No. 19-

IN THE

Supreme Court of the United States

LINKEDIN CORPORATION,

Petitioner,

v.

HIQ LABS, INC.,

Respondent.

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

PETITION FOR A WRIT OF CERTIORARI

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

ERIC A. SHUMSKY
ORRICK HERRINGTON & SUTCLIFFE LLP
1152 15th Street, NW
Washington, DC 20005
(202) 339-8400

BRIAN P. GOLDMAN
ORRICK HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105
(415) 773-5700

DONALD B. VERRILLI, JR.
Counsel of Record
JONATHAN S. MELTZER
MUNGER, TOLLES & OLSON LLP
1155 F Street NW, 7th Floor
Washington, DC 20004
(202) 220-1100
donald.verrilli@mto.com

JONATHAN H. BLAVIN
ROSEMARY T. RING
NICHOLAS D. FRAM
MARIANNA Y. MAO
MUNGER, TOLLES & OLSON LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105
(415) 512-4000

Counsel for Petitioner

QUESTION PRESENTED

Whether a company that deploys anonymous computer "bots" to circumvent technical barriers and harvest millions of individuals' personal data from computer servers that host public-facing websites—even after the computer servers' owner has expressly denied permission to access the data—"intentionally accesses a computer without authorization" in violation of the Computer Fraud and Abuse Act.

PARTIES TO THE PROCEEDING AND CORPORATE DISCLOSURE STATEMENT

Petitioner LinkedIn Corporation was appellant in the court of appeals and defendant in the district court. LinkedIn Corporation is a wholly owned subsidiary of Microsoft Corporation ("Microsoft"). Microsoft is a publicly traded company. No person or entity holds 10% or more of Microsoft's outstanding common stock.

Respondent hiQ Labs, Inc. was appellee in the court of appeals and plaintiff in the district court.

RELATED PROCEEDINGS

The proceedings directly related to this petition are:

- *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, No. 17-16783 (9th Cir. 2019), *rehearing en banc denied* (9th Cir. Nov. 8, 2019)
- *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, No.17-cv-03301-EMC (N.D. Cal. 2017)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

FEDERAL STATUTES

LEGISLATIVE MATERIALS

TREATISES

OTHER AUTHORITIES

PETITION FOR A WRIT OF CERTIORARI

LinkedIn Corporation ("LinkedIn") respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit.

OPINIONS BELOW

The Ninth Circuit's opinion affirming the judgment of the district court and remanding (Pet. App. 1a) is reported at 938 F.3d 985. The Ninth Circuit's order denying panel rehearing and rehearing en banc (Pet. App. 77a) is unreported. The district court's opinion granting hiQ a preliminary injunction (Pet. App. 39a) is reported at 273 F. Supp. 3d 1099.

JURISDICTION

The Ninth Circuit entered judgment on September 9, 2019, and denied a timely rehearing petition on November 8, 2019. Pet. App. 77a. On January 23, 2020, the Court extended the time to file this petition to March 9, 2020. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

STATUTORY PROVISION INVOLVED

The relevant provision of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is reproduced in its entirety in the appendix to this petition. Pet. App. 79a.

INTRODUCTION

This case raises a question of fundamental importance: whether the Computer Fraud and Abuse Act (CFAA) protects a public-facing website [1] from data-scraping by companies that surreptitiously harvest and exploit the personal data of the website's users for their own purposes.

LinkedIn is a professional social networking service that offers registered members the ability to create profiles that showcase their skills and accomplishments and to connect with other professionals to further their careers. When members do so, they entrust their personal information—such as education, work history, skills, test scores, volunteer activities, and organizational affiliations—to LinkedIn, which is then stored on LinkedIn's computer servers.

In making their information available on LinkedIn's website, LinkedIn's members do not relinquish control of all uses of that information to all persons for all time. To the contrary, LinkedIn gives its members considerable control over how their personal information will be used. Members can restrict public access to that information in various ways, and can change their minds as their needs or preferences change. And they can terminate their relationship with LinkedIn at any time, and thereby preclude further access to their information on LinkedIn's website and further use of that information by LinkedIn.

Over the years, LinkedIn has sought to develop a relationship of trust with its members by respecting the choices they make about how their personal information will be used. That relationship is integral to LinkedIn's

---

[1] The term "public-facing website" refers to a website that makes information available to visitors without the use of a password.

success, and LinkedIn works hard to protect it. But it is constantly threatened by entities that surreptitiously deploy anonymous computer "bots" that seek to scrape—*i.e.*, harvest—massive volumes of personal data from LinkedIn's servers. Many of those third parties repackage and use LinkedIn member data without permission from LinkedIn or its members, often in violation of the members' expectations of privacy and to their detriment. LinkedIn has established technological barriers to counter this unauthorized activity, but data scrapers in turn constantly update their own technologies to overcome these technological barriers.

One such entity is Respondent hiQ, which surreptitiously employs bots on a massive scale in a systematic effort to evade LinkedIn's barriers and to amass its own database of information about LinkedIn's members. hiQ uses that scraped data in a commercial product that operates as an early warning system for employers, alerting them when their employees are likely looking for a new job.

The CFAA, a computer trespass statute, imposes civil and criminal liability on a party for accessing a qualifying computer "without authorization." 18 U.S.C. § 1030(a)(2). For decades, website operators have invoked this statute successfully to stop systematic third-party scraping like that undertaken by hiQ. In this case, however, the Ninth Circuit held that hiQ did not intentionally access a computer server "without authorization," even though LinkedIn had employed technical measures designed to deny access to hiQ's data-scraping bots and sent a cease-and-desist letter informing hiQ that its bots did not have permission to access LinkedIn's servers. Pet. App. 22a-39a. In an unprecedented ruling, the Ninth Circuit concluded that public-facing websites are categorically ineligible to invoke the CFAA. According to the Ninth Circuit, because certain information

available on LinkedIn's website can be viewed by the public without submitting a password, LinkedIn had never granted—and therefore could not revoke—"authorization" to anyone, including surreptitious scrapers like hiQ.

The Ninth Circuit's opinion breaks sharply with every federal court that has interpreted Section 1030(a). The First Circuit and all district courts to consider the issue have uniformly held that Section 1030(a) applies, in accordance with its unambiguous text, to entities that scrape data from public-facing websites when the website owner has denied authorization for such scraping. And the conflict created by the Ninth Circuit's decision is not a tolerable one. Because the Internet is ubiquitous, the exact same conduct by the exact same entities will be subject to CFAA liability in some parts of the country and not others. By the same token, leading technology companies will be able to invoke the CFAA to protect themselves and their users in some parts of the country but not in the Ninth Circuit (where many of them are headquartered).

In addition to creating a circuit conflict and disrupting this prior uniformity, the Ninth Circuit's opinion presents an issue of exceptional importance. The need to protect personal data from the threat of unauthorized exploitation becomes more pressing every day. hiQ is far from alone in engaging in such activities. For example, recent reports have highlighted the actions of another company, Clearview, which has deployed bots to engage in the systematic scraping of social media websites to amass a database of more than three billion photos, without the consent of those websites or their users. Clearview has exploited that scraped data to support a powerful facial recognition technology that it has already licensed to more than 600 law enforcement agen-

cies and offered to some private individuals and companies.[2] And Clearview will surely not be the last company to engage in such conduct.

In the face of these increasing threats, the Ninth Circuit's decision has denied operators of public-facing websites a critical means of protecting user data from unauthorized third-party scrapers. Experts have already noted that the Ninth Circuit's decision "eviscerated the legal argument that" websites have used to block entities like hiQ and Clearview.[3] Review of that decision is plainly warranted.

STATEMENT

A. The Computer Fraud and Abuse Act

The CFAA is a computer trespass statute. Specifically, it creates criminal and civil liability for "[w]hoever ... intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). A "protected computer," in turn, is any computer "used in or affecting interstate or foreign commerce or communication," 18 U.S.C. § 1030(e)(2)(B)—in short, any computer connected to the Internet. The CFAA also provides a private right of action for "[a]ny

---

[2] Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, The New York Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, The New York Times (March 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.

[3] Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, The New York Times (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html (quoting director of Stanford Internet Observatory Alex Stamos).

person who suffers damage or loss [greater than $5,000] by reason of a violation of this section." 18 U.S.C. § 1030(g).

Although the CFAA was originally enacted in 1984, the provision at issue in this case, § 1030(a)(2), was adopted in its current form in 1996, when use of the Internet was already widespread. *See* Pub. L. No. 104-294, § 201, 110 Stat 3488, 3492 (1996). The 1996 amendment expanded the scope of § 1030(a)(2), which had previously applied only to unauthorized attempts to obtain certain financial records. *See* 18 U.S.C. § 1030(a)(2) (1994). As amended, the provision covered the act of obtaining *any* "information," financial or otherwise, from *any* protected computer "without authorization." *See* 18 U.S.C. § 1030(a)(2) (2000). *See also* S. Rep. No. 104-357, at 8-9 (1996) (recognizing that "accessing" a "publicly available" computer "via [a] World Wide Web site" without authorization could trigger CFAA liability).

After passage of the 1996 amendment, courts routinely held that Section 1030(a)(2) liability attached to accessing websites without authorization, even where information was publicly available without use of a password. *See, e.g.*, *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003). Those courts found that using bots in ways that were antithetical to the business interests of a publicly-available website operator or to the privacy interests of a website's users, after those websites had unequivocally withdrawn authorization for such access, violated the CFAA.

Against this backdrop, Congress amended the CFAA in 2001 and 2008, each time to *expand* the scope of online conduct that the CFAA would cover. As lower courts continued to apply the CFAA to impose liability when bots operated by third parties accessed public-facing websites

"without authorization," Congress thus gave no indication that courts were misinterpreting the statute's scope.

B. Factual Background

1. Petitioner LinkedIn is a professional networking service that allows its members to create, manage, and share their professional identities and interests online. 5ER-824.[4] Members do so by creating a "profile" containing professional information that appears on LinkedIn's website. The information that members entrust to LinkedIn—including work and education history, profile narratives, and photographs—is central to its business. LinkedIn's significant investment in its platform and its member community has resulted in over 500 million members signing up for its service worldwide. 5ER-824.

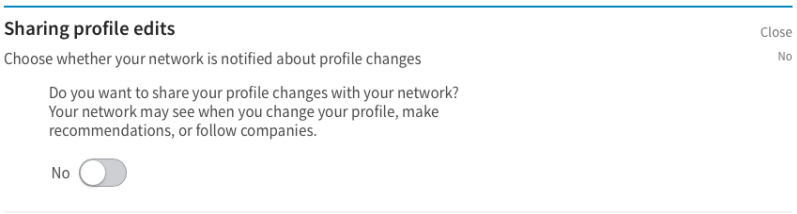
LinkedIn's members can use a variety of user controls and privacy settings to choose what information they share on their profiles, with whom they share it, and when to remove it from LinkedIn's servers and the Internet. When LinkedIn members remove information from their profiles, LinkedIn in turn removes that information from its servers. And when a user decides to close her LinkedIn account, that account, and the information in it, is removed from LinkedIn and the Internet. 4ER-764.

LinkedIn also enables its members to control how their personal information is shared and with whom. To this end, LinkedIn offers its members a "Do Not Broadcast" feature, which allows members to change their profiles without alerting others that any changes were made. Pet. App. 3a. This feature was specifically developed in response to employees' concerns about employers monitoring changes to their LinkedIn profiles. 3ER-427.

---

[4] "ER" cites are to the Appellant's Excerpts of Record on appeal in the Ninth Circuit.

And LinkedIn members can access their privacy settings and select this feature at any time, as demonstrated by this screenshot:



3ER-427. More than 50 million LinkedIn members have elected to employ the "Do Not Broadcast" feature, including 20 percent of active members who updated their profiles between July 2016 and July 2017. Pet. App. 3a.[5]

2. To protect its members' data and its business, LinkedIn actively works to prevent unauthorized data-scraping from its computers. Scraping is the automated, mass-extraction of data directly from a website's servers. Scraping is frequently performed by bots: computer programs that "query other computers over the Internet in order to obtain a significant amount of information." *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1060 n.2 (N.D. Cal. 2000).

Data-scraping bots can be employed for a variety of purposes. For example, search engines use bots to access and index information on websites. Pursuant to its privacy policy, LinkedIn has authorized certain "white

[5] Consistent with this feature, and in notable contrast to hiQ's approach, LinkedIn's "Recruiter" product—which enables recruiters to view information regarding prospective employees they may be interested in recruiting— "does not provide alerts about profile changes made by LinkedIn members who select the 'Do Not Broadcast' setting." Pet. App. 13a n.7.

listed" bots (*e.g.*, those employed by search engines such as Google and Bing) to index some member profile information. 4ER-761. LinkedIn's policy benefits members by allowing them to be found via search engines, and to thus present their professional information to the world in the manner of their choice. LinkedIn informs members that data on their "public-facing" profiles may be indexed by search engines, and allows them to limit which parts of their profiles are indexed, or opt out of being indexed altogether. 4ER-762, 4ER-772.

In contrast, third parties such as hiQ surreptitiously deploy bots without permission to access LinkedIn's computer servers and copy personal data that members have entrusted to LinkedIn. 3ER-759-761. These bots operate on a massive scale, scraping and analyzing data on a magnitude that even a vast army of human viewers could not replicate.[6] Some go so far as to make complete mirror-image copies of LinkedIn's website. Once the data is scraped from LinkedIn's servers, the scraper is able to repurpose that data in any manner the scraper desires—for instance, by combining it with data found elsewhere (such as photographs, telephone numbers or addresses), or selling it to the highest bidder.

