 Stat. 1807, 1808, 1812, 1813; Pub.L. 107-296, Title XXII, § 2207(g), formerly Title II, § 225(g), Nov. 25, 2002, 116 Stat. 2158; renumbered § 2207(g), Pub.L. 115-278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178; amended Pub.L. 110-326, Title II, §§ 203, 204(a), 205 to 208, Sept. 26, 2008, 122 Stat. 3561, 3563.)

Notes of Decisions (274)

Footnotes

1 So in original. The period probably should be a semicolon.

2 So in original. Probably should be followed by “or”.

3 So in original. The comma probably should not appear.

4 So in original. Probably should be “subclause”.

5 So in original. A period probably should appear.

18 U.S.C.A. § 1030, 18 USCA § 1030

Current through P.L. 116-63.

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 11, 2019.

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

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

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

Dated: October 11, 2019

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