Corey Worcester (*pro hac vice*)
coreyworcester@quinnemanuel.com
Renita Sharma (*pro hac vice*)
renitasharma@quinnemanuel.com
QUINN EMANUEL URQUHART AND SULLIVAN LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000

Terry L. Wit (SBN 233473)
terrywit@quinnemanuel.com
QUINN EMANUEL URQUHART AND SULLIVAN LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6331

*Attorneys for Plaintiff and Counterclaim Defendant hiQ Labs, Inc.*

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

hiQ Labs, Inc.,

*Plaintiff and Counterclaim Defendant*,

vs.

LinkedIn Corp.,

*Defendant and Counterclaim Plaintiff.*

Case No. 3:17-cv-03301-EMC

**PLAINTIFF AND COUNTERCLAIM DEFENDANT HIQ LABS, INC.'S MOTION TO DISMISS AND STRIKE IN PART DEFENDANT AND COUNTERCLAIM PLAINTIFF LINKEDIN CORP.'S COUNTERCLAIMS**

Judge: Hon. Edward M. Chen
Hearing Date: April 8, 2021
Hearing Time: 1:30 p.m.

**TABLE OF CONTENTS**

**Page**

## TABLE OF AUTHORITIES

**Page**

**Cases**

**Statutory Authorities**



**Rules and Regulations**

## NOTICE OF MOTION AND MOTION

PLEASE TAKE NOTICE THAT on April 8, 2021 at 1:30 p.m., or as soon thereafter as may be heard, before the Honorable Edward M. Chen in Courtroom 5, 17th Floor, 450 Golden Gate Avenue, San Francisco, CA 94102, Plaintiff and Counterclaim Defendant hiQ Labs, Inc. ("hiQ") will and hereby does move this Court for an order dismissing the Counterclaims filed by Defendant and Counterclaim Plaintiff LinkedIn Corp. (ECF No. 170 (LinkedIn's Answer and Counterclaims or "ACC")). This motion is made pursuant to Federal Rule of Civil Procedure 12(b)(6) and Federal Rule of Civil Procedure 12(f) and is based upon the following Memorandum of Points and Authorities; the argument of counsel; and any additional material as may be submitted to the Court before decision. hiQ seeks an order dismissing LinkedIn's counterclaims with prejudice for failure to state a claim upon which relief can be granted and striking in part LinkedIn's request for remedies for its claim of breach of contract.

## PRELIMINARY STATEMENT

LinkedIn's counterclaims against hiQ are a transparent attempt by LinkedIn to pose as a defender of user privacy by characterizing hiQ as a "scraper" and a "free rider." But as the Ninth Circuit previously found, "LinkedIn's own actions undercut its argument[s]" regarding user privacy. *hiQ Labs, Inc. v. LinkedIn* Corp., 938 F.3d 985,994-95 (9th Cir. 2019). Far from crusading for justice, LinkedIn is campaigning for its own bottom line and improperly attempting to use its counterclaims to shut down fair competition. LinkedIn's counterclaims fail to state a claim against hiQ and must be dismissed, and LinkedIn's request for injunctive or continuing remedies for its claim of breach of contract should be struck.

*First*, LinkedIn fails to state a claim under the Computer Fraud and Abuse Act because, under the Ninth Circuit's opinion in this case (and opinions that have followed it since), "accessing publicly available data" does not "constitute access without authorization under the CFAA." *Id.* at 1003. As LinkedIn cannot allege that the data accessed by hiQ was not accessible to the general public, LinkedIn's claim must be dismissed.

*Second*, LinkedIn fails to state a claim under the California Comprehensive Computer Data Access and Fraud Act because such claims "rise or fall" with claims under the Computer Fraud and

Abuse Act. *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 131 (N.D. Cal. 2020) (internal quotations omitted). As such, LinkedIn's CDAFA claim must be dismissed.

*Third*, while LinkedIn purports to state a claim for ongoing breaches by hiQ of LinkedIn's User Agreement that entitle LinkedIn to injunctive relief, hiQ is no longer a user of LinkedIn and thus is not bound by LinkedIn's User Agreement. As such, LinkedIn's claim that hiQ "continues to" breach the User Agreement should be dismissed, and any claim for injunctive relief or for relief accrued past the date of termination of the User Agreement should be struck.

*Fourth*, LinkedIn fails to state a claim for misappropriation of "data from the LinkedIn site," because LinkedIn has not and cannot allege that it owned the allegedly misappropriated data. In addition, to the extent LinkedIn alleges that hiQ misappropriated data that is non-public or would not be public but for LinkedIn's efforts, LinkedIn's claim would be preempted by the California Uniform Trade Secret Act.