---

[6] Although bots harvest data that is viewable by individual computer users, the massive scale of bot scraping renders it different in kind from individual human viewing. Bots can make thousands of server requests per second, "far in excess of what a human can accomplish." *eBay*, 100 F. Supp. 2d at 1061. While individuals are aware that their personal data can be viewed on publicly-available websites, efforts to manually harvest such data would be "difficult and costly," providing a "practical" limitation on such efforts. *United States v. Jones*, 565 U.S. 400, 429 (2012) (Alito, J., concurring in the judgment). But bots, which make "monitor[ing] and catalogu[ing] every single" profile change "easy and cheap," remove any such practical constraint. *Id.* at 429-30.

Website owners use technology to prevent unauthorized bots from accessing their servers. One method, employed by LinkedIn and countless other website owners, is to use automated countermeasures that identify and block unauthorized bots. LinkedIn invests millions of dollars annually on such countermeasures, which block roughly 95 million bot access attempts per day. 4ER759-761. But blocking unauthorized bots is a perpetual game of cat and mouse. Those who deploy bots that have been stymied by LinkedIn's technical barriers routinely redesign their bots to evade those barriers—including by masking their identities. 3ER-433.

As a result, LinkedIn also resorts to legal action. LinkedIn's User Agreement expressly prohibits using automated software—including "bots"—to access and scrape member data from LinkedIn's computers. 4ER-761-762. LinkedIn "reserves the right to restrict, suspend, or terminate" the access of those found to abuse their access privileges, including by scraping LinkedIn's computers with bots, 4ER-772, 4ER-775, and has sent cease and desist letters to offenders putting them on clear notice of such terms. And as particularly relevant here, LinkedIn also relies on the CFAA's prohibition against unauthorized access to computer servers.

3. hiQ runs a business that free rides on LinkedIn's investment and entrepreneurship and disregards LinkedIn members' interests. hiQ's bots continuously mass-scrape member profiles from LinkedIn's servers without the consent of LinkedIn or its members, and hiQ then repackages that data to sell to its clients. 4ER-766. The bots use various methods to evade LinkedIn's technical measures, including by using anonymous IP addresses that mask what they are doing. In so doing, they circumvent "LinkedIn's measures to prevent use of bots and implementation of IP address blocks." Pet. App. 61a; 4ER-766.

After surreptitiously scraping data from LinkedIn's servers, hiQ incorporates that data into the two products that it sells to its clients: (1) Keeper, which identifies for employers which employees are most likely to be recruited away (by assigning each user a "flight score"); and (2) Skill Mapper, which summarizes employees' skills in the aggregate. Pet. App. 5a-6a. hiQ introduced no evidence that these services benefit LinkedIn members, and it is easy to understand how they might not: if an employer believes an employee is about to leave, the employer could terminate the employee, diminish her role, or refuse to give her access to confidential information, even if she actually has no intention of leaving.

Although LinkedIn's User Agreement and Privacy Policy limit how LinkedIn can use the data that members entrust to it, LinkedIn members have not given their data to third parties like hiQ, and hiQ has no contractual relationship with LinkedIn's members. Nor does hiQ's Keeper product respect members' use of LinkedIn's "Do Not Broadcast" feature. *See* Pet. App. 46a; *supra* p. 8 n. 5. hiQ simply uses the data in whatever way it finds advantageous, with no regard for the privacy interests of LinkedIn members. LinkedIn members unsurprisingly have complained to LinkedIn when information that they wished not to share has been scraped and made available on third party websites. 3ER-431.

C. Proceedings Below

1. LinkedIn sent hiQ a cease-and-desist letter on May 23, 2017, demanding that hiQ stop accessing LinkedIn's servers to scrape LinkedIn member data. The letter explained that hiQ's use of bots to scrape data circumvented LinkedIn's technical protection measures and violated LinkedIn's User Agreement, and that any further

access to LinkedIn's servers would be "without authorization" under the CFAA. The letter also explained that LinkedIn was implementing additional "technical measures to prevent hiQ from accessing, and assisting others to access, LinkedIn's site." 4ER-743.

In response, hiQ brought this suit. hiQ's complaint alleged four affirmative claims for relief based on California tort and constitutional law, and sought a declaratory judgment that LinkedIn could not lawfully invoke the CFAA against it to stop its bot-based scraping. Pet. App. 42a-43a. hiQ also sought a temporary restraining order, which was converted into a motion for a preliminary injunction. Pet. App. 7a-8a. The district court granted that motion. Pet. App. 75a-76a. It held that hiQ had demonstrated "serious questions" about one of its claims for affirmative relief under California law and it rejected as a matter of law LinkedIn's argument that LinkedIn's invocation of the CFAA preempted hiQ's affirmative state law claims. Pet. App. 49a-64a, 69a-72a.

2. The Ninth Circuit affirmed. It recognized that "to scrape LinkedIn data, hiQ must access LinkedIn servers, which are 'protected computer[s]'" under the CFAA. Pet. App. 23a. It further noted that 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." Pet. App. 23a. But it held that LinkedIn could not rely on the CFAA as a defense.

In interpreting the text of the statute, the Ninth Circuit observed that the phrase "without authorization" means "accessing a protected computer without permission." Pet. App. 23a. The court then held, however, that the CFAA has no application in situations where a "prior authorization is not generally required, but a particular

person—or bot—is refused access." Pet. App. 24a. According to the court, the CFAA's prohibition of access "'without authorization' … suggests a baseline in which access is not generally available and so permission is ordinarily required …. 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.'" Pet. App. 24a. Although the information that hiQ wanted to access on LinkedIn's computers was protected by numerous technical measures designed to prevent unauthorized bot access, because LinkedIn did not employ a password system, the Ninth Circuit determined that "permission is not required." Pet. App. 28a. As a result, even though LinkedIn's servers are its private property, LinkedIn could not revoke hiQ's permission to access them, and could not render hiQ's access "without authorization." Pet. App. 28a. This textual interpretation, the court acknowledged, may be "debatable." Pet. App. 24a.

With respect to the user data and privacy implications of the injunction, the Ninth Circuit concluded that over 500 million 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." Pet App. 13a.

The Ninth Circuit denied LinkedIn's petition for panel rehearing or rehearing en banc. Pet. App. 77a-78a. This petition for certiorari followed.

REASONS FOR GRANTING THE PETITION

The Ninth Circuit has issued a sweeping ruling that public-facing websites are categorically unable to invoke Section 1030(a)(2) of the Computer Fraud and Abuse Act. That ruling creates a direct circuit conflict and

breaks sharply from the established consensus in the lower courts. It lacks any basis in the statutory text, and instead reflects a policy judgment—favoring a data-scraper's access to a website and the user data on it at the expense of privacy protections established by the website operator—that is flatly at odds with the statute Congress enacted.

The issue whether public-facing websites can invoke Section 1030(a)(2) is a recurring one that is likely to arise with increasing frequency because of the critical importance of protecting the privacy of user data to citizens and website operators alike. And there is a particularly pressing need for a uniform national rule. Website operators serve the entire nation over the Internet. Absent intervention by this Court, their ability to invoke the CFAA will depend on the happenstance of where their servers or their principal places of business are located. For the many Internet companies located in the Ninth Circuit, the effect of the ruling will be particularly pernicious. They will no longer be able to rely on the CFAA to protect the privacy of data provided by their users and to prevent free riding by parasitic would-be competitors whose actions erode user trust on the platform. Indeed, their efforts to protect their businesses and their users' privacy through technological means, like the ones LinkedIn employed here, will now trigger a barrage of state law claims like the ones hiQ asserted in this case. And far from fostering the free flow of information on the Internet, the Ninth Circuit's ruling may well have the perverse consequence of limiting publicly available information by forcing websites to place more information behind password walls to protect their business and the privacy of their users. For these reasons, review by this Court is manifestly warranted.

A. The Decision of the Court of Appeals Creates a Clear and Direct Circuit Conflict that Requires this Court's Resolution

1. Section 1030(a)(2) of the CFAA makes it unlawful to "intentionally access[] a computer without authorization." The Ninth Circuit has determined that this clear statutory prohibition is categorically inapplicable to public-facing websites that do not limit access to the website's contents on the basis of a password system or similar form of comprehensive access restriction. According to the court of appeals, there can be no access "without authorization" unless a website operator provides for access "with authorization" via a password or similar means. On this view, a website operator who makes a website generally available to the public is not "authoriz[ing]" anyone's access, and therefore cannot withhold or revoke anyone's authorization within the meaning of the CFAA. That is true even where, as here, a website owner directly notifies a scraper in a cease-and-desist letter that it does not have permission to access the website's computer servers, and the scraper nevertheless persists in doing so by circumventing technical barriers erected by the website owner.

The Ninth Circuit's interpretation of § 1030(a) directly conflicts with the First Circuit's decision in *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003). In that case, the plaintiff and a competitor operated rival travel websites. The competitor hired a company to use a bot to scrape pricing information from the plaintiff's publicly-accessible website. *Id.* at 60-61. The competitor then used that information to undercut the plaintiff's pricing. *Id.*

The First Circuit affirmed the district court's grant of a preliminary injunction against the competitor under

the CFAA. In doing so, the First Circuit expressly rejected the premise on which the Ninth Circuit's decision in this case rests: "that there is a 'presumption' of open access to Internet information." *Id*. at 63. To the contrary, the First Circuit held, "[t]he CFAA, after all, is primarily a statute imposing limits on access and *enhancing control by information providers*." *Id.* (emphasis added). To determine whether access to a website is authorized, the First Circuit explained, a court should look to what the owner of a publicly-accessible website has done and said: "we think that the public website provider can easily spell out explicitly what is forbidden." *Id.* As the Court noted, if the publicly-accessible website owner "wants to ban scrapers, let it say so." *Id.*

The difference between the interpretation of Section 1030(a) in the First Circuit and in the Ninth Circuit is outcome determinative. Under First Circuit law, if the owner of a publicly-accessible website wishes to deny a party scraping information access to its website, it need only inform that party that it is not authorized to scrape data from its computer servers. So long as an "explicit prohibition [is] in place," then "[a] lack of authorization [can] be established." *Id.* at 62.

That is precisely what LinkedIn did in this case. It put in place technical measures to prevent bots like hiQ's from accessing LinkedIn's servers. When hiQ nonetheless continued to use bots to circumvent those measures and scrape information, LinkedIn sent a cease-and-desist letter and erected additional technical measures specifically targeted at blocking further access by hiQ's bots. Pet. App. 7a. In the First Circuit, such actions would have rendered hiQ's continued attempts to scrape data from LinkedIn's website "without authorization" for purposes of the CFAA. *See EF Cultural Travel*, 318 F.3d at 62-63. In contrast, the decision below has established

a blanket rule that so long as a website contains "information for which access is open to the general public," the website's owner *cannot* withdraw permission and render a user's activity "without authorization." Pet. App. 27a-28a. Under those circumstances, the Ninth Circuit has held, the CFAA's "concept of 'without authorization' is inapt." Pet. App. 28a.[7]

2. The Ninth Circuit's decision also breaks sharply with the established two-decade consensus in the lower federal courts that the CFAA applies, according to its plain terms, to unauthorized scraping of data from public-facing websites. *See QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595-97 (E.D. Pa. 2016) (following CFAA cases that have concluded that "a web-user acts without 'authorization' when it crawls a public website," citing, *e.g.*, *EF Cultural Travel*, 318 F.3d at 62–63); *Couponcabin LLC v. Savings.com, Inc.*, No. 14-CV-39, 2016 WL 3181826, at *3-4 (N.D. Ind. June 8, 2016) ("CFAA liability may exist in certain situations where a party's authorization to access electronic data—including publicly accessible electronic data—has been affirmatively rescinded or revoked"); *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1184 (N.D. Cal. 2013) (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.

---

[7] While *EF Cultural Travel* focused on the "exceeds authorized access" prong of § 1030(a), its holding applies with equal force to the "without authorization" prong of that provision. This is for the simple reason that the court's holding turned on the meaning of "a lack of authorization," 318 F.3d at 62, which applies equally to both forms of liability. And, directly relevant here, the opinion states that "[a] lack of authorization could be established by an explicit statement" and that "the public website provider can easily spell out explicitly what is forbidden." *Id.* at 62-63.

Further access by 3Taps after that rescission was 'without authorization.'"); *Sw. Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 437 (N.D. Tex. 2004) (same); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 244, 251 (S.D.N.Y. 2000), *aff'd as modified*, 356 F.3d 393 (2d Cir. 2004) (same); *Ticketmaster LLC v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1102-03, 1113 (C.D. Cal. 2007) (same); *United States v. Lowson*, No. 10-cr-114, 2010 WL 9552416, at *5-*7 (D.N.J. Oct. 12, 2010) (same).

Prior to the decision of the Ninth Circuit in this case, LinkedIn and other companies that operate public-facing websites could rely on a clear rule that protected both website operators and users who provide data to them. The Ninth Circuit's decision upsets that stable understanding and prevents websites from setting and enforcing transparent standards that allow their users to understand how their data will (and will not) be used and made available to third parties.[8]

3. The Ninth Circuit's sharp departure from the existing consensus should be addressed now. Section 1030(a)(2) regulates the Internet, which by nature and design is "an international network." *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 849 (1997). The CFAA is

[8] A recently-filed petition seeks certiorari on the proper interpretation of "exceeds authorized access" under § 1030(a)(2), which has also created a conflict within the courts of appeals. *See Van Buren v. United States*, petition for cert. pending, No. 19-783 (filed Dec. 18, 2019). That case addresses whether a person who has been authorized to access a computer for certain purposes, but then uses that access for other improper purposes, violates § 1030(a)(2). Regardless of whether and how the Court resolves that distinct question, the question of the proper meaning of "without authorization" in § 1030(a)(2) will continue to require this Court's attention.

meant to provide nationwide uniformity in its application to computers connected to the Internet, but so long as this circuit conflict remains in place, it cannot do so.

