No. 17-16783

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

HIQ LABS, INC.,

Plaintiff-Appellee,

v.

LINKEDIN CORP.,

Defendant-Appellant.

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

No. 17-cv-03301-EMC

BRIEF OF *AMICUS CURIAE* CRAIGSLIST, INC. IN SUPPORT OF DEFENDANT/APPELLANT LINKEDIN CORP.

Perry J. Viscounty
LATHAM & WATKINS LLP
505 Montgomery Street
Suite 2000
San Francisco, CA 94111
Phone: (415) 391-0600
Fax: (415) 395-8095

Gregory G. Garre
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
Phone: (202) 637-2200
Fax: (202) 637-2201

Attorneys for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus curiae* craigslist, Inc. states that it is a privately held company, it has no publicly traded corporate parent or subsidiary, and no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

Page(s)

OTHER AUTHORITY

STATEMENT OF INTEREST OF *AMICUS CURIAE*

craigslist, Inc. ("craigslist") is the owner and operator of the craigslist.org website, which began as an email list for San Francisco events in 1995. Through years of hard work, expense, and efforts to enhance its users' experience, craigslist has developed one of the world's most popular websites, offering a simple and trusted—and mostly free[1]—classifieds platform for seeking employment, housing, goods and services, companionship, and community information. The popularity and success of craigslist's website is due, in no small part, to craigslist's dedication to user experience—*i.e.*, maintaining a website that is easily accessible and navigable (without mandatory log-ins, passwords, or other barriers), but with sufficient safeguards, rules, policies, and enforcement to earn and keep the trust of its users.

In some instances, individuals and entities have attempted to exploit the craigslist website and user base in a manner that threatens to undermine users' trust in the craigslist platform and runs counter to users' expectations regarding their control over the content they post. For example, bad actors have attempted to "scrape" information from the craigslist website to populate knock-off websites or

---

[1] Users may access the craigslist website and view and respond to any craigslist listing, free of charge. Posting content to the craigslist website is also free for the vast majority of users; only a small percentage of users—mostly commercial entities—are charged a nominal posting fee.

to identify targets for unsolicited email, text, or phone-based marketing campaigns. This conduct harms craigslist's users. For example, when a user advertises an apartment for rent on the craigslist website, the user expects to stop receiving calls after she rents the apartment and removes the listing. However, when a third party scrapes the rental posting and reposts it elsewhere, the user loses control over the posting and may continue to receive call for days, weeks, and even months after she has removed the posting from craigslist.

craigslist thus takes action against unpermitted scrapers to protect its users and website. Those actions have included both (1) implementing technological measures aimed at precluding bad actors from accessing craigslist's computers and, specifically, from scraping data, including craigslist's users' contact information; and (2) employing legal mechanisms to stop and deter the bad actors, including the revocation of permission to access the site under threat of remedies afforded by the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 et seq.

For example, craigslist was forced to initiate litigation in 2012 against 3taps, Inc. ("3taps") and related entities, to enforce craigslist's rights against the unauthorized retrieval of information from craigslist's website and servers. 3taps enlisted the help of off-shore contractors and engineers and deployed an evolving arsenal of technological weapons to circumvent craigslist's barriers for the purpose

of systematically harvesting *all* of the content from craigslist's website. The district court in that case (Breyer, J.) recognized that the CFAA plainly protected craigslist from such unauthorized access and abuse. The broad language of the District Court's opinion in the present case, however, has the potential to negatively impact the ability of a wide range of website owners, including craigslist, to protect their users, websites, and businesses through both technological and legal means.

Accordingly, craigslist has a direct stake in the proper resolution of LinkedIn's appeal and submits this *amicus* brief to provide the Court with additional facts and insights, based on craigslist's first-hand experience, regarding the potentially dangerous impact of the District Court's decision in this case.[2]

[2] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), craigslist states that no one, except for craigslist and its counsel, authored this brief in whole or in part, or contributed money towards the preparation of this brief. LinkedIn and hiQ have, through counsel, consented to the filing of this brief.