*Fifth and finally,* LinkedIn fails to state a claim for trespass to chattels because LinkedIn does not allege demonstrable, compensable harm.

For each of the foregoing reasons, LinkedIn has failed to state a counterclaim against hiQ and hiQ respectfully requests that the Court grant its motion to dismiss LinkedIn's counterclaims and its motion to strike with prejudice.

## BACKGROUND & PROCEDURAL HISTORY

hiQ was formed in July 2012 to serve previously-unmet needs among employers (particularly large employers, such as Fortune 500 companies) to assist in employee development and retention by analyzing the full scope of current and potential employees' skills and identifying those employees that were at the highest risk of leaving the company. (ECF No. 131 at 2-3.) hiQ did so by researching and utilizing wholly public information individuals chose to share via their professional social networking on LinkedIn, a site focused on business and professional networking that currently has over 500 million users. (*Id.* at 3.) LinkedIn permits users to upload a wide variety of professional content to its service and to choose their preferred level of privacy protection for that information. LinkedIn users may choose to keep their profiles (or portions of their profiles) entirely private, or to make them viewable by: (1) their direct connections on the site; (2) a broader network of indirect

connections; (3) all of LinkedIn's users; or (4) the entire public. In all cases, and according to LinkedIn's User Agreement, LinkedIn *users* own the content and information that they post to LinkedIn, not LinkedIn itself. *See* User Agreement[1], § 3.1.

hiQ does not analyze the private sections of LinkedIn, such as profile information that is only visible to signed-in users, or users' non-public data that is visible only to other users with whom they are "connected." (ECF No. 131 at 3.) Rather, hiQ uses software to access and analyze wholly public information visible to anyone on the internet without logging into the service.

For years, LinkedIn knew about and sanctioned hiQ's services and activities, including by attending hiQ's own conferences. (*Id.*) As hiQ grew, however, LinkedIn apparently decided that it wanted to profit from providing the same type of innovative and revolutionary analytics hiQ pioneered, and it developed its own competing version of that analytics service. In conjunction with that development, in May 2017, LinkedIn abruptly denied hiQ access to the portion of the LinkedIn website containing wholly public user profiles. (*Id.* at 4.) And on May 23, 2017, LinkedIn sent hiQ a cease-and-desist letter ordering hiQ to stop accessing LinkedIn and asserting that hiQ's continued access to the website violated the Computer Fraud and Abuse Act ("CFAA"), Digital Millennium Copyright Act ("DMCA") and California Penal Code § 502(c) (the "CDAFA") and constituted common law trespass to chattels. (*See* ECF No. 23-1 Ex. J.)

Deprived of access to the data that provides the foundation of its analytics, hiQ filed a complaint against LinkedIn on June 7, 2017, seeking a declaration that hiQ had not violated and would not violate federal or state law, including the CFAA, DMCA, and CDAFA, by accessing and copying wholly public information from LinkedIn's website. (ECF No. 1 at 1.) hiQ also moved for

[1] LinkedIn's User Agreement is an exhibit to, and incorporated in, hiQ's First Amended Complaint. (ECF No. 131 (hiQ's First Amended Complaint) at ¶ 20; ECF No. 131-1 (January 6, 2020 LinkedIn User Agreement).) The User Agreement is also referenced numerous times in LinkedIn's counterclaims (*see* ACC at 29 (¶¶ 7, 8), 31 (¶ 13), 35-36 (¶¶ 36, 37, 38, 41, 43), 37 (¶¶ 51, 52, 53)) and is cited therein via internet hyperlink (*id.* ¶ 36 n.10 (citing User Agreement available at https://www.linkedin.com/legal/user-agreement)). As such, the User Agreement may be considered by this Court on a motion to dismiss. *Beverly Oaks Physicians Surgical Center, LLC v. Blue Cross and Blue Shield of Illinois*, 983 F.3d 435, 439 (2020) (on a motion to dismiss, courts may "consider materials that are submitted with and attached to the complaint; judicial notice of matters of public record; and unattached evidence on which the complaint necessarily relies if: (1) the complaint refers to the document; (2) the document is central to the plaintiff's claim; and (3) no party questions the authenticity of the document.") (internal quotation omitted).

injunctive relief to prohibit LinkedIn from preventing hiQ's access, copying, or use of public profiles on LinkedIn's website. (ECF No. 3; see also ECF No. 23 (hiQ's Renewed Motion for Temporary Restraining Order).)

On August 14, 2017, this Court granted hiQ's request for preliminary injunction. This Court determined that the "key question" presented by hiQ's motion was "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." (ECF No. 63 at 10.) The Court held that it was not.