The consequences of leaving such a conflict in place are substantial. Efforts on the part of website owners like LinkedIn to fight off unauthorized scraping by third-party bots anywhere in the country will immediately subject them to copy-cat litigation in California seeking to impose liability for using technical measures to protect members' data and their own investments. Moreover, the Ninth Circuit's decision will have outsized importance because much of the technology industry is located within the Ninth Circuit. Twitter, Facebook, Craigslist, Yelp, Zillow, and many other websites that feature content that is not password-protected will be unable to prevent third parties under the CFAA from illicitly scraping data, even where that scraping is manifestly against the interest of the website owners and threatens the privacy interests of their users.

If the Ninth Circuit's decision is left in place, technology companies in that Circuit will have no recourse under the CFAA against, for instance, a third-party-scraper employing artificial intelligence to compile a massive database that could allow for instant facial recognition (and possible surveillance) of billions of people, while companies litigating in other circuits will be able to combat such activity. *See supra* pp. 4-5 & nn. 2-3. Incongruities of this kind are likely to arise in numerous contexts. Consider the example of TripAdvisor and Yelp. Both websites include user-generated reviews of restaurants, hotels, and other establishments, and much of their content is available without any login or password. TripAdvisor is headquartered in Massachusetts, while Yelp is headquartered in California. Because of the decision below, competitors could scrape data from Yelp's servers, potentially copying millions of reviews created by and for

Yelp and its users, and Yelp would be left with no recourse under the CFAA to protect its users' data or its years of investment. Meanwhile, TripAdvisor could invoke the CFAA to prevent any competitor from doing the same.

B. The Ninth Circuit's Interpretation of the CFAA is Incorrect

1. The Ninth Circuit's Decision Cannot be Reconciled with the Statute's Text and Structure

The CFAA provides liability for "[w]hoever … intentionally accesses a computer without authorization … and thereby obtains … information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). The decision below acknowledged that the CFAA's "phrase 'without authorization' is a non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission." Pet. App. 23a (internal quotation marks omitted). But the Ninth Circuit then abandoned any recognizable "ordinary meaning" of the terms "authorization" and "permission," reading into those terms a password requirement that simply is not there and that no court had previously recognized.

a. The court of appeals set forth its textual analysis in two short paragraphs. The court first noted that "'[a]uthorization' is an affirmative notion," defined as "'[o]fficial permission to do something; sanction or warrant.'" Pet. App. 24a (quoting Black's Law Dictionary (10th ed. 2014)). It then held that "[w]here the default is free access without authorization," there can be no "authorization" to revoke. *Id.* Thus, according to the Ninth Circuit, because LinkedIn operates a website that allows the public to access some information without a password, it could not *revoke* hiQ's authorization to access the website. As the court below saw it, "in ordinary parlance

one would characterize selective denial of access as a ban, not as a lack of 'authorization.'" *Id.*

That linguistic distinction comports with neither "common parlance" nor common sense. The Smithsonian Museums are open to the public. But if a visitor repeatedly touches the dinosaur bones at the Museum of Natural History, and is kicked out and told not to return, it would be equally accurate to describe that as a "ban" and as a revocation of permission or "authorization" to return. Likewise, banning someone from accessing a website is the same thing, both analytically and linguistically, as denying them authorization to access the website. That is because a ban *is* a denial of authorization. The Ninth Circuit itself defined "authorization" as "official permission." It makes no sense to say that hiQ had permission to access LinkedIn's servers when LinkedIn was employing sophisticated technological barriers to thwart that very access. And when LinkedIn sent its cease-and-desist letter informing hiQ that its bots were not welcome on LinkedIn's website, LinkedIn, in plain terms, withdrew "permission" for hiQ to access its website. Put simply, "where a user is altogether banned from accessing a website," further access is "without authorization." *3Taps*, 964 F. Supp. 2d at 1184.

The Ninth Circuit avoided this commonsense interpretation only by rewriting the CFAA's text, effectively converting the statutory phrase "without authorization" into "without prior authorization in the form of a password or other authentication barrier." *See* Pet. App. 22a-24a. The Ninth Circuit itself acknowledged that the textual basis for reading the statute this way is "debatable." Pet. App. 24a. It is far worse than that. Stripped of the Ninth Circuit's embroidery, the statutory text is clear: a party acts "'without authorization' when it continue[s] to pull data off of [a] website after [the owner] revoked its authorization to access the website. As the 'ordinary,

contemporary, common meaning' of the word indicates … 'authorization' turns on the decision of the 'authority' that grants—or prohibits—access." *3Taps*, 964 F. Supp. 2d at 1183-84.

b. To buttress its counterintuitive reading of the statutory text, the court of appeals pointed out that the CFAA is an "anti-intrusion statute" grounded in trespass law. Pet. App. 25a-26a; *see, e.g.*, H.R. Rep. No. 98-894, at 6, 9-10 (1984) (noting CFAA passed in response to "recent flurry of electronic trespassing incidents"); S. Rep. No. 99-432, at 7 (1986) (equating "unauthorized access" with "a simple trespass offense"); H.R. Rep. No. 99-612, at 5-6 (1986) (equating computer hackers to "trespassers, just ... as if they broke a window and crawled into a home while the occupants were away").

The Ninth Circuit was correct to look to trespass law for guidance but drew precisely the wrong lesson from that body of law. As this Court has explained, "[th]e law of trespass recognizes the interest in possession and control of one's property and for that reason permits exclusion of unwanted intruders." *Oliver v. United States*, 466 U.S. 170, 183 n.15 (1984). Even where a property owner has decided to allow the general public on her property, she retains the ability to exclude "unwanted intruders," and if they return, they do so "without authorization"—*i.e.,* they trespass. *See* 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").

This basic premise of trespass law accords with common understandings. For example, restaurant owners generally allow anyone to enter and dine, thus granting "permission" or "authorization" to the public as a whole. Nonetheless, if a particular owner bans an obnoxious or

abusive patron, the banned person—in "common parlance"—no longer has "authorization," or "permission," to enter the restaurant. And under the law of trespass, the owner of the restaurant has the right to eject the customer and, if need be, sue for trespass if the customer returns thereafter.

But following the Ninth Circuit's tortured logic, when a restaurant has a policy that anyone can enter and place an order, it has determined that no authorization is required. It would therefore lack the authority to revoke a customer's permission to be on the premises, regardless of how long they stay, how much they interfere with others' enjoyment, or how much they damage the restaurant's business. On this view, a private eating club could revoke the "authorization" of one of its members to dine at the establishment, but a restaurant could not prevent a disruptive customer from returning, simply because it never placed a bouncer with a guest list at the door. That is not how the law of trespass—which permits the "exclusion of unwanted intruders," *Oliver*, 466 U.S. at 183 n.15—applies, and it is likewise not how the CFAA should apply. Just as with a restaurant, when a website owner erects technical barriers against bots and sends a cease-and-desist letter making clear that a party does not have permission to access the website, it has revoked any previously-provided authorization. And those actions send a clear message that any further access is "without authorization," leaving no danger of liability to those who access websites without knowing that they lack authorization.

c. The Ninth Circuit's atextual distinction between password-protected and publicly-accessible websites is also inconsistent with the structure of the CFAA. In § 1030(a)(3), which applies to government computers and was adopted at the same time as its neighboring provision § 1030(a)(2), Congress proscribed "intentionally,

without authorization to access any nonpublic [government] computer …, access[ing] such a computer." 18 U.S.C. § 1030(a)(3). Congress inserted the "nonpublic" modifier because Congress understood that "accessing" a "publicly available" computer "via an agency's World Wide Web site" without authorization could otherwise trigger CFAA liability, *see* S. Rep. No. 104-357, at 8-9 (1996). Had Congress wished to likewise limit § 1030(a)(2)'s reach to exclusively nonpublic information, it could have done so. "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 1182–83.

In view of Congress's choice to include a "nonpublic" limitation in a closely adjacent provision but not in Section 1030(a)(2), the Ninth Circuit's decision to add the identical limitation into the latter provision amounted to "invent[ing] a statute rather than interpret[ing] one." *Pasquantino v. United States*, 544 U.S. 349, 359 (2005) (citation omitted); *see also, e.g.*, *Hardt v. Reliance Standard Life Ins. Co.*, 560 U.S. 242, 252 (2010) (where an express limitation was present in one provision and absent in the neighboring provision, "the contrast between these two paragraphs makes clear that Congress knows how to impose express limits" when it so desires).[9]

---

[9] The Ninth Circuit also relied on the Stored Communications Act (SCA), 18 U.S.C. § 2701 et seq., which it described as "nearly identical to the CFAA provision at issue." Pet. App. 30a. The court held that because courts have distinguished between public- and nonpublic-facing websites for purposes of the SCA, the similar language in the CFAA must be read consistently.

But the Ninth Circuit failed to acknowledge one critical difference: the SCA expressly carves out communications "readily accessible to the general public." 18 U.S.C. § 2511(2)(g). The CFAA contains no analogous language. *See 3Taps*, 964 F. Supp. 2d at

d. In contrast to the Ninth Circuit's reading of § 1030(a)(2), LinkedIn's interpretation is faithful to the statutory text and sets forth a clear rule. Where a website owner sets up technical measures to deny a third-party scraper access to its website or sends a cease-and-desist letter, thereby putting the scraper indisputably on notice that access is not authorized, any further efforts to access that website are "without authorization." That interpretation both gives faithful meaning to the words of the CFAA and protects Internet users who lack the requisite intent to access a website "without authorization" from the threat of criminal prosecution or civil liability.

2. The Legislative History Does not Support the Ninth Circuit's Interpretation

Unable to justify its reading of Section 1030(a)(2) on the basis of the statute's text, the Ninth Circuit turned to the legislative history. *See* Pet. App. 24a-27a. But this Court "do[es] not resort to legislative history to cloud a statutory text that is clear." *Ratzlaf v. United States*, 510 U.S. 135, 147–48 (1994); *see Whitfield v. United States*, 543 U.S. 209, 215 (2005). In any event, the legislative history confirms that the Ninth Circuit erred.

To begin with, the court of appeals focused on the *wrong* legislative history. It relied principally on the legislative history of the CFAA's original enactment in 1984 and of a 1986 amendment to support its contention that

---

1183. The presence of a carve-out for "public" communications in the SCA, and its absence in the CFAA, confirms that the CFAA should not be read to include such an exception. *See Marx v. Gen. Revenue Corp.*, 568 U.S. 371, 384 (2013) (Congress's "use of explicit language in other statutes cautions against inferring a limitation" not present in the plain text, as "Congress' explicit use of [language] in other provisions shows that it specifies such restrictions when it wants to." (citation omitted)).

the CFAA covered only pre-Internet computer hacking. But the provision at issue here, § 1030(a)(2), was added to the CFAA in *1996*—not 1984—as part of the same set of amendments that added the "nonpublic" modifier to government computers in § 1030(a)(3). *See supra*, pp. 6, 25-26. By the mid-1990s, the publicly-accessible Internet was well-known and in wide use. Shortly before Congress added these amendments, it passed the Telecommunications Act of 1996, which declared that "[it] is the policy of the United States … to promote the continued development of the Internet and other interactive computer services and other interactive media." Pub. L. No. 104-104, §230, 110 Stat 56, 62-63 (1996). And as previously noted, *see supra* p. 6, when Congress added § 1030(a)(2), it explicitly understood that "accessing" a "publicly available" computer "via an agency's World Wide Web site" without authorization could trigger CFAA liability, *see* S. Rep. No. 104-357, at 8-9 (1996). Congress inserted the word "nonpublic" into § 1030(a)(3) to avoid that result in the context of government computers, but did not do so in § 1030(a)(2). The suggestion that these CFAA provisions were not meant to apply to publicly-accessible website servers is thus implausible.