INTRODUCTION

One key question implicated by this appeal is whether the CFAA prevents an internet user from continuing to scrape data from a publicly accessible website *after* receipt of a cease and desist letter from the website owner that expressly notifies the recipient that the scraping is prohibited and the recipient is, therefore, not authorized to access the website. The plain language of the CFAA, as well as this Court's recent decision in *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), *petition for cert. filed*, No. 16-1105 (U.S. Mar. 9, 2017), compels that this question be answered in the affirmative. Such conduct constitutes access to a computer "without authorization" and thus triggers the protection of the CFAA. That is, in fact, the exact conclusion that the district court reached four years ago in *craigslist v. 3taps, Inc.*, 964 F. Supp. 2d 1178, 1183-84 (N.D. Cal. 2013) (Breyer, J.), a case involving similar circumstances. The District Court in this case, however, reached the opposite conclusion. In doing so, the court contravened the plain and unambiguous text of the CFAA, departed from this Court's precedent, and established a rule that risks jeopardizing the ability of website owners to protect themselves and their users from bad actors.

The following scenario illustrates the problems with the District Court's decision:

> Company A has a novel and innovative idea for an online platform that would be useful for tens of millions of individuals throughout the world.

> Company A invests decades' worth of time and effort into building the platform and attracting the user base. Company A implements rules for use of the platform to protect its users' postings from misappropriation and misuse. The users trust Company A to enforce those rules and, thus, they submit content, including personal contact information, for display on the online platform.
>
> Company B decides to build a business based on the exploitation of the user-submitted content (including user contact information) on Company A's platform. Company B ignores Company A's rules and hires "skilled hackers" to scrape all of the content from the platform. Company B then makes that content available to any and all spammers, scammers, and other third parties who want it, regardless of their intended use of the content. Company A's users complain that the content they submitted has been hijacked and they have become the targets of spam, scams, and other forms of unwanted contact.
>
> Company A notifies Company B, in writing and in no uncertain terms, that Company B is no longer allowed to access the website. Company A also implements technological blocks aimed at preventing Company B from accessing the website and exploiting Company A's users. Company B uses a variety of means to evade those blocks and continues scraping Company A's website.
>
> Unfortunately, that illustration is not a hypothetical. Rather, it comes

straight from the facts underlying the *3taps* case, in which Judge Breyer found that, "under the plain language of the [CFAA], 3taps was 'without authorization' when it continued to pull data off of craigslist's website after craigslist revoked its authorization to access the website." 964 F. Supp. 2d at 1183-84. Ultimately, the case resulted in judgments and injunctions against 3taps, its various alter egos, and two of its "customers," barring their scraping activities. The ability of craigslist to utilize both technological blocks and the CFAA were instrumental in craigslist stopping 3taps and protecting its users and website from such abuse.

The District Court's decision in the present case, however, puts at risk the users of publicly accessible online websites—such as those created by craigslist, LinkedIn, and countless others accessed daily by millions of Americans. If applied broadly, the District Court's reasoning could eliminate a key legal protection—the CFAA—that Congress extended to the public and that website owners have used for years to protect their users and websites. And the District Court did not stop there. Its interpretation of California's Unfair Competition Law ("UCL") could be read as eliminating a website owner's ability to use technology to prevent bad actors from accessing the website owners' computer servers, so long as the bad actors' business is dependent on such access for survival.

The District Court's decision is not only wrong as a matter of law, but also establishes a potentially dangerous precedent that could unravel the protections available to website owners against bad actors who seek to scrape their data. Accordingly, craigslist urges the Court to reverse the decision below.

BACKGROUND

Hundreds of millions of Americans access the internet each day—often many times a day—to obtain information or avail themselves of services from online websites like craigslist, LinkedIn, and others, which have enhanced and improved their lives and businesses. Unfortunately, not everyone who accesses such websites does so for legitimate purposes. There are also bad actors who

access websites not for the purpose of availing themselves of the authorized information or services offered to the public, but instead to systematically "scrape"—or steal—information from the websites to use for *unauthorized* purposes. Because the *3taps* litigation illustrates craigslist's experience with such bad actors, we begin by summarizing the key facts of that case.