Following an extensive analysis, this Court concluded that the CFAA, which was enacted as an anti-hacking statute, "was not intended to police traffic to publicly available websites on the Internet." (*Id.* at 10.) As such, the Court had "serious doubts whether LinkedIn's revocation of permission to access the public portions of its site render[ed] hiQ's access 'without authorization' within the meaning of the CFAA." (*Id.* at 15.) The Court was similarly skeptical of LinkedIn's claim that the CFAA should at least be read to limit hiQ's automatic scraping of data, finding that "'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." (*Id.* (emphasis in original).) As such, 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." (*Id.* at 16.) Therefore, the Court concluded that hiQ had raised serious questions as to the merits of its claims for declaratory relief under the CFAA.

The Court also concluded that hiQ had raised serious questions going to the merits of its affirmative claim under the California Unfair Competition Law, that public interest favored a preliminary injunction, that hiQ had established irreparable harm absent an injunction, and that the balance of hardships tipped "sharply in hiQ's favor." (*Id.* at 7, 25.) This Court ordered LinkedIn to withdraw its cease-and-desist letters, and enjoined LinkedIn from preventing or blocking hiQ's access, copying, or use of public profiles on LinkedIn's website. (*Id.* at 25.)

LinkedIn immediately appealed this Court's preliminary injunction. (ECF No. 72.) On September 9, 2019, the Ninth Circuit issued an opinion affirming hiQ's right to access public

information individuals chose to share on LinkedIn. *hiQ Labs, Inc. v. LinkedIn* Corp., 938 F.3d 985 (9th Cir. 2019).

In pertinent part for this Motion, the Ninth Circuit affirmed this Court's conclusion that hiQ had raised serious questions going to the merits of LinkedIn's defense based on the CFAA. As had this Court, the Ninth Circuit found that 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." *Id*. at 999. The Court found that the "wording of the statute" suggested that it applied where the "baseline [was that] access is not generally available and so permission is ordinarily required." *Id*. at 1000. As such, the Court found 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." *Id*. at 1001. By contrast, "[i]t 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." *Id*. at 1003. As "[t]he 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 had "therefore raised serious questions about whether LinkedIn may invoke the CFAA." *Id*. at 1003-04. The Ninth Circuit also found that the balance of hardships posed by an injunction "tip[ped] decidedly" in hiQ's favor and affirmed the issuance of the injunction. *Id*. at 995.

After the Ninth Circuit remanded the case to this Court, hiQ filed an amended complaint, which reasserted hiQ's claims for declaratory judgment and asserted antitrust claims under the Sherman and Clayton Acts. (ECF No. 131.) LinkedIn moved to dismiss hiQ's antitrust claims and all claims for damages, asserting that its conduct was protected by the *Noerr-Pennington* doctrine and California litigation privilege. (ECF No. 137.)

The Court denied LinkedIn's motion to dismiss on the basis of the *Noerr-Pennington* doctrine or California litigation privilege, but granted LinkedIn's motion to dismiss the antitrust claims on the basis that hiQ had failed to adequately allege a product market or anticompetitive conduct by LinkedIn. (ECF No. 158 at 21.) LinkedIn filed its answer and counterclaims on November 11, 2020. (ECF No. 170.)

LinkedIn asserts five counterclaims against hiQ: under the Computer Fraud and Abuse Act (18 U.S.C. § 1030, the "CFAA") and the California Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code § 520 et seq. (the "CDAFA")), and for breach of contract, misappropriation, and trespass to chattels.[2] hiQ now respectfully moves this Court for an order dismissing LinkedIn's counterclaims.

## LEGAL STANDARD

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. "Plausibility requires pleading facts, as opposed to conclusory allegations," *Somers v. Apple, Inc.*, 729 F.3d 953, 959 (9th Cir. 2013), and "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555. Plausibility requires "more than a sheer possibility that a defendant has acted unlawfully," and "[w]here a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief." *Iqbal*, 556 U.S. at 678 (quotation marks and citation omitted).

## ARGUMENT

### I. LINKEDIN HAS NOT PLED A CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT OR CALIFORNIA PENAL CODE § 502

The CFAA was enacted as a prohibition on computer network hacking and 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." 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

[2] In a footnote, LinkedIn states that the "question of whether the CFAA applies to unauthorized access to webpages that are not behind a password wall is raised in the petition for a writ of certiorari that LinkedIn filed with the Supreme Court of the United States," and that LinkedIn "pleads this cause of action to preserve it." ACC at 44 n.15. It appears that, by this footnote, LinkedIn intends to concede that, as hiQ argues, the Ninth Circuit's Opinion in this case requires that LinkedIn's counterclaim be dismissed.

authorization; and (2) obtaining access with authorization but then using that access improperly." *Musacchio v. United States*, 136 S. Ct. 709, 713 (2016).