Ignoring the relevant history, the Ninth Circuit focused instead on a single line of the same report, which stated that § 1030(a)(2) was amended "to increase protection for the privacy and confidentiality of computer information." Pet. App. 27a (quoting S. Rep. No. 104-357, at 7). But the Ninth Circuit's construction actually undermines privacy protection. *See infra*, pp. 29-33. In addition, the same report made clear that the CFAA would attach liability to accessing publicly available computers. *See* S. Rep. No. 104-357, at 8-9 (1996); *3Taps*, 964 F. Supp. 2d at 1186 (noting that the legislative history identifies both protection of privacy and preventing trespass as goals of the statute). The court of appeals' claim that the

1996 Senate Report "makes clear that the prohibition on unauthorized access is properly understood to apply only to private information" is thus belied by the Report itself. Pet. App. 27a

C. The Decision Below Raises Issues of Exceptional Importance That Should Be Addressed Now

The control of Internet users' data and protection of their privacy are issues of enormous and increasing national importance. *See generally* Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 Duke L.J. 555, 585 (2018). The decision below bears upon those issues in a direct and profound way that warrants this Court's immediate review.[10]

1. The decision below has extraordinary and adverse consequences for the privacy interests of the hundreds of millions of users of websites that make at least some

---

[10] Although the court of appeals purported to hold only that hiQ had raised serious questions on the merits for purposes of its preliminary injunction motion, it rested that conclusion on a definitive construction of the meaning of "without authorization" in Section 1030(a)(2). That ruling is binding on the district court in this case and binding generally in the Ninth Circuit. *See M.R. v. Dreyfus*, 697 F.3d 706, 709 n.1 (9th Cir. 2012) (noting that "*all* published opinions—including those interpreting statutory law at the preliminary injunction stage … constitute law of the circuit, such that they constitute[ ] binding authority which must be followed unless and until overruled by a body competent to do so") (emphasis and alteration in original and internal quotation marks omitted). This Court routinely and in a variety of circumstances grants certiorari where a court of appeals has granted a preliminary injunction, and has thus only analyzed the likelihood of success on the merits. *See, e.g.*, *Trump v. Hawaii*, 138 S. Ct. 2392, 2404 (2018); *Ashcroft v. Am. Civil Liberties Union*, 542 U.S. 656, 661 (2004); *City of Los Angeles v. Lyons*, 461 U.S. 95, 100 (1983).

user data publicly accessible. When users share information on a website, they understand that the information will in one sense be available to the public that views the information. But they also expect that limitations on viewing and exploiting their information will be respected—for instance, rights that the website grants them to restrict access to or remove their personal information when they so choose. Users do not expect, or consent to, the exploitation of their personal information in perpetuity by third parties that the users and the website owner did not authorize and whose interests are not aligned with the interests of the owners of that personal information. But the decision below, by casting aside the privacy interests of users and the interests of website owners in protecting user privacy, invites scrapers like hiQ to take personal information from a website on which millions of users have decided to share their information and copy it to a server to use for a different purpose, where those who provided the information no longer control its accessibility, reproduction, and exploitation.

The uproar over Cambridge Analytica's massive misuse of Facebook user information and, more recently, Clearview's compilation of a vast database that will potentially allow for instant facial recognition (and possible surveillance) of billions of people, leaves no doubt that the public is deeply concerned about the issue of control of personal information and privacy on the Internet.[11]

---

[11] *See* Matthew Rosenberg & Sheera Frankel, *Facebook's Role in Data Misuse Sets off Storms on Two Continents*, The New York Times (Mar. 18, 2018), https://www.nytimes.com/2018/03/18/us/-cambridge-analytica-facebook-privacy-data.html; *supra,* pp. 4-5 & nn. 2-3.

LinkedIn and its peer companies are attempting to protect their users' personal data in a manner that respects the needs and expectations of those users. Section 1030(a)(2) is vital to their ability to do so, as "the premise of [§ 1030(a)(2)] is privacy protection." *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, No. 11-cv-01073, 2012 WL 3862209, at *12 (S.D. Ohio Sept. 5, 2012) (internal quotation marks omitted); *Doe v. Dartmouth-Hitchcock Med. Ctr.*, No. 00-cv-100, 2001 WL 873063, at *4 (D.N.H. July 19, 2001) (same); *Am. Online, Inc. v. Nat'l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1275 (N.D. Iowa 2000) (same). But at the very moment when control and protection of personal information on the Internet has become surpassingly important, the Ninth Circuit has made it markedly harder for website owners to meet their users' privacy expectations. As many commentators have recognized, after the Ninth Circuit's decision, "it's unclear whether [companies] have any legal recourse" to end scraping like Clearview's,[12] because, as the head of the Stanford Internet Observatory put it, the decision below "eviscerated the legal argument that [websites] used to use on scammers and spammers."[13]

2. This case vividly illustrates the damage the Ninth Circuit's rule will cause. LinkedIn members own the content and information that they submit or post on LinkedIn. Pet. App. 2a. The privacy settings LinkedIn offers its members allow them to specify who can see different portions of their profile; to choose a "Do Not Broadcast" option, which prevents others from being notified about changes made to an individual's profile; and

---

[12] Louise Matsakis, *Scraping the Web is a Powerful Tool. Clearview AI Abused it*, Wired (Jan. 25 2020), https://www.wired.com/story/clearview-ai-scraping-web/

[13] Hill, *supra* n.3.

to prevent continuing access to their personal information if they choose to delete some data or close their accounts. *Id.* Unsurprisingly, LinkedIn users have complained to LinkedIn when those expectations are upset, including when they discover their data has been scraped from LinkedIn and made available on other websites. *See* 3ER-431-432.

The decision below casts aside the interests of LinkedIn members in controlling who has access to their data, the privacy of that data, and the desire to protect personal information from abuse by third parties, and it has done so in the service of hiQ's narrow business interests. Rather than allow LinkedIn members to control their own professional information in order to advance their careers, the Ninth Circuit leaves them at the mercy of unaccountable scrapers like hiQ that gather members' data and use it against their interests and without their knowledge. Whereas LinkedIn's privacy policy creates obligations for LinkedIn to its members and their privacy rights, third parties like hiQ can do whatever they want with member data under the Ninth Circuit's ruling. But, as the Ninth Circuit itself 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." Pet. App. 11a-12a (internal quotation marks omitted).

The Ninth Circuit nevertheless assumed that LinkedIn's members (and Internet users generally) would have few qualms about these harms because they purportedly expect their data to be "accessed by others, including for commercial purposes," even purposes antithetical to their selected privacy settings. Pet. App. 14a. To the contrary, LinkedIn's members have made clear that they care deeply about controlling how and with whom they share their personal information. And the

broad public outcry over Cambridge Analytica, Clearview, and other privacy-invading misuses of personal data leaves little doubt that the court of appeals' assumptions about public expectations of privacy are far off the mark, and certainly do not justify the court's decision to restrict the CFAA's scope.

3. The damage done by the opinion below extends beyond user privacy and affects the owners of publicly-accessible websites and the Internet itself in ways that independently justify immediate plenary review. Because of the Ninth Circuit's rule, platforms seeking to protect their information and the privacy of their users will face enormous pressure to put their systems behind walls. As noted above, LinkedIn blocks approximately 95 million automated calls to its servers every day. Under the Ninth Circuit's rule, every company with a public portion of its website that is integral to the operation of its business—from online retailers like Ticketmaster and Amazon to social networking platforms like Twitter—will be exposed to invasive bots deployed by free-riders unless they place those websites entirely behind password barricades. But if that happens, those websites will no longer be indexable by search engines, which will make information less available to discovery by the primary means by which people obtain information on the Internet. 4ER-762. Erecting a complete password wall would harm not only LinkedIn's users but also the free flow of information on the Internet. The decision below wrongly requires websites to choose between allowing free riders to abuse their users' data and slamming the door on the benefits to their users of the Internet's open forum.

The Ninth Circuit's rule also threatens to stifle innovation. Entrepreneurs will be discouraged from developing groundbreaking platforms if abusive technological copycats can hide behind the Ninth Circuit's reading of

the CFAA. For example, if the Ninth Circuit rule persists, Craigslist could not prevent an entity from scraping data to "'essentially replicate[] the entire craigslist website,'" *3Taps*, 964 F. Supp. 2d at 1180, simply because Craigslist's business requires that the information on its website be available to the public. Nor could online retailers prevent their sites from being scraped by bots, again because a publicly-available website could not revoke authorization absent a password system. *QVC, Inc.*, 159 F. Supp. 3d at 581, 591. There is thus every reason to think that the Ninth Circuit's rule will lead to less investment, less entrepreneurship, and fewer accompanying benefits for users of websites featuring publicly accessible information.

* * *

The Ninth Circuit's opinion is not only wrong as a matter of law and in conflict with every federal court to consider the question; it also raises important questions about the future of protection of user data and innovation on the Internet. Companies like LinkedIn require clarity as to how to safeguard their members' data and privacy and conduct their operations under the CFAA. This Court's review is necessary to provide that guidance.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

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

ERIC A. SHUMSKY
ORRICK HERRINGTON & SUTCLIFFE LLP
1152 15th Street, NW
Washington, DC 20005
(202) 339-8400

BRIAN P. GOLDMAN
ORRICK HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105
(415) 773-5700

DONALD B. VERRILLI, JR.
Counsel of Record
JONATHAN S. MELTZER
MUNGER, TOLLES & OLSON LLP
1155 F Street NW, 7th Floor
Washington, DC 20004
(202) 220-1100
donald.verrilli@mto.com

JONATHAN H. BLAVIN
ROSEMARY T. RING
NICHOLAS D. FRAM
MARIANNA Y. MAO
MUNGER, TOLLES & OLSON LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105
(415) 512-4000

Counsel for Petitioners

MARCH 9, 2020

APPENDIX

APPENDIX A

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 17-16783

HIQ LABS, INC.,

Plaintiff-Appellee,

v.

LINKEDIN CORPORATION,

Defendant-Appellant.

Appeal from the United States District Court for the Northern District of California Edward M. Chen, District Judge, Presiding, D.C. No. 3:17-cv-03301-EMC

Filed September 9, 2019

Before: J. CLIFFORD WALLACE and MARSHA S. BERZON, Circuit Judges, and TERRENCE BERG,* District Judge.

Concurrence by Judge Wallace

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

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

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]

---

[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

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 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

---

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).

[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.merriamwebster.com/dictionary/bot (last visited

several technological systems to detect suspicious activity and 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

---

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).

[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).

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 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,

---

[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.

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."

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

---

[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).

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, 129 S.Ct. 365, 172 L.Ed.2d 249 (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. 1002, 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

---

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

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 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, 270 Cal.Rptr. 1, 791 P.2d 587 (1990).[8]

---

[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, 11 Cal.Rptr. 97, 359 P.2d 465 (1961), *abrogated on other grounds by Brown v. Kelly Broadcasting Co.*,

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

---

48 Cal. 3d 711, 753 n.37, 257 Cal.Rptr. 708, 771 P.2d 406 (1989); *see also Pac. Gas & Elec. Co.*, 50 Cal. 3d at 1129, 270 Cal.Rptr. 1, 791 P.2d 587 ("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.").

designed to induce a breach or disruption" of hiQ's contractual relationships with third parties. *Pac. Gas & Elec. Co.*, 50 Cal. 3d at 1126, 270 Cal.Rptr. 1, 791 P.2d 587; *cf. Winchester Mystery House, LLC v. Global Asylum, Inc.*, 210 Cal. App. 4th 579, 597, 148 Cal.Rptr.3d 412 (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. 992–94.

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, 77 Cal.Rptr.2d 709, 960 P.2d 513 (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, 77 Cal.Rptr.2d 709, 960 P.2d 513. 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, 112 P.2d 631 (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, 45 Cal.Rptr.2d 436, 902 P.2d 740 (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, 112 P.2d 631; *see id.* at 37, 112 P.2d 631 ("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, 112 P.2d 631.

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, 14 Cal.Rptr. 294, 363 P.2d 310 (1961). Considerations include whether "the means of interference involve no more than recognized trade practices," *Buxbom v. Smith*, 23 Cal. 2d 535, 546, 145 P.2d 305 (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, 172 Cal.Rptr. 74 (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, 159 Cal.Rptr. 285 (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, 145 P.2d 305—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, 172 Cal.Rptr. 74. 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]

---

[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

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. 994–95, 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.

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

---

for the purpose of eliminating hiQ as a competitor in the data analytics field, and thus potentially 'violates [the UCL].' "

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 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

---

[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, 70 Cal.Rptr.3d 727, 174 P.3d 741 (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.

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*, —— U.S. ——, 138 S. Ct. 314, 199 L.Ed.2d 207 (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

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

"misappropriation statute," *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*, —— U.S. ——, 138 S. Ct. 313, 199 L.Ed.2d 206 (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

---

[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."

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 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 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, 93 S.Ct. 2201, 37 L.Ed.2d 48 (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

---

[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.

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, 125 S.Ct. 377, 160 L.Ed.2d 271

(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

---

[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.

chattels claims may still be available.[15] And other causes of action, such as copyright 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

---

[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. 995–96, 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. 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, 1 Cal.Rptr.3d 32, 71 P.3d 296 (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).

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 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 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.

---

[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.

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

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 "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).

APPENDIX B

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

Civil Action No. 17-cv-03301-EMC

HIQ LABS, INC.,

Plaintiff,

v.

LINKEDIN CORPORATION,

Defendant.

[Filed: August 14, 2017]

ORDER GRANTING PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

Docket No. 23

EDWARD M. CHEN, United States District Judge

I. INTRODUCTION

Plaintiff hiQ initiated this action after Defendant LinkedIn issued a cease and desist letter and attempted to terminate hiQ's ability to access otherwise publicly available information on profiles of LinkedIn users. The letter threatens action under the Computer Fraud and Abuse Act (CFAA). LinkedIn also employed various blocking techniques designed to prevent hiQ's automated data collection methods. LinkedIn brought this action after years of tolerating hiQ's access and use of its data.

hiQ's business involves providing information to businesses about their workforces based on statistical analysis of publicly available data. Its data analytics business is wholly dependent on LinkedIn's public data. hiQ contends that LinkedIn's actions constitute

unfair business practices under Cal. Bus. & Prof. Code §§ 17200 *et seq*. hiQ also raises a number of common law tort and contract claims, including intentional interference with contract and promissory estoppel, and further contends that LinkedIn's actions constitute a violation of free speech under the California Constitution.