In April 2010, an ad appeared on the craigslist website seeking a "Skilled Hacker at Scraping Web Content." The ad was placed by an individual who had decided to launch a crusade—under the name "3taps"—to steal all of craigslist's publicly accessible content and user contact information and distribute it (for profit) to any third party who wanted the data, regardless of motive or intended use. As a result of the ad, 3taps hired an expatriate computer hacker who was apparently living on a boat in the Caribbean to evade U.S. law enforcement while he scraped (in his own words) "over 7,500 sites like craigslist, Twitter, Groupon, Zagat, and others." 3taps' hired gun then built a "Scraper Machine" designed to continuously scrape all content from the craigslist website. 3taps indiscriminately made the scraped content, including users' contact information, available to anyone who signed up for the 3taps "data feed."

3taps' unauthorized scraping and indiscriminate distribution of information taken from craigslist's computers directly and negatively impacted craigslist's users. For example, two of 3taps' "customers" were online apartment rental start-

ups—Lovely and Padmapper—that used the data from scraped craigslist apartment listings to populate their own websites. Importantly, when users post classified ads to the craigslist website, which often include their personal contact information, they do so with certain expectations. Those expectations are typically founded, at least in part, on craigslist's Terms of Use ("TOU"), which govern the access to, and use of, the website by all users.

For example, craigslist's users expect (1) to maintain control over their advertisement, including the ability to remove it when the listed item is sold or rented; and (2) their information will only be used or displayed in connection with the craigslist advertisement that they created. Specifically, those who post apartment listings to craigslist do so with the expectation that they will have control over the content of the ad (the price, the descriptions, etc.), as well as its life span—*i.e.*, the poster will control when the ad is taken down, such as when they find a tenant. 3taps' actions violated those expectations.

Once 3taps scraped the ads from the craigslist website, they could be relisted elsewhere without the users' knowledge or consent, and the users lost control over their ads and were negatively impacted, as described in the unsolicited complaints that they submitted to craigslist. For example, users[3] stated:

- "I regularly post apartment rental listings on Craigslist for a building I

[3] Comments on file with authors.

> manage, and find Craigslist more effective than any other website for this purpose. Recently I have discovered that all our apartment listings are being scraped and copied from Craigslist by Lovely (livelovely.com).
>
> This scraping and copying is unauthorized by me, and obviously prohibited by Craigslist's terms of Use. Even more frustrating is the fact that every time Lovely steals one of our listings from Craigslist, their algorithm/software introduces serious factual errors into the text."

- "I posted my ad . . . yesterday for an extra room in my house that I'm looking to rent. A person showed up to my house today, unannounced, and that said they saw my posting on the website: https://www.padmapper.com. I only posted my ad on craigslist, and have a problem with my information being shared with other websites. If this site is taking information without the user's permission, then it seems craigslist should have a problem with this practice, and make sites such as padmapper stop. If this is an acceptable practice of craigslist, then I would like to know, and I will no longer use the site."

To combat scrapers like 3taps—and protect its users—craigslist spent a great deal of time, effort, and resources in developing and implementing sophisticated technological measures to block the scrapers from accessing its website. But 3taps then sought to circumvent those efforts by engaging teams of foreign and domestic hackers to develop sophisticated workarounds to evade the blocks and continue exploiting craigslist's website and users. craigslist blocked IP addresses associated with 3taps and, in response, 3taps cycled through 300,000+ IP addresses per day, and utilized various anonymity services and botnets. craigslist implemented measures specifically aimed at protecting its users' contact information, and 3taps

responded by bombarding craigslist's servers with over 10,000 scraper requests every minute aimed solely at users' contact information.

craigslist routinely monitors spam traffic that is routed through its computer system to protect its users. Each time craigslist implemented a sophisticated new block that temporarily stopped 3taps' scraping, craigslist observed *dramatic* reductions in the volume of spam sent to its users in the immediate aftermath of the block. The drastic drops in spam traffic following craigslist's blocking efforts underscores how fully spammers relied on scraped craigslist content to carry out their unlawful email campaigns. And, unfortunately, when 3taps discovered means to circumvent those blocks, the volume of spam spiked again.

3taps' scraping efforts blatantly violated craigslist's TOU and robots.txt instructions. For example, craigslist's TOU prohibits the use of "[r]obots, spiders, scripts, scrapers, [and] crawlers" and the collection of "users' personal and/or contact information." *See* craigslist, Terms of Use, http://www.craigslist.org/about/terms.of.use (last visited Oct. 10, 2017). Moreover, craigslist's robots.txt instructions prohibit even authorized indexers of the craigslist website (*i.e.*, general purpose search engines, such as Google) from accessing the portions of craigslist's website that contain users' contact information.