LinkedIn claims that hiQ's conduct violates the CFAA because, *first*, LinkedIn's "website and servers are not unconditionally open to the general public" as "they require authorization or permission from LinkedIn to access," which hiQ did not have. ACC at 44-45, ¶ 90. *Second*, LinkedIn claims that, to the extent hiQ did have authorization, "any authorization" was "revoked . . . when [LinkedIn] sent the May 23, 2017 cease-and-desist letter." *Id.* at 45, ¶ 91.

LinkedIn has failed to state a claim against hiQ for violations of the CFAA because—as LinkedIn does not contest—the data that hiQ accessed was accessible to the general public. Therefore, neither the purported technical barriers nor LinkedIn's May 23, 2017 letter change the conclusion mandated by the Ninth Circuit's holding in this case: that "accessing publicly available data" does not "constitute access without authorization under the CFAA." *hiQ Labs*, 938 F.3d at 1003. While the Ninth Circuit's Opinion was "in the context of a motion for injunctive relief," courts within the Ninth Circuit have "f[ound] that its reasoning is persuasive in determining . . . [a] dismissal motion." *Miller v. 4Internet, LLC*, 471 F. Supp. 3d 1085, 1090 (N.D. Cal. 2020); *see also Brodsky*, 445 F. Supp. 3d at 110 (relying on Ninth Circuit opinion to dismiss claim under the CFAA). This Court should do the same.

### A. hiQ Did Not Act Without Authorization And Did Not Access Non-Public Information

The Ninth Circuit's reasoning in its opinion affirming this Court's Preliminary Injunction Order requires the dismissal of LinkedIn's counterclaim under the CFAA. The Ninth Circuit concluded that hiQ had not acted "without authorization" under the CFAA because a "user's accessing . . . publicly available data will not constitute access without authorization under the CFAA." *hiQ Labs*, 938 F.3d at 1003. This is because "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.'" *Id.* at 1000. In support of its conclusion, the Ninth Circuit cited the legislative history of the CFAA, a statute that had originally been "limited to a narrow range of computers—none of . . . which . . . were accessible to the general public." *Id.* at 1001. The Court stated that this history

"mad[e] 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." *Id*. As such, the Ninth Circuit held "that hiQ has raised a serious question as to whether the reference to access 'without authorization' limits the scope of the statutory coverage to computer information for which authorization or access permission, such as password authentication, is generally required." *Id.*

In an apparent attempt to distinguish the Ninth Circuit's holding, LinkedIn argues that its "website and servers are not unconditionally open to the general public" because "LinkedIn has invested significant technical and human resources to detect, limit, and block data scraping." ACC at 28 (¶ 6), 45 (¶ 90). LinkedIn argues that hiQ circumvented these alleged barriers by, *inter alia*, masking its IP addresses, which is prohibited by LinkedIn's User Agreement. *Id.* at 45, ¶ 90.

The purported distinction drawn by LinkedIn is immaterial. According to the Ninth Circuit, "authorization is only required [by the CFAA] for password-protected sites or sites that otherwise prevent the general public from viewing the information." *hiQ Labs*, 938 F.3d at 1001. LinkedIn does not contend that either its User Agreement or its purported technological barriers limited the general public's ability to view its websites. As such, under the Ninth Circuit's reasoning, the CFAA's "concept of 'without authorization' is inapt." *Id.* at 1002.

Moreover, as this Court stated in its Preliminary Injunction Order, "'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." (ECF No. 63 at 15); *see also Brodsky*, 445 F. 3d at 110 (same). As such, "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." (ECF No. 63 at 16.) Accordingly, the simple fact that hiQ accessed LinkedIn's publicly-accessible websites via automatic web crawler does not bring that access within the ambit of the CFAA.

Other courts have affirmed that accessing publicly-available data, even via efforts to evade technical restrictions, or restrictions imposed by terms of use, do not amount to a CFAA violation. For example, in *Facebook, Inc. v. Power Ventures, Inc*., 844 F.3d 1058 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 313 (2017), the Ninth Circuit stated that a "violation of the terms of use of a website—

without more—cannot establish liability under the CFAA." 884 F.3d at 1067; *see also United States v. Nosal* (*Nosal I*), 676 F.3d 854, 862 (9th Cir. 2012) ("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.").