Now pending before the Court is hiQ's motion for a preliminary injunction. For the reasons set forth in more detail below, the Court **GRANTS** the motion. In summary, the balance of hardships tips sharply in hiQ's favor. hiQ has demonstrated there are serious questions on the merits. In particular, the Court is doubtful that the Computer Fraud and Abuse Act may be invoked by LinkedIn to punish hiQ for accessing publicly available data; the broad interpretation of the CFAA advocated by LinkedIn, if adopted, could profoundly impact open access to the Internet, a result that Congress could not have intended when it enacted the CFAA over three decades ago. Furthermore, hiQ has raised serious questions as to whether LinkedIn, in blocking hiQ's access to public data, possibly as a means of limiting competition, violates state law.

II. FACTUAL AND PROCEDURAL BACKGROUND

Founded in 2002, LinkedIn is a social networking site focused on business and professional networking. It currently has over 500 million users; it was acquired by Microsoft in December 2016 for $26.2 billion.

LinkedIn allows users to create profiles and then establish connections with other users. When LinkedIn users create a profile on the site, they can

choose from a variety of different levels of privacy protection. They can choose to keep their profiles entirely private, or to make them viewable by: (1) their direct connections on the site; (2) a broader network of connections; (3) all other LinkedIn members; or (4) the entire public. When users choose the last option, their profiles are viewable by anyone online regardless of whether that person is a LinkedIn member. LinkedIn also allows public profiles to be accessed via search engines such as Google.

hiQ was founded in 2012 and has, to date, received $14.5 million in funding. hiQ sells to its client businesses information about their workforces that hiQ generates through analysis of data on LinkedIn users' publicly available profiles. It offers two products: "Keeper," which tells employers which of their employees are at the greatest risk of being recruited away; and "Skill Mapper," which provides a summary of the skills possessed by individual workers. Docket No. 23–4 (Weidick Decl.) ¶¶ 4–6. hiQ gathers the workforce data that forms the foundation of its analytics by automatically collecting it, or harvesting or "scraping" it, from publicly available LinkedIn profiles. hiQ's model is predicated entirely on access to data LinkedIn users have opted to publish publicly. hiQ relies on LinkedIn data because LinkedIn is the dominant player in the field of professional networking.

On May 23, 2017, LinkedIn sent a letter demanding that hiQ "immediately cease and desist unauthorized data scraping and other violations of LinkedIn's User Agreement." Docket No. 23–1 ("Gupta Decl.") Ex. J. In the letter, LinkedIn demanded that hiQ cease using software to "scrape,"

or automatically collect, data from LinkedIn's public profiles. LinkedIn noted that its User Agreement prohibits various methods of data collection from its website, and stated that hiQ was in violation of those provisions. LinkedIn also stated that it had restricted hiQ's company page on LinkedIn and that "[a]ny future access of any kind" to LinkedIn by hiQ would be "without permission and without authorization from LinkedIn." LinkedIn further stated that it had "implemented technical measures to prevent hiQ from accessing, and assisting other to access, LinkedIn's site, through systems that detects, monitor, and block scraping activity." LinkedIn stated that any further access to LinkedIn's data would violate state and federal law, including California Penal Code § 502(c), the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, state common law of trespass, and the Digital Millennium Copyright Act. LinkedIn reserved the right to pursue litigation, should hiQ fail to cease and desist from accessing LinkedIn's website, computer systems, and data.

After hiQ and LinkedIn were unable to agree on an amicable resolution, and LinkedIn declined to permit hiQ's continued access in the interim, hiQ filed the complaint in this action, which asserts affirmative rights against the denial of access to publicly available LinkedIn profiles based on California common law, the UCL, and the California Constitution. hiQ also seeks a declaration that hiQ has not and will not violate the CFAA, the DMCA, California Penal Code § 502(c), and the common law of trespass to chattels, by accessing LinkedIn public profiles. Docket No. 1. At the same time, hiQ also filed a request for a temporary restraining order and

an order to show cause why a preliminary injunction should not be issued against LinkedIn. Docket No. 23. After a hearing on the TRO request, the parties entered into a standstill agreement preserving hiQ's access to the data and converting hiQ's initial motion into a motion for a preliminary injunction. A hearing on the motion for preliminary injunction was held on July 27, 2017.

III. DISCUSSION

"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, 129 S.Ct. 365, 172 L.Ed.2d 249 (2008). In evaluating these factors, courts in the Ninth Circuit employ a "sliding scale" approach, according to which "the elements of the preliminary injunction test are balanced, so that a stronger showing of one element may offset a weaker showing of another. For example, a stronger showing of irreparable harm to plaintiff might offset a lesser showing of likelihood of success on the merits." *All. for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011). At minimum, "[u]nder *Winter*, plaintiffs must establish that irreparable harm is *likely,* not just possible, in order to obtain a preliminary injunction." *Id.* (emphasis in original). Specifically, the Ninth Circuit "has adopted and applied a version of the sliding scale approach under which a preliminary injunction could issue where the likelihood of success is such that 'serious questions going to the merits were raised and the balance of hardships tips sharply in [plaintiff's] favor.'"

(quoting *Clear Channel Outdoor, Inc. v. City of Los Angeles*, 340 F.3d 810, 813 (9th Cir. 2003)). Thus, upon a showing that the balance of hardships tips sharply in its favor, a party seeking a preliminary injunction need only show that there are "serious questions going to the merits" in order to be entitled to relief. Because the balance of hardships, including the threat of irreparable harm faced by each party, informs the requisite showing on the merits, the Court addresses that prong first.

A. Irreparable Harm and Balance of Hardships

hiQ states that absent injunctive relief, it will suffer immediate and irreparable harm because its entire business model depends on access to LinkedIn's data. If LinkedIn prevails, hiQ will simply go out of business; it "will have to breach its agreements with its customers, stop discussions with its long list of prospective customers, lay off most if not all its employees, and shutter its operations." Docket No. 24 ("Motion") at 24. These are credible assertions, given the undisputed fact that hiQ's entire business depends on its access to LinkedIn's public profile data.[1] These potential consequences are

[1] At the hearing, LinkedIn pointed to the fact that other companies operate in the data analytics field without making use of LinkedIn's member data. But as hiQ pointed out, these companies employ entirely different business models. For example, one company highlighted by LinkedIn, Glint, creates its own data by taking surveys of employees working for its clients. Requiring hiQ to rebuild its business on an entirely different business model, such as that employed by Glint, from scratch would constitute harm comparable to simply going out of business. LinkedIn also suggests that hiQ could make use of other sources of data, such as Facebook. But while Facebook may have a comparable number of professionals using its service, LinkedIn has not argued that the professional data

sufficient to constitute irreparable harm. "The 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); *see also Doran v. Salem Inn, Inc.*, 422 U.S. 922, 932, 95 S.Ct. 2561, 45 L.Ed.2d 648 (1975) (holding that "a substantial loss of business and perhaps even bankruptcy" constitutes irreparable harm sufficient to warrant interim relief). Similarly, "[e]vidence of threatened loss of prospective customers or goodwill certainly supports a finding of the possibility of irreparable harm." *Stuhlbarg Int'l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001).

For its part, LinkedIn argues that it faces significant harm because hiQ's data collection threatens the privacy of LinkedIn users, because even members who opt to make their profiles publicly viewable retain a significant interest in controlling the use and visibility of their data.[2] In particular, LinkedIn points to the interest that some users may have in preventing employers or other parties from tracking *changes* they have made to their profiles. LinkedIn posits that when a user updates his profile, that action may signal to his employer that he is looking for a new position. LinkedIn states that over 50 million LinkedIn members have used a "Do Not Broadcast" feature that prevents the site from notifying other users when a member makes profile

---

available at Facebook is of a similar quality to that available at LinkedIn. Moreover, if LinkedIn's view of the law is correct, nothing would prevent Facebook from barring hiQ in the same way LinkedIn has.

[2] LinkedIn does not claim a proprietary interest in its users' profiles.

changes. This feature is available even when a profile is set to public. LinkedIn also points to specific user complaints it has received objecting to the use of data by third parties. In particular, two users complained that information that they had *previously* featured on their profile, but subsequently removed, remained viewable via third parties. (These complaints involved third parties other than hiQ.) LinkedIn maintains that all of these concerns are potentially undermined by hiQ's data collection practices: while the information that hiQ seeks to collect is publicly viewable, the posting of changes to a profile may raise the risk that a current employee may be rated as having a higher risk of flight under Keeper even though the employee chose the Do Not Broadcast setting. hiQ could also make data from users available even after those users have removed it from their profiles or deleted their profiles altogether. LinkedIn argues that both it and its users therefore face substantial harm absent an injunction; if hiQ is able to continue its data collection unabated, LinkedIn members' privacy may be compromised, and the company will suffer a corresponding loss of consumer trust and confidence.

These considerations are not without merit, but there are a number of reasons to discount to some extent the harm claimed by LinkedIn. First, LinkedIn emphasizes that the fact that 50 million users have opted into the "Do Not Broadcast" feature indicates that a vast number of its users are fearful that their employer may monitor their accounts for possible changes. But there are other potential reasons why a user may opt for that setting. For instance, users may be cognizant that their profile changes are generating a large volume of unwanted notifications broadcasted

to their connections on the site. They may wish to limit annoying intrusions into their contacts.[3] Second, LinkedIn has presented little evidence of users' actual privacy expectation; out of its hundreds of millions of users, including 50 million using Do Not Broadcast, LinkedIn has only identified *three* individual complaints specifically raising concerns about data privacy related to third-party data collection. Docket No. 49–1 Exs. A–C. None actually discuss hiQ or the "Do Not Broadcast" setting. Third, LinkedIn's professed privacy concerns are somewhat undermined by the fact that LinkedIn allows other third-parties to access user data without its members' knowledge or consent. LinkedIn offers a product called "Recruiter" that allows professional recruiters to identify possible candidates for other job opportunities. LinkedIn avers that when users have selected the Do Not Broadcast option, the Recruiter product respects this choice and does not update recruiters of profile changes. However, hiQ presented marketing materials at the hearing which indicate that regardless of other privacy settings, information including profile changes are conveyed to third parties who subscribe to Recruiter. Indeed, these materials inform potential customers that when they "follow" another user, "[f]rom now on, when they update their profile or celebrate a work anniversary, you'll receive an update on your homepage. And don't worry—they don't know you're following them." LinkedIn thus trumpets its own product in a way

[3] Though the "Do Not Broadcast" feature makes it less likely to draw immediate attention to a profile update, it does nothing to prevent an employer, or any other third-party, from visiting an employee's page periodically to determine whether significant changes have been made.

that seems to afford little deference to the very privacy concerns it professes to be protecting in this case.

LinkedIn stresses that its privacy policy expressly permits disclosures of this sort, whereas it expressly prohibits third-party scraping of the sort that hiQ engages in. Accordingly, LinkedIn argues that the Recruiter program accords with its members' expectations of privacy, whereas hiQ's data collection does not.[4] It is unlikely, however, that most users' *actual* privacy expectations are shaped by the fine print of a privacy policy buried in the User Agreement that likely few, if any, users have actually read.[5] To the contrary, it is not obvious that LinkedIn members who decide to set their profiles to be publicly viewable expect much privacy at all in the profiles they post.

In sum, hiQ unquestionably faces irreparable harm in the absence of an injunction, as it will likely be driven out of business. The asserted harm LinkedIn faces, by contrast, is tied to its users' expectations of privacy and any impact on user trust in LinkedIn. However, those expectations are uncertain at best, and in any case, LinkedIn's own actions do not appear to have zealously safeguarded

---

[4] LinkedIn argues hiQ signed up as a LinkedIn user and is thus bound by the User Agreement. But LinkedIn has since terminated hiQ's user status. LinkedIn has not demonstrated that hiQ's aggregation of data from LinkedIn's public profiles is dependent on its status as a LinkedIn user.

[5] *See*, *e.g.*, Tom Towers, *Thousands Sign up for Community Service After Failing to Read Terms and Conditions*, Metro News (July 14, 2017, 11:12 PM), http://metro.co.uk/2017/07/14/thousandssign-up-for-community-service-after-failing-to-read-terms-and-conditions-6781034/.

those privacy interests.

Furthermore, despite the fact that hiQ has been aggregating LinkedIn's public data for five years with LinkedIn's knowledge, LinkedIn has presented no evidence of harm, financial or otherwise resulting from hiQ's activities. Indeed, LinkedIn has not explained why suddenly it has now chosen to revoke its consent (or at least tolerance) of hiQ's use of that data.

The Court concludes that based on the record presented, the balance of hardships tips sharply in hiQ's favor. To be entitled to an injunction, therefore, hiQ needs only show that it has raised "serious questions going to the merits." *All. for the Wild Rockies*, 632 F.3d at 1131.

B. Serious Questions Going to the Merits

hiQ argues that it is likely to prevail on the merits—or at least raises serious questions going to the merits—on each of its claims. For its part, LinkedIn argues that all of hiQ's claims necessarily fail because hiQ's unauthorized access to LinkedIn's computers violates the CFAA. Thus, not only is LinkedIn's cease and desist letter backed by the CFAA, to the extent that any of hiQ's state claims have merit, they would be preempted by the CFAA. The Court thus first addresses the likelihood that the CFAA applies.

1. CFAA

Whether hiQ's continued access to the LinkedIn public profiles violates the CFAA constitutes a key threshold question in this case. The CFAA creates civil and criminal liability for any person who "intentionally accesses a computer without

authorization or exceeds authorized access, and thereby obtains ... information from any protected computer."[6] 18 U.S.C. § 1030(a)(2)(C). As the Supreme Court has explained, the statute "provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Musacchio v. United States*, ––– U.S. ––––, 136 S.Ct. 709, 713, 193 L.Ed.2d 639 (2016).