While craigslist expended massive amounts of time and effort to stop 3taps from scraping and to protect its users through various technological blocks, equally

important was craigslist's ability to utilize the CFAA as a legal enforcement mechanism to stop 3taps' misconduct. After craigslist learned of 3taps' activities, it sent 3taps a cease and desist letter expressly revoking any preexisting permission to access the craigslist website and instructing 3taps to stop its unauthorized activities. 3taps nevertheless continued to access the website and wreak the havoc described above. Accordingly, craigslist brought suit against 3taps and certain related entities, asserting claims under, among other laws, the CFAA.

The district court denied 3taps' motion to dismiss craigslist CFAA's claims on largely the same grounds that hiQ Labs asserted here (*see 3taps*, 964 F. Supp. 2d at 1183-84) and, ultimately, enjoined each of the defendants from scraping craigslist's website. At that point, finally, the scraping stopped.

ARGUMENT

This appeal tests the scope of the CFAA in protecting the operators of online websites, and the public more generally, from individuals or entities that access websites not for the purpose of availing themselves of information or services under the Terms of Use, but instead to systematically scrape information from the websites—"without authorization" from either the website owners or the individuals who provided the information—to use the information for improper purposes. Critical to the resolution of that issue is understanding the ways in which bad actors have exploited access to such websites to steal the information

compiled on the websites for unintended purposes. craigslist's experience in the *3taps* litigation underscores both the threat that website owners and their users face and the important safeguard that the CFAA provides.

I. Website Owners Like craigslist and LinkedIn Invest Tremendous Time and Resources to Develop Useful, Popular Online Platforms and to Protect the Content Entrusted to Those Platforms.

To understand the importance of the CFAA and other measures that may be deployed to protect and preserve the successful operation of a popular, publicly accessible website such as craigslist or LinkedIn, it is necessary to consider how such a website becomes a sought after and trusted resource for millions of users in the first place. It is also crucial to consider that one negative implication of that popularity is to make the website an attractive target for unscrupulous actors. As craigslist's experience illustrates, to grow from humble beginnings to massive popularity and public utility typically requires tremendous investments of time and resources, both to build the website and user base and, equally important, to protect the website and its users from exploitation once the website takes off.

A. craigslist Invested Enormous Time and Resources to Build an Online Classified Advertisement Platform that Millions of Users Trust with Their Information Daily.

Founded in San Francisco in 1995, craigslist has grown from a local email list for friends and coworkers to one of the world's most popular websites. Today, tens of millions of users rely on craigslist's simple and trusted localized classified

advertisement platform to buy and sell goods and services. The explosive growth of craigslist's popularity and user base can be largely attributed to craigslist's dedication to user experience and safety. To enhance the user experience, the craigslist website is simple to use, with no required log-ins or passwords needed to access and browse the website. craigslist nevertheless protects its users, and earns their trust, by combatting unwanted spam and scams and the unauthorized harvesting or use of user content and personal information by third parties. Like many otherwise successful, publicly available websites, craigslist expressly prohibits such conduct in its TOU.

Authorized users who abide by craigslist's TOU may search, browse, and respond to postings listed on the website. Additionally, authorized users who affirmatively agree to craigslist's TOU may post classified ads on the craigslist.org website, primarily free of charge. Users post classified ads to the craigslist website, often with their personal contact information included, with certain expectations. For example, users expect (1) to maintain control over their advertisement, including the ability to remove it when the listed item is sold or rented; and (2) that their information will only be used or displayed in connection with the specific craigslist advertisement that they created.

When scrapers harvest the content from the craigslist website and repurpose it for their own ends—such as by selling it to spammers or using the data to

populate their own competing classified advertising website—the users lose control over their ads, lose trust in the craigslist platform, and are often subjected to intrusive and unwanted contact from the scrapers or the scrapers' customers. The wholesale automated harvesting of information from craigslist's website is prohibited by craigslist's TOU, is antithetical to the business model that helped craigslist grow into one the nation's most popular websites, and presents an unwanted threat to the millions of users who post on craigslist.