In *Miller v. 4Internet*, the court dismissed a CFAA counterclaim against a service which automatically "crawled the web to search for [and scrape] photos." 471 F. Supp. 3d 1085, 1087, 1091 (D. Nev. 2020). There, counterclaim-plaintiff 4Internet operated an internet search engine. 4Internet alleged that a web crawler used by counterclaim-defendants Andrew Higbee and H&A to scrape 4Internet's site violated the CFAA because it evaded technological barriers, exceeded 4Internet's terms of use, and imposed significant demands on 4Internet's servers. *Id.* at 1087. The court dismissed the counterclaim with prejudice, finding that under the Ninth Circuit's opinion in *hiQ Labs*, the CFAA did not apply because 4Internet "d[id] not allege that the information that Higbee and H&A accessed is the kind for which 'authorization' is required." *Id.* at 1090; *see also Facebook*, 844 F.3d at 1067 ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA.").

Similarly, in *Sandvig v. Barr*, academic researchers brought a pre-enforcement challenge to the imposition of criminal liability under the CFAA. The researchers intended to access and "audit test[]" online hiring websites by "creat[ing] profiles for fictitious job seekers," which would violate the target websites' terms of services. The researchers argued that application of the CFAA to that conduct would violate their constitutional rights, including under the First Amendment. The court, declining to reach that constitutional question, found that the CFAA would not apply to the researchers' proposal because "violating public websites' terms of service, as Wilson and Mislove propose to do for their research, does not constitute a CFAA violation under the 'exceeds authorized access' provision." *Sandvig v. Barr*, 451 F. Supp. 3d 73, 91 (D.D.C. 2020).

The *Sandvig* court based its holding on the Ninth Circuit's reasoning in *hiQ Labs*. While *hiQ Labs* addressed civil liability under the CFAA, the Ninth Circuit had noted that the CFAA's "statutory prohibition on unauthorized access applies both to civil actions and to criminal prosecutions" (*hiQ Labs*, 938 F.3d at 1003) and that it "'must interpret the statute consistently, whether we encounter its

application in a criminal or noncriminal context'" (*id.*, quoting *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004)). As such, the *Sandvig* court found that the Ninth Circuit's reasoning was applicable to criminal liability under the CFAA. The court stated that the Ninth Circuit's analysis "contemplates a view of the internet as divided into at least two realms—public websites (or portions of websites) where no authorization is required and private websites (or portions of websites) where permission must be granted for access." 451 F. Supp. 3d at 85 (emphasis in original). "Adopting th[is] formulation," the court agreed that the CFAA only applied to private websites protected by "permission requirements." *Id.* at 87. The court further found that a website's "terms of service do not constitute 'permission requirements' that, if violated, trigger criminal liability" because "[c]riminalizing terms-of-service violations risks turning each website into its own criminal jurisdiction." *Id.* at 88; *see also Bittman v. Fox*, 107 F. Supp. 3d 896, 900-01 (N.D. Ill. 2015) (concluding that defendants did not "exceed[ ] authorized access" by creating "a fake social media account in violation of a social media company's terms of service"). The same concern, regarding what the *Sandvig* court called an "unworkable and standardless" system, 451 F. Supp. 3d at 88, would apply if civil liability were imposed based solely on the violation of private terms of service.

The opinions in *4Internet and Sandvig* confirm what the Ninth Circuit's holding in this case requires: namely that because LinkedIn concedes that hiQ accessed only publicly available data, hiQ did not violate the CFAA and LinkedIn's counterclaim must be dismissed.

**B. hiQ Did Not Exceed Any Authorization Simply Because It Accessed Public Information After Receiving LinkedIn's May 23, 2017 Cease-and-Desist Letter**

LinkedIn next claims that, even to the extent hiQ had authorization to access its websites, "any authorization" was "revoked . . . when [LinkedIn] sent the May 23, 2017 cease-and-desist letter," rendering future access a violation of the CFAA's prohibition on "exceed[ing] authorized access" to a protected computer. ACC at 44-45, ¶ 91; *see* 18 U.S.C. § 1030(a)(2)(C).

The CFAA defines the term "exceeds authorized access" as meaning "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." 18 U.S.C. § 1030(e)(6). LinkedIn's argument fails because the Ninth Circuit has already determined that "accessing publicly available data" does not

require the website operator's authorization; therefore, that access—even after a cease-and-desist letter—also cannot "exceed" authorization. *See hiQ Labs,* 938 F.3d at 1003.

Moreover, the Ninth Circuit expressly considered the effect of LinkedIn's May 23, 2017 letter, when it determined that "[t]he 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.'" The Court expressed serious doubts that hiQ's conduct after receipt of the letter could amount to a CFAA violation, describing comparisons to the authorities cited by LinkedIn as "inapt". *See id. at* 999, 1002. Accordingly, LinkedIn's threat to "revoke" permission in its May 23, 2017 letter is immaterial to its claim—it has no authority to grant or withdraw "authorization" to access wholly public information. Because LinkedIn concedes that hiQ accessed only publicly available data, hiQ did not violate the CFAA and LinkedIn's counterclaim must be dismissed.