The key question regarding the applicability of the CFAA in this case is whether, by continuing to access public LinkedIn profiles after LinkedIn has explicitly revoked permission to do so, hiQ has "accesse[d] a computer without authorization" within the meaning of the CFAA. LinkedIn argues that under the plain meaning of "without authorization," as well as under relevant Ninth Circuit authority, hiQ has. LinkedIn relies primarily on two cases.

First, in *Facebook, Inc. v. Power Ventures, Inc.*, the Ninth Circuit held that "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or *when such permission has been revoked explicitly*." 844 F.3d 1058, 1067 (9th Cir. 2016) (emphasis added). In *Power Ventures*, the defendant operated a site that extracted and aggregated users' social networking information from Facebook and other sites on a single page. The defendant gained access to password-protected Facebook member

---

[6] As LinkedIn notes, because its computers are connected to the Internet and affect interstate commerce, they are "protected computers" under the CFAA. *See United States v. Nosal* (*Nosal I*), 676 F.3d 854, 859 (9th Cir. 2012). hiQ does not dispute this fact.

profiles when its users supplied their Facebook login credentials. When users selected certain options on the defendant's site, the defendant, in many instances, "caused a message to be transmitted to the user's friends within the Facebook system." *Id.* at 1063. Facebook had sent a cease and desist letter demanding that Power Ventures cease accessing information on users' pages. The Ninth Circuit found a CFAA violation where "after receiving written notification from Facebook" Power Ventures "circumvented IP barriers" and continued to access Facebook servers. *Id.* at 1068. In short, Power Ventures accessed Facebook computers "without authorization."

LinkedIn also relies on *United States v. Nosal* (*Nosal II*), 844 F.3d 1024 (9th Cir. 2016). There, the Ninth Circuit held that an employee "whose computer access credentials were affirmatively revoked by [his employer] acted 'without authorization' in violation of the CFAA when he or his former employee coconspirators used the login credentials of a current employee" to gain access to the employer's computer systems. *Id.* at 1038. Specifically, the defendant persuaded current employees of the company to use their login credentials to access and collect confidential information, including trade secrets that Nosal and the employees planned to use to start a competing business. *Id.* at 1028–29. The court held "that 'without authorization" is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission." *Id.* at 1028. Defendant's authorization had been revoked when he left the company.

Each of these cases is distinguishable in an

important respect: none of the data in *Facebook* or *Nosal II* was *public* data. Rather, the defendants in those cases gained access to a computer network (in *Nosal II*) and a portion of a website (in *Power Ventures*) that were protected by a password authentication system. In short, the unauthorized intruders reached into what would fairly be characterized as the private interior of a computer system not visible to the public. Neither of those cases confronted the precise issue presented here: whether visiting and collecting information from a publicly available website may be deemed "access" to a computer "without authorization" within the meaning of the CFAA where the owner of the web site has selectively revoked permission.

To be sure, LinkedIn's construction of the CFAA is not without basis. Visiting a website accesses the host computer in one literal sense, and where authorization has been revoked by the website host, that "access" can be said to be "without authorization." *See Craigslist Inc. v. 3Taps Inc.*, 942 F.Supp.2d 962 (N.D. Cal. 2013). However, whether "access" to a publicly viewable site may be deemed "without authorization" under the CFAA where the website host purports to revoke permission is not free from ambiguity. The Supreme Court has cautioned that "[w]hether a statutory term is unambiguous ... does not turn solely on dictionary definitions of its component words. Rather, 'the plainness or ambiguity of statutory language is determined [not only] by reference to the language itself, [but as well by] the specific context in which that language is used, and the broader context of the statute as a whole.'" *Yates v. United States*, —— U.S. ——, 135 S.Ct. 1074, 1082, 191 L.Ed.2d 64 (2015) (quoting

Robinson v. Shell Oil Co., 519 U.S. 337, 341, 117 S.Ct. 843, 136 L.Ed.2d 808 (1997)) (holding that a fish is not a "tangible object" within the meaning of the Sarbanes–Oxley Act). *See also Bond v. U.S.*, —— U.S. ——, 134 S.Ct. 2077, 2090, 189 L.Ed.2d 1 (2014) (rejecting literal reading of Chemical Weapons Convention Implementation Act that would have permitted prosecution of woman who caused minor chemical burns to spouse's lover's thumb because "[p]art of a fair reading of statutory text is recognizing that 'Congress legislates against the backdrop' of certain unexpressed presumptions") (quoting *EEOC v. Arabian American Oil Co.*, 499 U.S. 244, 248, 111 S.Ct. 1227, 113 L.Ed.2d 274 (1991)).

The CFAA must be interpreted in its historical context, mindful of Congress' purpose. The CFAA was not intended to police traffic to publicly available websites on the Internet—the Internet did not exist in 1984. The CFAA was intended instead to deal with "hacking" or "trespass" onto private, often password-protected mainframe computers. *See* H.R. Rep. No. 98–894, 1984 U.S.C.C.A.N. 3689, 3691–92, 3695–97 (1984); S. Rep. No. 99–432, 1986 U.S.C.C.A.N. 2479, 2480 (1986). The Ninth Circuit has recognized this statutory purpose, explaining that "Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking, recognizing that, '[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system.'" *United States v. Nosal* (*Nosal I*), 676 F.3d 854, 858 (9th Cir. 2012) (quoting S.Rep. No. 99–432, a 9 (1986), 1986 U.S.C.C.A.N. 2479, 2487 (Conf. Rep.)). It was originally enacted to protect government computers from hacking; it was expanded in 1986 to

protect commercial computer systems. *See* S.Rep. No. 99–432, at 2 (1986), 1986 U.S.C.C.A.N. 2479, 2480 (Conf. Rep.)). The Ninth Circuit, in considering a related provision of the statute, cautioned against an overbroad interpretation that would "expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer," thereby "mak[ing] criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *Nosal I*, 676 F.3d at 859.

As hiQ points out, application of the CFAA to the accessing of websites open to the public would have sweeping consequences well beyond anything Congress could have contemplated; it would "expand its scope well beyond computer hacking." *Nosal I*, 676 F.3d at 859. Under LinkedIn's interpretation of the CFAA, a website would be free to revoke "authorization" with respect to any person, at any time, for any reason, and invoke the CFAA for enforcement, potentially subjecting an Internet user to criminal, as well as civil, liability. Indeed, because the Ninth Circuit has specifically rejected the argument that "the CFAA only criminalizes access where the party circumvents a technological access barrier," *Nosal II*, 844 F.3d at 1038, merely *viewing* a website in contravention of a unilateral directive from a private entity would be a crime, effectuating the digital equivalence of Medusa. The potential for such exercise of power over access to publicly viewable information by a private entity weaponized by the potential of criminal sanctions is deeply concerning.[7] This effect would be particularly

[7] Although there is no indication of any current threat of criminal prosecution in this case as LinkedIn thus far has

pernicious because once it is found to apply, the CFAA as interpreted by LinkedIn would not leave any room for the consideration of either a website owner's reasons for denying authorization or an individual's possible justification for ignoring such a denial. Website owners could, for example, block access by individuals or groups on the basis of race or gender discrimination. Political campaigns could block selected news media, or supporters of rival candidates, from accessing their websites. Companies could prevent competitors or consumer groups from visiting their websites to learn about their products or analyze pricing. Further, in addition to criminalizing any attempt to obtain access to information otherwise viewable by the public at large, the CFAA would preempt all state and local laws that might otherwise afford a legal right of access (*e.g.*, state law rights asserted by hiQ herein). A broad reading of the CFAA could stifle the dynamic

---

alluded only to possible civil enforcement of the CFAA, a construction of the CFAA must take into account the fact the statute may be enforced criminally and that its interpretation would apply uniformly to criminal as well as civil enforcement. *See, e.g., Ratzlaf v. United States*, 510 U.S. 135, 143, 114 S.Ct. 655, 126 L.Ed.2d 615 (1994) ("A term appearing in several places in a statutory text is generally read the same way each time it appears. We have even stronger cause to construe a *single* formulation ... the same way each time it is called into play."); *F.C.C. v. American Broadcasting Co.*, 347 U.S. 284, 296, 74 S.Ct. 593, 98 L.Ed. 699 (1954) (rejecting notion that "the same substantive language has one meaning if criminal prosecutions are brought ... and quite a different meaning" in civil action by private party); *U.S. v. Charnay*, 537 F.2d 341, 348 (9th Cir. 1976) (agreeing there was "no reasonable basis that some different interpretation [of Rule 10b–5] should apply to a criminal action than in a civil action" for meaning of "deceptive device" under 15 U.S.C. § 78j(b)).

evolution and incremental development of state and local laws addressing the delicate balance between open access to information and privacy—all in the name of a federal statute enacted in 1984 before the advent of the World Wide Web.[8]

Congress could not have intended these profound consequences when it enacted the CFAA in 1984. The Court is reluctant to give the CFAA the expansive interpretation sought by LinkedIn absent convincing authority therefor.

Construction of the CFAA, including the terms "access" and "without authorization," should be informed not only by Congress' intent but also by the

---

[8] LinkedIn argued at the hearing on this motion that the likelihood of these negative consequences is lessened because violation of the CFAA may be invoked only where the alleged violation "caused ... loss ... aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(1). However, a violation of § 1030(a)(2) is punishable as a misdemeanor without regard to amount of loss. 18 U.S.C. § 1030(c)(2)(A). Although felony charges or a civil action may not be brought unless there is a loss of at least $5,000, *see* § 1030(c)(4)(A)(i)(1) and 18 U.S.C. § 1030(g), the CFAA defines "loss" broadly as "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." 18 U.S.C. § 1030(e)(11). As a number of courts have explained, this "broadly worded provision plainly contemplates consequential damages of the type sought by [Plaintiff]—costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). Because merely investigating a potential violation may satisfy the statutory damage threshold, it is unlikely that the $5,000 requirement will provide a meaningful check on the potential reach of the CFAA.

Act's theoretical underpinning. The CFAA's origin as a statute addressing the problem of computer "trespass" suggests an interpretation of the statute informed by examining general principles which govern trespass laws. In an article cited approvingly by the Ninth Circuit in both *Nosal II* and *Power Ventures*, Professor Orin Kerr argues the analogy to trespass laws is key to understanding the appropriate scope of the "without authorization" provision of the CFAA. *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016). Kerr argues that in the context of physical space, whether or not an action constitutes a trespass depends on a set of shared social norms that "tell us, at an intuitive level, when entry to property is forbidden and when it is permitted." *Id.* at 1149. Thus, the Court understands that it is generally impermissible to enter into a private home without permission in any circumstances. By contrast, it is presumptively *not* trespassing to open the unlocked door of a business during daytime hours because "the shared understanding is that shop owners are normally open to potential customers." *Id.* at 1151. These norms, moreover, govern not only the time of entry but the manner; entering a business through the back window might be a trespass even when entering through the door is not.

Kerr argues that the process of discerning and applying similar norms should govern "trespass" in the digital realm, and that because the Web is generally perceived as "inherently open," in that it "allows anyone in the world to publish information that can be accessed by anyone else without requiring authentication," courts should incorporate this norm by "adopt[ing] presumptively open norms for the

Web." *Id.* at 1162. This general understanding of the open nature of the Web squares with language used in a recent Supreme Court decision relied on by hiQ. In *Packingham v. North Carolina*, —— U.S. ——, 137 S.Ct. 1730, 198 L.Ed.2d 273 (2017), the Court struck down a North Carolina law making it a felony for a registered sex offender to access social media websites like Facebook and Twitter. The Court explained that at present, social media sites are for many people "the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge." *Id.* at 1737. The Court's analogy of the Internet in general, and social networking sites in particular, to the "modern public square," *id.*, embraces the social norm that assumes the openness and accessibility of that forum to all comers. *Cf. Ampex Corp. v. Cargle*, 128 Cal.App.4th 1569, 1576, 27 Cal.Rptr.3d 863 (2005) ("Web sites that are accessible free of charge to any member of the public where members of the public may read the views and information posted, and post their own opinions, meet the definition of a public forum for purposes of section 425.16 [the California anti–SLAPP statute].").

What would the adoption of such a norm of openness mean for the interpretation of the CFAA? According to Professor Kerr, the upshot is that "authorization," in the context of the CFAA, should be tied to an authentication system, such as password protection:

> The authorization line should be deemed crossed only when access is gained by bypassing an authentication

> requirement. 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. This line achieves an appropriate balance for computer trespass law. It protects privacy when meaningful steps are taken to seal off access from the public while also creating public rights to use the Internet free from fear of prosecution.

Id. at 1161. This approach would square with the results in both *Nosal II* and *Power Ventures* while avoiding the negative consequences of an overly broad reading of "authorization." In both *Nosal II* and *Power Ventures*, the defendants had bypassed a password authentication system. In that sense, their "access" was, as *Nosal II* explained, clearly "without authorization" within the meaning of the CFAA. And while *Nosal II* stated that the term "authorization" has a plain and ordinary meaning, that meaning was in the context of determining whether a former employer could control "access" to its *private* data protected by an authentication process. The plain meaning of "authorization" of "access" as analyzed in *Nosal II* is not so plain when viewed in the context of presumptively open public page on the Internet.

Where a website or computer owner has imposed a password authentication system to regulate access, it makes sense to apply a plain meaning reading of "access" "without authorization" such that "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly." *Power Ventures*, 844 F.3d at 1067. But, as noted above, in

the context of a publicly viewable web page open to all on the Internet, the "plainness" of the meaning of "access" "without authorization" is less obvious. Context matters.