B. craigslist Makes Every Effort to Protect Its Users and the Information They Entrust to the Website from Bad Actors.

craigslist has gone to great lengths to protect its users and the information they entrust to the craigslist website, without compromising the accessibility and public nature of the website which attracted the user base in the first place. For example, craigslist has invested heavily in developing a wide range of protective measures, ranging from laying the basic ground rules for interacting with the craigslist website (*e.g.*, publishing a TOU and robots.txt file) to implementing an array of highly sophisticated technological measures to enforce those rules (*e.g.*, spam filters, IP blocks, anti-scraping measures, user contact information protections, etc.). Like many website owners, craigslist is engaged in a perpetual technological arms race to combat bad actors.

Unfortunately, however, these measures are not always enough to stop bad actors from exploiting the public accessibility of a website like craigslist's and

harvesting information for unauthorized purposes. And when such protective efforts are not, by themselves, enough to stop bad actors, craigslist—and other similarly situated website owners—needs the threat of potent legal consequences to buttress its rules-based and technological enforcement efforts. The CFAA—as written by Congress and as interpreted by this Court—provides exactly that.

II. As the *3taps* Litigation Underscores, The CFAA is a Critical Tool in Combatting Bad Actors and Protecting the Owners and Users of All Websites, Whether Publicly Accessible or Otherwise.

A. The CFAA is Plain and Unambiguous.

The CFAA authorizes civil and criminal penalties against any person who "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).[4] The statute further grants a private right of action to the victims of such unauthorized activities for "compensatory damages and injunctive

---

[4] The full text of the relevant provision states:

> (a) Whoever–
> . . . .
> (2) intentionally accesses ***a computer*** without authorization or exceeds authorized access, and thereby obtains–
> . . . .
> (C) ***information*** from any protected computer;
> . . . .
> shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(2)(C) (emphases added).

relief or other equitable relief." *Id*. § 1030(g).

The statute is clear and unambiguous in three important respects:

First, it applies to "computer[s]," as defined to include any computer "used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B). It does not distinguish between "private computers," "nonpublic computers," or "password-protected computers"; but rather, applies to *all* computers used in or affecting interstate or foreign commerce, without qualification. That includes computers used to host internet websites, which users access when they enter the website. *See, e.g., United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) ("protected computer" means "effectively all computers with Internet access").

Second, the statute protects "information" (18 U.S.C. § 1030(a)(2)(C)), without distinguishing between "public" or "nonpublic" information, including whether information is password-protected or not.

And *third*, the statute is triggered when someone intentionally seeks to access information on a computer "without authorization." *Id.* § 1030(a)(2). As this Court recognized in *United States v. Nosal*, "the plain and ordinary meaning of the words 'without authorization'" is clear-cut: "'authorization' means 'permission or power granted by an authority'"; and thus, someone "'accesses a computer "without authorization" when he gains admission to a computer without

approval.'" 844 F.3d 1024, 1034-37 (9th Cir. 2016) (citations omitted).

Thus, under its plain and unambiguous terms, the CFAA applies to *any* information obtained from *any* computer that was accessed *without approval*.

B. This Court's Holding in *Power Ventures* Confirms that Whether Access was "Unauthorized" Under the CFAA Hinges on *Notice*, Not the Public/Private Nature of a Website.

Last year, this Court clearly articulated the dispositive question when determining whether access to an online website is "without authorization" under the CFAA: Did the defendant access the website to obtain information after the defendant's "permission [to access it] has been revoked explicitly"? *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016). If so, then the access was "without authorization" and, thus, actionable under the CFAA. *Id.*

Power Ventures involved a suit brought by Facebook under the CFAA against a company (Power Ventures) that accessed Facebook users' data and then initiated emails and other electronic messages promoting its own website. When Facebook learned of these activities, it sent Power Ventures a cease and desist letter that "plainly put Power [Ventures] on notice that it was no longer authorized to access Facebook's computers," and sought to block its access to Facebook's website. *Id.* at 1067 n.3. Power Ventures nevertheless continued to access Facebook's website after it received the cease and desist letter. *Id.* at 1067-68.

This Court had little difficulty holding that Power Ventures was liable under

the CFAA. As the Court explained, because Power Ventures had continued to access Facebook's computers (through its website) "after receiving written notification from Facebook" that it should cease and desist its activities, Power Ventures "accessed Facebook's computers 'without authorization' within the meaning of the CFAA and is liable under that statute." *Id.* at 1068.