**C. hiQ Has Not Violated California Penal Code § 502**

LinkedIn also alleges that hiQ violated sections 502(c)(1) and (c)(2) of the California Comprehensive Computer Data Access and Fraud Act ("CDAFA") by "knowingly access[ing] LinkedIn's website and servers, and, without permission t[aking], cop[ying] and m[aking] use of data and files from LinkedIn's computers, computer systems, and/or computer networks, including to wrongfully control and/or obtain such data." ACC at 46, ¶¶ 100-01.

"California Penal Code § 502 is the California equivalent of the federal Computer Fraud and Abuse Act." *Nexsales Corp. v. Salebuild, Inc.*, 2012 WL 216260, at *3 (N.D. Cal. Jan. 24, 2012) (citing *Multiven, Inc. v. Cisco Sys., Inc.,* 725 F. Supp. 2d 887, 895 (N.D.Cal.2010) ("the necessary elements of Section 502 do not differ materially from the necessary elements of the [Computer Fraud and Abuse Act]")). As such, "[c]ase law suggests that Plaintiffs' [CDAFA] claims rise or fall with Plaintiffs' CFAA claims because the necessary elements of Section 502 do not differ materially from the necessary elements of the CFAA, except in terms of damages." *Brodsky*, 445 F. Supp. 3d at 131 (internal quotations omitted). For the reasons cited above, LinkedIn's CFAA claim fails because the publicly-accessible data accessed by hiQ does not require "authorization" under the CFAA. Accordingly, LinkedIn's CDAFA allegations against hiQ also fail to state a claim and must be dismissed.

## II. LINKEDIN'S BREACH OF CONTRACT CLAIM SHOULD BE DISMISSED, AND ITS REQUEST FOR REMEDIES STRUCK, AS TO THE PERIOD AFTER THE USER AGREEMENT HAD BEEN TERMINATED

As its third cause of action, LinkedIn claims that hiQ has breached and is currently in breach of LinkedIn's User Agreement. ACC at 47-48, ¶¶ 106-127. LinkedIn claims that the User Agreement "is enforceable and binding on hiQ," that "[a]ny future use of LinkedIn's website by hiQ is subject to the terms of the User Agreement," and that hiQ's alleged breach "caused and continues to cause irreparable harm and injury to LinkedIn." *Id.* at 47-48, ¶¶ 114, 125, & 126. As such, LinkedIn claims that it is entitled to "injunctive relief, declaratory relief, compensatory damages, and/or other equitable relief." *Id.* at 48, ¶ 127.

hiQ disputes that its past conduct constituted a breach of the User Agreement. *See, e.g.*, ECF No. 33 at 13. However, even accepting that there had been any breach, LinkedIn's claim that hiQ "continues to" breach the User Agreement is precluded by the findings of this Court and the Ninth Circuit and should be dismissed. Furthermore, as LinkedIn cannot state a claim for any continuing or ongoing breach of the User Agreement, LinkedIn's claim of injunctive relief or for relief accrued past the date of hiQ's termination should be struck.

*First,* even to the extent that hiQ *was* bound by and breached the User Agreement in the past (which it disputes), LinkedIn fails to state a claim insofar as it claims that the User Agreement is *currently* binding on hiQ. LinkedIn's claim is precluded by the findings of both this Court and the Ninth Circuit. As this Court previously confirmed, while hiQ once had a company page on LinkedIn, "LinkedIn has terminated hiQ's user status." ECF No. 63 at 7 n. 4. The Ninth Circuit also held that "*[h]iQ is no longer bound by the User Agreement*, as LinkedIn has terminated hiQ's user status." 983 F.3d at 991 n. 5 (emphasis added). As such, even to the extent that LinkedIn could state a claim for *past* breaches of its User Agreement, hiQ is no longer bound by that Agreement. LinkedIn's breach of contract claim therefore fails insofar as it purports to claim any breach after the date of LinkedIn's own termination of hiQ's user status.

