UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

HIQ LABS, INC., Plaintiff, v. LINKEDIN CORPORATION, Defendant.	Case No. 17-cv-03301-EMC **ORDER DEFERRING IN PART AND DENYING IN PART PLAINTIFF'S MOTION TO DISMISS AND STRIKE COUNTERCLAIMS** Docket No. 182

This case arises out of Plaintiff hiQ Labs, Inc.'s access to and use of public profiles of Defendant LinkedIn Corp.'s users. hiQ initiated this lawsuit against LinkedIn, bringing claims for, *inter alia*, declaratory relief, tortious interference, and unfair competition. In response, LinkedIn has asserted counterclaims, including violation of the federal Computer Fraud and Abuse Act, breach of contract, and misappropriation. Currently pending before the Court is hiQ's motion to dismiss the counterclaims. Having considered the parties' briefs and accompanying submissions, the Court hereby **DEFERS** in part and **DENIES** in part hiQ's motion.

I. FACTUAL & PROCEDURAL BACKGROUND

LinkedIn is a company that provides a social network for professionals. *See* Countercl. ¶ 20. Members of LinkedIn "create individual profiles that serve as their professional profiles online." Countercl. ¶ 21. Today, the company has more than 700 million members worldwide. *See* Countercl. ¶ 21.

LinkedIn gives its members numerous privacy protections and privacy choices. For example:

- "[I]f a member decides that he or she wants to delete his or her profile, LinkedIn will permanently delete the account and all of the data that the member posted to LinkedIn within 30 days." Countercl. ¶ 56 (alleging that this "helps ensure that members are the ones who have ultimate control over [their information]").

- Members can choose to have all or part of their profiles exempt from indexing by well-known search engines such as Google, Bing, and Duck Duck Go. *See* Countercl. ¶ 55.
- When members update information in their profiles, they can choose whether to broadcast that change on LinkedIn. *See* Countercl. ¶ 57 (alleging that, if a member chooses the "Do Not Broadcast" setting, the "changes that the member makes to his or her profile will be visible, but the fact that the member made a change will not be broadcast to his or her LinkedIn connections or to anyone else"); *see also* Countercl. ¶ 58 (alleging that this feature was put in place "in response to feedback from LinkedIn members who were hesitant to update their profiles for fear that their co-workers or employers would suspect they were searching for a new job or otherwise thinking of leaving their current jobs").

"LinkedIn's website and servers are not unconditionally open to the general public." Countercl. ¶ 25. "This is because LinkedIn's servers are protected by sophisticated defenses . . . that evaluate whether to grant each request made to LinkedIn's servers." Countercl. ¶ 25. These defenses "currently block hundreds of millions of requests to access guest profiles per day from bots and scrapers, which constitute the majority of the requests made to LinkedIn's servers for guest profiles." Countercl. ¶ 25.

Examples of LinkedIn's defenses include the following:

- The Sentinel system. "Through Sentinel, LinkedIn maintains a list of IP addresses that are not permitted to make calls on LinkedIn's servers because they either have in the past or are engaged in abuse." Countercl. ¶ 27.
- LinkedIn's "robots.txt" file. The file "provides a set of instructions to any automated technologies visiting the LinkedIn site, as well as an explicit warning . . . [,] that the use of bots to access LinkedIn without express permission is strictly

prohibited." Countercl. ¶ 33. The file "does permit some webcrawlers (e.g., search engines such as Google or Bing) to crawl and index the site." Countercl. ¶ 33; *see also* Countercl. ¶ 55 (alleging that that LinkedIn's "Privacy Policy expressly informs members that search engines may index and display information in their profiles" but "LinkedIn limits such indexing to well-known search engines, such as Google, Bing and Duck Duck Go"; furthermore, "LinkedIn permits members to choose the parties of their profiles that search engines index, or to opt out of this feature entirely").

- LinkedIn's "custom rules." LinkedIn applies "over 200 custom rules . . . to requests made to its servers to determine whether the requests is from a human or bot." Countercl. ¶ 30. Some of the rules fall under LinkedIn's Guest Request Scoring System and Member Request Scoring System. The Guest Request Scoring System "monitors and limits page requests made by users who are not logged into LinkedIn. If unusual patterns or high levels of activity are detected, the user is redirected to LinkedIn's log-in page and is prevented from viewing additional LinkedIn pages while not logged in." Countercl. ¶ 32. "The Member Request Scoring System monitors page requests made by LinkedIn members while logged into their accounts. If high levels of activity are detected for certain types of accounts, the member is logged out and may either be warned, restricted, or challenged with a CAPTCHA in order to log back into LinkedIn." Countercl. ¶ 31.
- Password barrier. "Much of the information on LinkedIn's website is behind a password barrier. Periodically, LinkedIn will prevent 'logged-out' users from viewing more than a certain number of pages before being asked to enter a user name and password to see more." Countercl. ¶ 34.
- The FUSE system. "FUSE scans and imposes a limit on the activity that an individual LinkedIn member may initiate on the site. This limit is intended to prevent would-be data scrapers utilizing automated technologies from quickly accessing a substantial volume of member profiles." Countercl. ¶ 26.