Nowhere in its *Power Ventures* opinion did this Court make any reference to—much less rely on—the public or private nature of the Facebook website (or portions thereof) or any password-authentication requirement associated with Facebook's website, computers, or data.[5] The particular characteristics of how Facebook's computers operated, or how the information was obtained from them, did not factor into the Court's analysis at all. And that is not surprising, given that, as explained above, the CFAA does not in any way differentiate the "computers" or "information" covered by the Act based on any of those factors.

C. The *3taps* Court Correctly Recognized that the CFAA Protects Publicly Accessible Websites from Unauthorized Scraping after Express Notice and Revocation of Permission to Access.

The Court's analysis in *Power Ventures* applies equally to the situation where an entity enters a publicly accessible website for the purpose of scraping its

---

[5] In fact, millions of Facebook and LinkedIn users alike have chosen to make their profiles public and accessible to nearly every person in the world with a computer or mobile device connected to the internet. That does not change the protections afforded to website owners under the CFAA.

content after it has been told to cease and desist its activities, because in that scenario all the same elements are present: (1) access to a "computer" through a website, (2) to obtain "information," (3) after the entity has been told in no uncertain terms to cease and desist its scraping activities. The District Court below nevertheless concluded that the protections of the CFAA are limited to situations where the website is "protected by a password authentication system." That is incorrect, as the *3taps* decision underscores.

In *3taps*, Judge Breyer held that "under the plain language of the [CFAA], 3Taps was 'without authorization' when it continued to pull data off of [c]raigslist's website after [c]raigslist revoked its authorization to access the website." 964 F. Supp. 2d at 1183-84. As he explained:

> [c]raigslist gave the world permission (i.e., "authorization") to access the public information on its public website. Then, just as [*LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009)] instructed that an "authority" can do, it rescinded that permission for 3Taps. Further access by 3Taps after that rescission was "without authorization."

Id. at 1184; *see also Facebook, Inc. v. Grunin*, 77 F. Supp. 3d 965, 972 (N.D. Cal. 2015) (citing *3taps* approvingly and finding violation of CFAA where "Facebook sent two cease-and-desist letters to Grunin and . . . took technical measures to block Grunin's access to Facebook's site and services, [but] Grunin nonetheless continued to access Facebook's site and services").

In so holding, Judge Breyer rejected the argument that the CFAA was

somehow inapplicable because craigslist had made "the classified ads on its website publicly available." *3taps*, 964 F.2d at 1182 (record citations omitted). As he explained, the fact that craigslist made the information publicly available (rather than password-protected) "does not answer the question here, which is whether [c]raigslist had the power to revoke, on a case-by-case basis, the general permission it granted to the public to access the information on its website." *Id.* And on that question, Judge Breyer held, "the plain language of the statute" requires an affirmative answer. *Id.* at 1183.

Not only is the term "without authorization" clear and unambiguous, but Congress declined to write a statute that distinguished between "public" and "nonpublic" information. Indeed, as Judge Breyer explained:

> Congress might have written § 1030(a)(2) to protect only "nonpublic" information. A neighboring provision in the CFAA includes that very modifier, and prohibits access without authorization to "nonpublic" government computers. *See* 18 U.S.C. § 1030(a)(3). Another adjacent provision applies only to certain kinds of financial information. *See* § 1030(a)(2)(A). ***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***.

Id. at 1182-83 (emphasis added); *see also Keene Corp. v. United States*, 508 U.S. 200, 208 (1993) ("Where Congress includes particular language in one section of a statute but omits it in another . . . it is generally presumed that Congress acts intentionally and purposefully in the disparate inclusion or exclusion." (alteration

in original) (citation omitted)).

The District Court's reliance in this case on a "password authentication" requirement for CFAA claims involving data obtained from an online website is directly at odds with Judge Breyer's well-reasoned decision in the *3taps* case, not to mention the plain text of the statute and this Court's decision in *Power Ventures*. Moreover, if adopted by this Court, the District Court's analysis would threaten to eviscerate a powerful legal tool that has been relied upon by website owners—including craigslist—to protect themselves and their users from unscrupulous actors that continue to access their computers and scrape information after being told in no uncertain terms that they are *un*authorized to do so.