*Second*, because LinkedIn cannot state a claim for breach of the User Agreement beyond the date of LinkedIn's termination of hiQ, LinkedIn's claim for injunctive and declaratory relief for alleged breach of contract, and its claim for compensatory damages which accrued beyond the date of

termination, must be struck. LinkedIn's clam for injunctive relief for breach of the User Agreement is based on the allegation that hiQ "continues to cause irreparable harm and injury to LinkedIn." ACC at 48, ¶¶ 125-26. However, because hiQ is "no longer bound by the User Agreement," 983 F.3d at 991 n. 5, LinkedIn cannot establish irreparable harm. In the Ninth Circuit, "[m]otions to strike requests for particular remedies will be granted pursuant to Rule 12(f) if such relief cannot be recovered under the applicable law." *Roger v. First Health Corp*., 2009 WL 10672289, at *4 (C.D. Cal. Nov. 19, 2009) (citing *Torrance Redevelopment Agency v. Solvent Coating Co*., 763 F. Supp. 1060, 1057-78 (C.D. Cal. 1991)). As such, insofar as LinkedIn states that it is entitled to injunctive relief because hiQ "continues to cause irreparable harm" by its alleged breach of the User Agreement, or that LinkedIn is entitled to compensatory damages alleged accrued beyond the date of LinkedIn's termination of hiQ, LinkedIn's request for those remedies should be struck under Federal Rule of Civil Procedure Rule 12(f).

## III. LINKEDIN'S MISAPPROPRIATION CLAIM SHOULD BE DISMISSED

As its fourth cause of action, LinkedIn alleges that hiQ misappropriated "data from the LinkedIn site," thereby "reap[ing] what it did not sow." ACC at 48-49, ¶¶ 129-32. LinkedIn fails to state a claim for misappropriation because, *first*, LinkedIn has not and cannot allege that it owned the allegedly-misappropriated data, and *second*, because any such claim would be preempted by the California's California Uniform Trade Secret Act ("CUTSA").

### A. LinkedIn Cannot State a Claim for Misappropriation of Data Owned By LinkedIn's Users

"The elements of a claim for misappropriation under California law consist of the following: (a) the plaintiff invested substantial time, skill or money in developing its property; (b) the defendant appropriated and used plaintiff's property at little or no cost to defendant; (c) the defendant's appropriation and use of the plaintiff's property was without the authorization or consent of the plaintiff; and (d) the plaintiff can establish that it has been injured by the defendant's conduct." *United States Golf Assn. v. Arroyo Software Corp*., 69 Cal. App. 4th 607, 618 (1999). "[I]n order to state a claim based on the taking of information, a plaintiff must show that he has some property right in such information (*i.e.* that the information is proprietary)." *SunPower Corp. v. SolarCity Corp.*,

2012 WL 6160472, at *5 (N.D. Cal. Dec. 11, 2012). LinkedIn's claim therefore fails because it cannot establish the first element of misappropriation: that hiQ appropriated any of *LinkedIn's* property.

While LinkedIn alleges that hiQ appropriated data from LinkedIn's website (ACC at 48, ¶ 130), that data is owned, if at all, by LinkedIn's users, not LinkedIn. *hiQ Labs*, 938 F.3d at 1003 ("The data hiQ seeks to access is not owned by LinkedIn"). LinkedIn's User Agreement states that "as between [users] and LinkedIn, [users] own the content and information that you submit or post to the Services." *See* ECF No. 131-1 (LinkedIn User Agreement) at § 3.1; *see also id.* at § 1.1 (defining Services as "LinkedIn.com, LinkedIn-branded apps, LinkedIn Learning and other LinkedIn-related sites, apps, communications and other services that state that they are offered under this Contract").

Because LinkedIn does not have a property or ownership right in the data that hiQ allegedly misappropriated, LinkedIn cannot state a claim for misappropriation. *See Hollywood Screentest of Am., Inc. v. NBC Universal, Inc.*, 151 Cal. App. 4th 631, 650, 660 Cal. Rptr. 3d 279, 294 (2007) (affirming summary judgment in favor of defendant on misappropriation claim where the interest in dispute was not created by defendant, but by unrelated entities such that "appellants cannot show that NBC appropriated any ideas from appellants."); *see also SunPower Corp.*, 2012 WL 6160472, at *5. As such, LinkedIn's fourth cause of action must be dismissed.

**B. Any Misappropriation Claim Is Preempted By CUTSA**

*Second*, even if LinkedIn could establish the elements of a claim for common law misappropriation (which it cannot), LinkedIn's claim—to the extent LinkedIn alleges that hiQ misappropriated data that is non-public or would not be public but for LinkedIn's efforts—would be preempted by CUTSA, which preempts "claims based on the same nucleus of facts as trade secret misappropriation." *K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc.,* 171 Cal. App. 4th 939, 962 (2009); *see also AccuImage Diagnostics Corp v. Terarecon, Inc.*, 260 F. Supp. 2d 941, 954 (N.D. Cal. 2003) ("[CUTSA] occupies the field in California. Plaintiff's common law misappropriation of trade secrets claim is therefore deemed superseded . . . .").