An analogy to physical space, while inevitably imperfect when analyzing the digital world, may be helpful. With respect to a closed space (*e.g.*, behind a locked door which requires a key to pass), the Court intuitively understands that where an individual does not have permission to enter, he would be trespassing if he did so. Even if the door is open to the public for business, the shop owner may impose limits to the manner and scope of access (*e.g.*, by restricting access to a storage or employees-only area). But if a business displayed a sign in its storefront window visible to all on a public street and sidewalk, it could not ban an individual from looking at the sign and subject such person to trespass for violating such a ban. LinkedIn, here, essentially seeks to prohibit hiQ from viewing a sign publicly visible to all.

In sum, viewed in a proper context, the Court has serious doubt whether LinkedIn's revocation of permission to access the public portions of its site renders hiQ's access "without authorization" within the meaning of the CFAA. Neither *Nosal I*, *Nosal II*, nor *Power Ventures* so hold.

Lastly, with respect to the CFAA, LinkedIn argues in part that what it objects to is not merely hiQ's access to the site, but hiQ's automated scraping of user data. But "authorization," as used in CFAA § 1030(a)(2), is most naturally read in reference to the *identity* of the person accessing the computer or website, not *how* access occurs. *Cf. Nosal I*, 676 F.3d

at 857–59 (distinguishing between unauthorized access to versus use of data). Thus, Professor Kerr persuasively argues that where an individual employs an automated program that bypasses a CAPTCHA—a program designed to allow humans but to block "bots" from accessing a site—he has still not entered the website "without authorization." Unlike a password gate, a CAPTCHA does not limit access to certain individuals; it is instead intended "as a way to slow[ ] a user's access rather than as a way to deny authorization to access." Kerr, *supra*, at 1170. Other measures taken by website owners to block or limit access to bots may be thought of in the same way. A user does not "access" a computer "without authorization" by using bots, even in the face of technical countermeasures, when the data it accesses is otherwise open to the public.[9] Thus, under Professor Kerr's analysis, hiQ's circumvention of LinkedIn's measures to prevent use of bots and implementation of IP address blocks does not violate the CFAA because hiQ accessed only publicly viewable data not protected by an authentication gateway.[10]

This is not to say that a website like LinkedIn cannot employ, *e.g.*, anti-bot measures to prevent,

---

[9] To take the analogy above another step, when a business displays a sign in a storefront window for the public to view, it may not prohibit on pain of trespass a viewer from photographing that sign or viewing it with glare reducing sunglasses.

[10] Circumvention of a technological barrier does not automatically give rise to a CFAA violation. *See Nosal II*, 844 F.3d at 1038 (rejecting at least in *dicta* the argument that "the CFAA only criminalizes access where the party circumvents a technological access barrier").

e.g., harmful intrusions or attacks on its server. Finding the CFAA inapplicable to hiQ's actions does not remove all arrows from LinkedIn's legal quiver against malicious attacks.[11]

The Court therefore concludes that hiQ has, at the very least, raised serious questions as to applicability of the CFAA to its conduct.[12] Accordingly, the Court

---

[11] In addition to technological self-help, LinkedIn may be able to pursue other legal remedies. For example, LinkedIn argues that if it cannot invoke the CFAA to prevent unauthorized access by bots, it may be left open to denial of service attacks. However, the CFAA creates liability against "[w]hoever"—whether access is authorized or not—"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." 18 U.S.C. § 1030(a)(5)(A). Additionally, such attacks are likely remediable under, *e.g.*, the common law tort of trespass to chattel. Trespass to chattel requires a plaintiff to prove that a defendant intentionally interfered with plaintiff's use or possession of personal property, with resultant injury. *See* California Civil Jury Instructions 2101; *Itano v. Colonial Yacht Anchorage*, 267 Cal.App.2d 84, 90, 72 Cal.Rptr. 823 (1968). California Courts have recognized that trespass to chattel may be accomplished through purely electronic means. *See Thrifty–Tel, Inc. v. Bezenek*, 46 Cal.App.4th 1559, 54 Cal.Rptr.2d 468 (1996) (upholding trespass to chattel verdict in favor of plaintiff where defendants "employed computer technology" to crack access and authorization codes and make long-distance phone calls without paying for them).

[12] hiQ also argues that the interpretation of the CFAA that LinkedIn urges should be rejected under the canon of constitutional avoidance, because it raises potentially serious problems under the First Amendment. *See Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575, 108 S.Ct. 1392, 99 L.Ed.2d 645 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress."). Because the Court

rejects LinkedIn's interpretation on the grounds discussed above, it need not reach hiQ's First Amendment arguments. The Court observes, however, that the threshold issue of state action presents a serious hurdle to any direct First Amendment claim against LinkedIn in this case. *See, e.g., Brunette v. Humane Society of Ventura County*, 294 F.3d 1205, 1210 (9th Cir. 2002) (private party may be deemed to have engaged in state action if it is a willful participant in joint action with the government; if the government has insinuated itself into a position of interdependence with it; and if it performs functions traditionally and exclusively reserved to the states); *Brentwood Academy v. Tennessee Secondary School Athletic Ass'n*, 531 U.S. 288, 300–301, 121 S.Ct. 924, 148 L.Ed.2d 807 (2001) (state action may be found where private entity is controlled by an agency of the state, when its activity results from the state's exercise of coercive power, when the state provides encouragement, or when government is "entwined" in the entity's policies, management, or control). LinkedIn is not a state official or governmental agency; it is a private party and there is no evidence that the CFAA has served to compel or encourage LinkedIn to withdraw hiQ's authorization to access its website. Compare *Brentwood Academy*, 531 U.S. at 300, 121 S.Ct. 924 (private party's actions may be characterized as state action "when the State provides significant encouragement, either overt or covert") (citation and quotation omitted) with *Blum v. Yaretsky*, 457 U.S. 991, 1005, 102 S.Ct. 2777, 73 L.Ed.2d 534 (1982) (nursing homes' decisions to discharge patients were not state action because they were made by private parties according to professional standards not established by the state, and the simple fact "[t]hat the State responds to such actions by adjusting benefits does not render it *responsible* for those actions"). However, the same interpretation of the statute would apply uniformly to both civil and criminal actions, *see supra* n.7, and a criminal prosecution under the CFAA would undoubtedly constitute state action. Thus, because the act of viewing a publicly accessible website is likely protected by the First Amendment (*see, e.g., Packingham*, 137 S.Ct. at 1737 (statute's prohibition on sex offender access to social media websites raised serious First Amendment concerns because, *inter alia*, "[s]ocial media allows users to gain access to information ...."); *Kleindienst v. Mandel*, 408 U.S. 753, 762–63, 92 S.Ct. 2576, 33 L.Ed.2d 683 (1972) (noting the "variety of

cannot conclude, at this stage, that the CFAA preempts hiQ's affirmative claims under state law. The question then is whether hiQ is entitled to preliminary injunctive relief not only against enforcement of the CFAA but also against the use of technological barriers. To obtain such relief, hiQ would have to raise at least serious questions as to whether it has rights under state laws which are violated by LinkedIn's conduct. The Court thus turns to those state claims.[13]

---

contexts [in which] this Court has referred to a First Amendment right to receive information and ideas") (quotation omitted); *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 782, 98 S.Ct. 1407, 55 L.Ed.2d 707 (1978) (the First Amendment plays a role to protect "not only" "individual self-expression but also ... affording public access to discussion, debate, and the dissemination of information and ideas"); *Board of Edu., Island Trees Union Free School Dist. No. 26 v. Pico*, 457 U.S. 853, 867, 102 S.Ct. 2799, 73 L.Ed.2d 435 (1982) (noting that the right to receive information "is an inherent corollary of the rights of free speech and press that are explicitly guaranteed by the Constitution"); *cf. Branzburg v. Hayes*, 408 U.S. 665, 684–85, 92 S.Ct. 2646, 33 L.Ed.2d 626 (1972) (explaining that "[n]ewsmen have no constitutional right of access to the scenes of crime or disaster when the general public is excluded," perhaps suggesting that the right extends at least to information to which the general public has access), the doctrine of constitutional avoidance might well be properly considered in interpreting the CFAA, even if the First Amendment were not directly implicated in this particular case. *See Sosa v. DIRECTV, Inc.*, 437 F.3d 923, 932, 942 (9th Cir. 2006) (statute should be construed to avoid burdening First Amendment interests where possible). The doctrine of constitutional avoidance, if applicable, would substantiate the Court's doubt about the applicability of the CFAA to hiQ's conduct.

[13] For the same reasons, the Court concludes that hiQ has raised serious questions about whether provisions of the California analog to the CFAA, California Penal Code § 502, referring to unauthorized access apply to the conduct here. *Cf.*

2. California Constitutional Claim

hiQ argues that LinkedIn's actions violate California's constitutional free speech protections. Article I, Section 2 of the California Constitution provides that "[e]very person may freely speak, write, and publish his or her sentiments on all subjects." The California Supreme Court has long recognized that this provision confers broader free speech rights than those provided by the First Amendment. *See Dailey v. Superior Court of City & Cty. of San Francisco*, 112 Cal. 94, 97–98, 44 P. 458 (1896). In particular, unlike the First Amendment, California's provision is not limited to restraining state entities. The California Supreme Court, in its landmark decision in *Robins v. Pruneyard Shopping Ctr.*, 23 Cal.3d 899, 905, 153 Cal.Rptr. 854, 592 P.2d 341 (1979), held that the state's guarantee of free expression may take precedence over the rights of private property owners to exclude people from their property. *Robins* concerned attempts by a large shopping mall to exclude individuals engaging in political speech. In holding that this speech was protected by the state constitution, the court emphasized the importance of the shopping mall as a public forum and center of community life, a place where "25,000 persons are induced to congregate

---

City of Los Angeles, 155 Cal.App.4th 29, 34, 65 Cal.Rptr.3d 701 (2007) (noting that "[s]ection 502 defines 'access' in terms redolent of 'hacking' or breaking into a computer"). Though the statute also includes a provision that prohibits "knowingly access[ing] and without permission tak[ing], cop[ying], or mak[ing] use of any data from a computer, computer system, or computer network," Cal. Pen. Code § 502(c)(2), the Court similarly concludes there are serious questions about whether these provisions criminalize viewing public portions of a website.

daily to take advantage of the numerous amenities offered." *Id.* at 910, 153 Cal.Rptr. 854, 592 P.2d 341.

hiQ argues that LinkedIn is an internet-age equivalent to the Pruneyard Shopping Center. hiQ notes that like the shopping center, "LinkedIn opens the public profile section of its website to the public. LinkedIn promises its members that the public profiles on its site can be viewed by everyone." Motion at 17. Moreover, LinkedIn "expressly holds itself out as a place 'to meet, exchange ideas, [and] learn,' ... making it a modern-day equivalent of the shopping mall or town square, a marketplace of ideas on a previously unimaginable scale." *Id.* For that reason, hiQ argues, it has a right under the California Constitution to access that marketplace on equal terms with all other people and that LinkedIn's private property rights in controlling access to its computers cannot take precedence. *Cf. Nicholson v. McClatchy Newspapers*, 177 Cal.App.3d 509, 223 Cal.Rptr. 58 (1986) (concluding that under federal case-law, "[w]hile reporters are not privileged to commit crimes and independent torts in gathering the news, and the press has no special constitutional right of access to information, 'news gathering is not without its First Amendment protections'") (quoting *Branzburg*, 408 U.S. at 707, 92 S.Ct. 2646). *See generally Beeman v. Anthem Prescription Management, LLC*, 58 Cal.4th 329, 341, 165 Cal.Rptr.3d 800, 315 P.3d 71 (2013) ("The state Constitution's free speech provision is at least as broad as and in some ways is broader than the comparable provision of the federal Constitution's First Amendment.") (citations and quotations omitted); *Dailey*, *supra,* 112 Cal. at 97–98, 44 P. 458.

No court has expressly extended *Pruneyard* to the

Internet generally. Although the California Supreme Court has held that, under *Pruneyard*, "the actions of a private property owner constitute state action for purposes of California's free speech clause only if the property is freely and openly accessible to the public," *Golden Gateway Center v. Golden Gateway Tenants Assn.*, 26 Cal.4th 1013, 1033, 111 Cal.Rptr.2d 336, 29 P.3d 797 (2001), this discussion occurred in the context of real property. Though certain spaces on the Internet share important characteristics of the traditional public square, *see*, *e.g.*, *Packingham*, 137 S.Ct. at 1737 (characterizing social network sites as "the modern public square"), at this juncture, the Court has doubts about whether *Pruneyard* may be extended wholesale into the digital realm of the Internet. No court has had occasion to so hold or to consider the reach and potentially sweeping consequences of such a holding. For instance, would all publicly viewable websites on the Internet be subject to constitutional constraints regardless of size of the business? Does *Pruneyard*, which involves a single owner of the public forum (the shopping center), apply to a website which constitutes only a portion of the Internet and where there is no single controlling entity? Would the entire Internet or only a particular collection of websites constitute a public forum? If the Internet were a public forum governed by constitutional speech, would social network sites such as Facebook be prohibited from engaging in any content-based regulation of postings? The analogy between a shopping mall and the Internet is imperfect, and there are a host of potential "slippery slope" problems that are likely to surface were *Pruneyard* to apply to the Internet.