III. Adopting the District Court's Decision in This Case Would Invite Bad Actors to Scrape the Contents of Popular and Publicly Available Websites Like craigslist and LinkedIn.

A. The District Court's Decision Invites Bad Actors to Attempt to Exploit Owners and Users of Publicly Accessible Websites.

The District Court's atextual, password-authentication requirement risks opening the door for the 3taps' of the world to target publicly accessible websites and their users with impunity. As described above, 3taps and its band of offshore hackers scraped the data, including users' contact information, from millions of ads posted on craigslist on a daily basis. 3taps then made that data indiscriminately available to third parties to use for whatever potentially nefarious purposes they wanted. craigslist and its users felt the very real impacts of 3taps' abuse of the

craigslist website, as the users were harassed by telemarketers and scammers, and lost control over their listings as they were repurposed for display on other websites without the users' knowledge or consent.

While particularly egregious, the 3taps saga is not an isolated event, either for craigslist or other website owners. Rather, craigslist must constantly stay vigilant to protect its website and users from bad actors who, like 3taps, seek to scrape and exploit craigslist and its users for their own commercial gain. In craigslist's experience, those unscrupulous actors include, among other variations, startups seeking to piggy back on craigslist's success and amass user bases with minimal time and effort, as well as scammers/spammers who collect users' email addresses and phone numbers to send unsolicited (often highly misleading) commercial messages to craigslist's users.

craigslist's users have complained—including to both craigslist and to the scrapers themselves—about the negative impacts of the scrapers' actions. For example:

- "[REDACTED] is reposting my ads on the[ir] web site from my craigslist ad with my phone number and pictures and showing units I have deleted as currently rentable. They have even gone to my address of my building and put up a sign on the property. They have no number to call from their website and I don't know what to do. . . . [W]hat suggestion do you have for me to stop this abuse[?]"
- "A few months back, I advertised my car for sale and I sold it over Craigslist. Over the last few days, I started getting texts about my car being for sale. One person said they found my car over an app called

> [REDACTED]. The interesting thi[ng] is that I never even heard of [REDACTED] until yesterday . . . . I never downloaded their app, nor advertised my car with them. . . . I am not a user, nor did I give consent to be contacted by potential buyers over [REDACTED]. They said they removed the ad, but I am frustrated."

- "I have recently sold a car through a private CL transaction. Few days later, I get a message from someone looking to buy the same car & said that they saw it from the [REDACTED] app, which I thought was odd. I only posted the car ad in CL. I honestly don't like the idea of CL sharing my ad and/or having these Car Apps make their own ad for me."

- "FYI a place called [REDACTED] has pulled my ad[] off craigslist and is pestering me to sell through them."

- "I am getting unwanted solicitation from [REDACTED] on my CL posting of my vehicle for sale. It seems that they are calling all vehicle posts regardless of whether or not they say they want solicitation or not."

- From a user-submitted craigslist ad: "ATTN [REDACTED], stop calling me. I have no interest in paying you to relist my vehicle. You are the reason CraigsList says 'do NOT contact me with unsolicited services or offers.'"

In short, publicly available websites, such as those operated by craigslist, LinkedIn, and others, are targets for bad actors who harm the website owners and users by accessing such websites without authorization and stealing information to use for unauthorized purposes. Website owners need potent legal tools, such as the CFAA, to protect themselves and their users. Here, the District Court's opinion threatens to eviscerate the CFAA as a viable mechanism for the owners of publicly accessible websites to protect their users, websites, and businesses from malicious actors such as 3taps and other scrapers, spammers, and scammers.

B. The District Court's Decision Also Threatens to Restrict Speech on the Internet and Lessen Public Access to Valuable Information and Services.

At the same time, the District Court's decision in this case would create a perverse incentive for website owners to *restrict* the public's access to important and helpful information. For many legitimate reasons, a website operator may choose to adopt password or related restrictions, including authentication codes, for accessing information on its website. But it is also perfectly appropriate for a website to make its information easier for the public to access—by forgoing passwords, log-ins, or other authentication barriers.

By conditioning the availability of the CFAA's important protections on the use of a "password authentication" requirement or the like, the District Court's decision creates a legal incentive to constrain the public's access to information. Yet there is absolutely no indication that Congress intended that result, and such a rule would surely draw the ire of millions of Americans who enjoy the ease of access to important information on websites like craigslist.