A plaintiff cannot avoid CUTSA preemption simply by electing not to plead a CUTSA claim. *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 840 (N.D. Cal. 2014) (CUTSA preemption

applies even where plaintiff has not pled a CUTSA claim); *see also SunPower Corp.*, 2012 WL 6160472, at *5 (to find that misappropriation claim was not precluded "would allow plaintiffs to avoid the preclusive effect of CUTSA . . . by simply failing to allege one of the elements necessary for information to qualify as a trade secret."). CUTSA preemption applies even for "claims based on the misappropriation of information that does not satisfy the definition of trade secret under CUTSA," if "the basis of the alleged property right is in essence that the information is not . . . generally known to the public," because then "the claim is sufficiently close to a trade secret claim that it should be superseded." *Lifeline Food Co. v. Gilman Cheese Corp.*, 2015 WL 2357246, at *1 (N.D. Cal. May 15, 2015).

LinkedIn's claim is based on the alleged "substantial investment in time, labor, skill, and financial resources made by LinkedIn" in order to create the data at issue. ACC at 48-49, ¶ 131. LinkedIn alleges that the data "that hiQ took included time-sensitive updates to member profiles," and that hiQ "circumvent[ed] . . . various technical barriers" to "wrongfully access[] LinkedIn's website, computer systems, and servers." ACC at 48, ¶ 130. As such, to the extent LinkedIn alleges that hiQ misappropriated data that is "not . . . generally known to the public," or that would not be generally known but for LinkedIn's efforts, LinkedIn's claim is preempted by CUSTA and must be dismissed.

## IV. LINKEDIN HAS NOT PLED A CLAIM FOR TRESPASS TO CHATTELS

While LinkedIn cannot state a claim for violations of the CFAA because the data accessed by hiQ "has not been demarcated by LinkedIn as private," the Ninth Circuit acknowledged that "state law trespass to chattels claims may still be available" to LinkedIn "at least when it causes demonstrable harm." *hiQ Labs*, 938 F.3d at 1003, 1004, 1004 at n.15. In this instance, however, LinkedIn cannot state a claim for trespass to chattels because LinkedIn does not allege demonstrable, compensable harm.

"[I]n the context of trespass to a computer system or other similar devices, injury is adequately alleged where the plaintiff pleads 'that the purported trespass: (1) caused physical damage to the personal property, (2) impaired the condition, quality, or value of the personal property, or (3) deprived plaintiff of the use of personal property for a substantial time.'" *Grace v. Apple Inc.*, No. 17-CV-00551, 2017 WL 3232464, at *11 (N.D. Cal. July 28, 2017).

LinkedIn alleges that hiQ trespassed by "intentionally interfer[ing] with LinkedIn's use and possession of LinkedIn's servers and infrastructure." However, LinkedIn does not allege that hiQ's access to servers and infrastructure caused any "physical damage" or "deprived [LinkedIn] of the use" of any of that property. *See* ACC at 49, ¶¶ 135-39. Instead, LinkedIn merely alleges that "hiQ's conduct, *if expanded and/or replicated unchecked by others*, will cause harm to LinkedIn in the form of impaired condition, quality and value of its servers, infrastructure and services." ACC at 49, ¶ 139 (emphasis added).

LinkedIn's failure to allege that hiQ's conduct has or will itself impair the condition, quality, or value of LinkedIn's product requires dismissal of LinkedIn's claim. As the California Supreme Court has recognized, the tort of trespass to chattels "does not encompass . . . an electronic communication that neither damages the recipient computer system nor impairs its functioning." *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003); *see also Brodsky*, 445 F. Supp. 3d at 124-25 (dismissing claim of trespass to chattel where electronic access did not damage or impair property or deprive plaintiff of its use), *Engle v. Unified Life Ins. Co., Inc.*, 2014 WL 12508347, at *7 (S.D. Cal. Oct. 27, 2014) (same). As such, LinkedIn has not alleged that it has yet suffered any cognizable trespass. And LinkedIn cannot plead damages against hiQ based upon hypothetical future conduct by unnamed and unrelated third parties; to permit that would vitiate the requirement that plaintiffs plead damages at all. LinkedIn's claim of trespass to chattel therefore should be dismissed for failure to plead the required element of damage.

## CONCLUSION

For the foregoing reasons, hiQ respectfully requests that this Court dismiss LinkedIn's counterclaims with prejudice for failure to state a claim upon which relief can be granted and strike in part LinkedIn's request for remedies for its claim of breach of contract.

Dated: January 18, 2021

QUINN EMANUEL URQUHART & SULLIVAN LLP

By: */s/ Corey Worcester*
Corey Worcester

*Attorneys for Plaintiff hiQ Labs*