It is true that a number of California state courts

have determined that publicly accessible websites may constitute public fora within the meaning of the state's anti–SLAPP law. In *Ampex Corp.*, the California Court of Appeal held that postings made on an internet message board constituted speech in a public forum for the purposes of the statute. The court explained that "[t]he term 'public forum' includes forms of public communication other than those occurring in a physical setting. Thus the electronic communication media may constitute public forums. Web sites that are accessible free of charge to any member of the public where members of the public may read the views and information posted, and post their own opinions, meet the definition of a public forum *for purposes of section 425.16*." *Ampex Corp.*, 128 Cal.App.4th at 1576, 27 Cal.Rptr.3d 863 (emphasis added). The reach of the anti–SLAPP statute is broader than the scope of constitutionally protected speech; it applies to a cause of action arising from an act "in furtherance of" the person's right of free speech under the constitution. Cal. Civ. Proc. Code § 425.16(b); *Ampex Corp.*, 128 Cal.App.4th at 1575, 27 Cal.Rptr.3d 863; *cf. Lieberman v. KCOP Television, Inc.*, 110 Cal.App.4th 156, 166, 1 Cal.Rptr.3d 536, 542 (2003) (explaining that the anti–SLAPP law's protections are "not limited to the exercise of [the] right of free speech, but to all conduct *in furtherance* of the exercise of the right to free speech in connection with a public issue" (emphasis in original)).

Similarly, in *Barrett v. Rosenthal*, 40 Cal.4th 33, 51 Cal.Rptr.3d 55, 146 P.3d 510 (2006), two physicians brought an action for libel and libel per se against a health activist who had posted messages attacking the physicians' character to publicly

accessible Internet newsgroups. The California Supreme Court agreed with the Court of Appeals that "[w]eb sites accessible to the public ... are 'public forums' for the purposes of the anti–SLAPP statute." *Id.* at 41 n.4, 51 Cal.Rptr.3d 55, 146 P.3d 510. As in *Ampex*, however, this holding was limited to whether the defendant could invoke the anti–SLAPP statute's protections. Indeed, the Court of Appeals in that case had treated the speech in question as "act or acts ... taken '*in furtherance* of [her] right of petition or free speech'" under the anti–SLAPP law. *Barrett v. Rosenthal*, 114 Cal.App.4th 1379, 9 Cal.Rptr.3d 142, 149 (Ct. App. 2004) (emphasis added).

Because the anti–SLAPP statute protects conduct beyond constitutionally protected speech itself, neither *Ampex Corp.* nor *Barrett* can be read to hold that the Internet generally is a public forum subject to Art. I, Section 2 of the California Constitution. In light of the potentially sweeping implications discussed above and the lack of any more direct authority, the Court cannot conclude that hiQ has at this juncture raised "serious questions" that LinkedIn's conduct violates its constitutional rights under the California Constitution.

3. UCL Claim

hiQ next argues that LinkedIn's decision to block its access to member data was made for an impermissible anticompetitive purpose—namely that it wants to monetize this data itself with a competing product—and that its conduct therefore constitutes "unfair" competition under California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200 *et seq*.

The UCL broadly prohibits any "unlawful, unfair

or fraudulent business act or practices." *Id.* Practices are "unfair" when grounded in "some legislatively declared policy or proof of some actual or threatened effect on competition." *Cel–Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal.4th 163, 187, 83 Cal.Rptr.2d 548, 973 P.2d 527 (1999). One such set of policies are those embodied in the federal antitrust laws. *Id.*; *see also Blank v. Kirwan*, 39 Cal.3d 311, 320, 216 Cal.Rptr. 718, 703 P.2d 58 (1985) (noting that California law looks to the Sherman Act for guidance). Significantly, however, "unfair" practices under the UCL are not limited to actual antitrust violations, but also include "conduct that threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition." *Cel–Tech*, 20 Cal.4th at 187, 83 Cal.Rptr.2d 548, 973 P.2d 527.

hiQ argues that LinkedIn's conduct violates the spirit of the antitrust laws in two ways: First, "LinkedIn is unfairly leveraging its power in the professional networking market to secure an anticompetitive advantage in another market—the data analytics market." Motion at 11. hiQ asserts that LinkedIn is taking advantage of its dominant position in the field of professional networking to secure a competitively unjustified advantage in a different market. Second, hiQ argues that LinkedIn's conduct violates the "essential facilities" doctrine, "which precludes a monopolist or attempted monopolist from denying access to a facility it controls that is essential to its competitors." *Id.* at 12. The Court agrees that hiQ has raised serious questions with respect to its claim that LinkedIn is

unfairly leveraging its power in the professional networking market for an anticompetitive purpose.

The Sherman Act prohibits companies from leveraging monopoly power to "foreclose competition or gain a competitive advantage, or to destroy a competitor." *Otter Tail Power Co. v. United States*, 410 U.S. 366, 377, 93 S.Ct. 1022, 35 L.Ed.2d 359 (1973). In this case, hiQ plausibly asserts that LinkedIn enjoys a position as the dominant power in the market of professional networking. Furthermore, hiQ has presented evidence that LinkedIn is seeking to compete with hiQ in the market of data analytics. In a news segment airing on national television on June 21, 2017, LinkedIn's CEO announced that "[w]hat LinkedIn would like to do is leverage all this extraordinary data we've been able to collect by virtue of having 500 million people join the site ... to make sure that each individual member has information about where those jobs are" and that "[f]or employers, [the goal is to provide] an understanding of what skills they're gonna need to be able to continue to grow, and where that talent exists." Docket No. 34 (Gupta Decl.) Ex. U. at 2. In other words, LinkedIn appears to be developing a product that competes directly with hiQ's Skill Mapper product, which helps employers understand what skills the members of their workforces possess. There is thus a plausible inference that LinkedIn terminated hiQ's access to its public member data in large part because it wanted exclusive control over that data for its own business purposes; as noted above, hiQ faces an existential threat. That inference is supported by the timing of the commencement of its employer product which appears to coincide roughly with its terminating hiQ's access.

LinkedIn argues that it acted solely out of concern for member privacy, but, as discussed above, that argument is put in question by the fact that LinkedIn itself makes user data available to third parties. hiQ also points to other litigation in which LinkedIn has taken the position that its members have no privacy interest in the information they choose to make public. In *Perkins v. LinkedIn Corp.*, No. 13–cv–4303–LHK (N.D. Cal.), LinkedIn members brought a putative class action against LinkedIn alleging that it wrongfully harvested their contacts' email addresses and repeatedly sent emails soliciting them to join LinkedIn without the members' consent. LinkedIn argued that its communications included only information which the plaintiffs in that case had "chos[en] to make public." Gupta Decl. Ex. W at 23. Of course, hiQ here seeks also to collect only information which users have chosen to make public.

To be sure, LinkedIn may well be able to demonstrate it was not motivated by anticompetitive purposes and that there is in fact no threatened anti-trust violation; instead, it is motivated by a desire to preserve user privacy preferences and its users' trust. But, 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 policy or spirit" of the Sherman Act. *Cel–Tech*, 20 Cal.4th at 187, 83 Cal.Rptr.2d 548, 973 P.2d 527. While hiQ will have to do much more to prove such a claim, it has raised at least serious enough questions on the merits of its UCL claim at this juncture to support the issuance of a preliminary injunction.

4. Promissory Estoppel

Lastly, hiQ argues that it is likely to prevail on claims under the common law of promissory estoppel.[14] This claim appears meritless. hiQ bases its promissory estoppel on LinkedIn's alleged promise to its users that they control the visibility of their data. By restricting hiQ's access to public member data, hiQ contends that LinkedIn has reneged on that promise with respect to members who want their data to be publicly available to all viewers. But 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, and there is no indication that LinkedIn has made any promises to users that their data may be used in that way. Thus, LinkedIn's restrictions in hiQ's collection do not violate any promise made to its users. Moreover, hiQ has not cited any authority applying promissory estoppel to a promise made to someone *other* than the party asserting that claim. For instance, hiQ does not claim to be a cognizable third party beneficiary of such promise or that even that a third party beneficiary doctrine applies to promissory estoppel.

C. Public Interest

At the final step of its preliminary injunction

---

[14] hiQ also asserts a common law claim of tortious interference with contract, but the California Supreme Court has held that such a claim is foreclosed as long as the defendant "had a legitimate business purpose which justified its actions." *Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal.4th 26, 57, 77 Cal.Rptr.2d 709, 960 P.2d 513 (1998). For that reason, the analysis of the tortious interference claim simply overlaps with the analysis of the unfair competition claim: if LinkedIn acted for an improper anticompetitive purpose, then the tortious interference claim may lie; if, on the other hand, it acted out of legitimate concern for member privacy, then the claim fails.

analysis, the Court must consider where the public interest lies. Here, each party contends that the public interest favors its position, because each party believes that its position will maximize the free flow of information. hiQ argues that a private party should not have the unilateral authority to restrict other private parties from accessing information that is otherwise available freely to all. Granting such authority, hiQ argues, would raise serious constitutional questions, as it would delegate to private parties the sole authority to decide who gets to participate in the marketplace of ideas located in the "modern public square" of the Internet. Moreover, at issue is the right to receive and process publicly available information. In view of the vast amount of information publicly available, the value and utility of much of that information is derived from the ability to find, aggregate, organize, and analyze data.

LinkedIn, by contrast, argues that in addition to safeguarding its users' privacy, *its* position is actually the speech-maximizing position. It contends that if its users knew that their data was freely available to unrestricted collection and analysis by third parties for any purposes, they would be far less likely to make such information available online. Granting an injunction, therefore, will have a substantial chilling effect on the very speech that makes the Internet the modern equivalent of the public square.

For present purposes, the Court concludes that the public interest favors hiQ's position. As explained above, the actual privacy interests of LinkedIn users in their *public* data are at best uncertain. It is likely that those who opt for the public view setting expect their public profile will be subject to searches, date mining, aggregation, and analysis. On the other

hand, conferring on private entities such as LinkedIn, the blanket authority to block viewers from accessing information publicly available on its website for any reason, backed by sanctions of the CFAA, could pose an ominous threat to public discourse and the free flow of information promised by the Internet.

Finally, given the Court's holding that hiQ has raised serious questions that LinkedIn's behavior may be anticompetitive conduct in violation of California's Unfair Competition Law, a preliminary injunction leans further in favor of the public interest. *See*, *e.g.*, *American Exp. Co. v. Italian Colors Restaurant*, 133 U.S. 2304, 133 S.Ct. 2304, 2313, 186 L.Ed.2d 417 (2013) (noting "the public interest in vigilant enforcement of the antitrust laws").

IV. CONCLUSION

In sum, the Court concludes that: (1) the balance of hardships tips sharply in hiQ's favor; (2) hiQ has raised serious questions going to the merits of its UCL claim and the applicability of the CFAA; and (3) the public interest favors a preliminary injunction. For these reasons, the Court **GRANTS** hiQ's motion for a preliminary injunction and **ORDERS** as follows:

1. Defendant LinkedIn Corporation and its officers, agents, servants, employees, and attorneys are hereby enjoined from (1) preventing hiQ's access, copying, or use of public profiles on LinkedIn's website (*i.e.*, information which LinkedIn members have designated public, meaning it is visible not just to LinkedIn members but also to others, including those who may access LinkedIn's website via Google, Bing, other services, or by direct URL) and (2) blocking or putting in place any mechanism (whether legal or technical) with the effect of blocking hiQ's

access to such member public profiles. To the extent LinkedIn has already put in place technology to prevent hiQ from accessing these public profiles, it is ordered to remove any such barriers within 24 hours of the issuance of this Order.

2. Defendant LinkedIn Corporation and its officers, agents, servants, employees, and attorneys shall withdraw the cease and desist letters to hiQ dated May 23, 2017 and June 24, 2017. LinkedIn shall refrain from issuing any further cease and desist letters on the grounds therein stated during the pendency of this injunction.

3. This preliminary injunction shall take effect immediately.

4. No bond shall be required, as Defendant has not demonstrated it is likely to be harmed by being so enjoined.

This order disposes of Docket No. 23.

IT IS SO ORDERED.

APPENDIX C

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 17-16783

HIQ LABS, INC.,

Plaintiff-Appellee,

v.

LINKEDIN CORPORATION,

Defendant-Appellant.

Appeal from the United States District Court for the Northern District of California Edward M. Chen, District Judge, Presiding, D.C. No. 3:17-cv-03301-EMC

[Filed November 8, 2019]

Before: WALLACE and BERZON, Circuit Judges, and BERG,* District Judge.

ORDER

The panel has unanimously voted to deny appellant's petition for rehearing. Judge Berzon has voted to deny the petition for rehearing en banc. Judge Wallace and Judge Berg recommend denial of the petition for rehearing en banc.

The full court has been advised of the petition for rehearing en banc, and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

---

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

The petition for rehearing is denied and the petition for rehearing en banc is rejected.

APPENDIX D

18 U.S.C. § 1030

Fraud and related activity in connection with computers

Effective: November 16, 2018

(a) Whoever--

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

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

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained

in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

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

(C) information from any protected computer;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(C) a fine under this title or imprisonment for not

more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

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

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

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

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

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

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

(III) physical injury to any person;

(IV) a threat to public health or safety;

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

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

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

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

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

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

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

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

offense under this section; or

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

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

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

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

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

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

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

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

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

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

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

section.

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

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

(e) As used in this section--

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

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

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

the financial institution or the Government; or

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

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

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

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

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

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

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

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

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

(G) the Securities Investor Protection Corporation;

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

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

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

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

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

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

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

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

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information

to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

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

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

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

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

(a)(5).

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

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

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

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

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

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

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