At a bare minimum, this Court should insist upon a clear indication of intent from Congress before adopting a rule that would have such a speech-restricting effect on the internet, one of the most important engines for speech ever created.

IV. The District Court Erred in Invoking California UCL as Basis for Preventing Website Owners From Employing Technological Measures to Block Bad Actors and Protect Authorized Users.

The District Court's decision in this case is flawed in another important respect, distinct from its misguided interpretation of the CFAA. The District Court not only limited the CFAA as a safeguard in protecting against bad actors unless a website operator can meet the District Court's added, "password-authentication" requirement, but also took the incredible step of preliminarily enjoining LinkedIn from using *any* technological means to stop hiQ from scraping the LinkedIn website. In doing so, the District Court fundamentally misapplied the UCL in a manner that, if upheld, would have troubling implications for the owners and users of publicly available websites.

To succeed on the merits, hiQ's asserted UCL claim requires an actual or incipient antitrust violation. But there can be no antitrust violation where one company merely prevents another from accessing data residing on its servers. *See* LinkedIn Br. 19-22; *Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 411 (2004) (recognizing that "there is no duty to aid competitors"); *see also Novell, Inc. v. Microsoft Corp.*, 731 F.3d 1064, 1074 (10th Cir. 2013) (Gorsuch, J.) ("Even a monopolist generally has no duty to share (or continue to share) its intellectual or physical property with a rival."). Nevertheless, the District Court found that hiQ's UCL claim warranted injunctive relief because

hiQ's business depends on continuously scraping information from LinkedIn's servers for its survival. That is incorrect.

Enjoining a website operator from using technological measures to prevent unauthorized access to its website is not only an absurd result under the law, but it creates at least two significant policy concerns. First, compelling companies "to share the source of their advantage [*e.g.*, the data contained on their websites] is in some tension with the underlying purpose of antitrust law, since it may lessen the incentive" for companies to innovate and invest in useful platforms such as those created by craigslist, LinkedIn, and others. *Trinko*, 540 U.S. at 407-08.

Second, enjoining website operators from using technological protective measures would create perverse incentives for second-movers and bad actors. Indeed, it would *embolden them* to scrape and steal an established competitor's online data, knowing they could then turn around and claim unfair competition by simply alleging that their businesses would fail without the scraped content. The more they rely on a competitor's hard-earned data, the greater the "hardship" they would suffer if enjoined and, thus, the less the victimized competitor can do to stop them. In the 3taps context, for example, the District Court's reasoning could have allowed 3taps to scrape with impunity and continue abusing craigslist's users for years pending a decision on the merits.

There is no basis, under the UCL or otherwise, to reward bad actors, such as

3taps, at the expense of innocent users of publicly available websites, simply because they base their business model on unauthorized scraping. And website operators like craigslist and LinkedIn have every right to employ technological measures to block such unauthorized scraping on their websites and, when need be, invoke the legal protections of the CFAA against such abuses.

CONCLUSION

For the foregoing reasons, the District Court's decision should be reversed.

Respectfully submitted,

October 10, 2017

s/ Perry J. Viscounty
Perry J. Viscounty
LATHAM & WATKINS LLP
505 Montgomery Street
Suite 2000
San Francisco, CA 94111
Phone: (415) 391-0600
Fax: (415) 395-8095

Gregory G. Garre
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
Phone: (202) 637-2200
Fax: (202) 637-2201

Attorneys for Amicus Curiae

CERTIFICATION OF COMPLIANCE

Counsel for *amicus curiae* craigslist, Inc. certifies:

1. This brief complies with the type-volume limitation of Federal Rules of Appellate Procedure 29(a)(5) and Ninth Circuit Rules 32-1(a) because this brief contains 6,346 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because this brief has been prepared in proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font type.

s/ Perry J. Viscounty
Perry J. Viscounty

Attorney for Amicus Curiae

Dated: October 10, 2017

CERTIFICATE OF SERVICE

I hereby certify that on this 10th day of October, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system, which will send notice of such filing to all participants in the case who are registered CM/ECF users.

s/ Perry J. Viscounty
Perry J. Viscounty