In addition to the above defenses, LinkedIn's User Agreement "prohibits accessing and scraping of LinkedIn's website through automated software and other technologies." Countercl. ¶ 36; *see also* Countercl. ¶ 49 (citing § 8.2 of the User Agreement). Members of LinkedIn are subject to the User Agreement but so too are users and visitors of the LinkedIn website. *See* Countercl. ¶ 37. For example, "[t]he relevant version of the User Agreement, effective October 23, 2014, states that 'You agree that by clicking "Join Now[,]" "Join LinkedIn" "Sign Up" or similar[] registering, accessing, or using our services . . . , you are entering into a legally binding agreement (even if you are using our Services on behalf of a company).'" Countercl. ¶ 37.

Notwithstanding these measures, hiQ accesses and aggregates publicly available profiles on LinkedIn and uses the data for the data analytic tools it sells.

A. hiQ's First Amended Complaint ("FAC")

In its FAC, hiQ asserts the following claims for relief:

(1) A declaratory judgment that hiQ has not violated and will not violate the Computer Fraud and Abuse Act of 18 U.S.C. § 1030 by accessing LinkedIn public profiles.

(2) A declaratory judgment that hiQ has not violated and will not violate the Digital Millennium Copyright Act, 17 U.S.C. § 1201, by accessing LinkedIn public profiles.

(3) A declaratory judgment that hiQ has not committed and will not commit common law trespass to chattels by accessing LinkedIn public profiles.

(4) A declaratory judgment that hiQ has not violated and will not violate California Penal Code § 502(c) by accessing LinkedIn public profiles.

(5) Intentional interference with contract.

(6) Intentional interference with prospective economic advantage.

(7) Unfair competition in violation of California Business & Professions Code § 17200.

(8) Unlawful competition in violation of § 17200.

(9) Fraudulent competition in violation of § 17200.

B. LinkedIn's Counterclaims

In its responsive counterclaims, LinkedIn pleads the following causes of action against hiQ:

(1) Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

(2) Violation of the California Comprehensive Computer Access and Fraud Act, Cal. Pen. Code § 502 *et seq.*

(3) Breach of contract.

(4) Misappropriation.

(5) Trespass to chattels.

C. Prior Court Rulings

Before LinkedIn filed its counterclaims in the instant case, this Court issued an order granting hiQ a preliminary injunction with respect to its claims for relief. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099 (N.D. Cal. 2017) (hereafter *hiQ I*). LinkedIn appealed that order; the Ninth Circuit affirmed. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019) (hereinafter *hiQ II*). LinkedIn thereafter filed a petition for a writ of certiorari with the Supreme Court. LinkedIn's petition is still pending.

II. DISCUSSION

A. Legal Standard

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). *See* Fed. R. Civ. P. 12(b)(6). To overcome a Rule 12(b)(6) motion to dismiss after the Supreme Court's decisions in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), a plaintiff's "factual allegations [in the complaint] 'must . . . suggest that the claim has at least a plausible chance of success.'" *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014). The court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). But "allegations in a complaint . . . may not simply recite the elements of a cause of action [and] must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Levitt*, 765 F.3d at 1135 (internal quotation marks omitted). "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. "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (internal quotation marks omitted).

In the instant case, hiQ has challenged under Rule 12(b)(6) each of LinkedIn's five counterclaims:

(1) Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

(2) Violation of the California Comprehensive Computer Access and Fraud Act, Cal. Pen. Code § 502 *et seq.*

(3) Breach of contract.

(4) Misappropriation.

(5) Trespass to chattels.

B. Violation of the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") provides in relevant part: "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access,[1] and thereby obtains . . . information from any protected computer . . . shall be punished" by fine or imprisonment." 18 U.S.C. § 1030(a)(2)(C).

In its decision affirming the preliminary injunction in this case, the Ninth Circuit provided guidance on its views of the CFAA. It determined, for example, that hiQ had raised a serious question as to its contention that, "where access is open to the general public, the CFAA 'without authorization' concept is inapplicable." *hiQ II*, 938 F.3d at 1000.

Primarily relying on the Ninth Circuit's decision, hiQ argues that the Court should dismiss

[1] "[E]xceeds authorized access" under the CFAA "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." 18 U.S.C. § 1030(e)(6).

United States District Court
Northern District of California

LinkedIn's CFAA counterclaim. At this juncture, however, the Court finds it prudent to defer ruling on hiQ's motion because LinkedIn has asked the Supreme Court to review the Ninth Circuit's decision. In addition, the Supreme Court currently has before it a case that will address a related issue – *i.e.*, when does a person exceed authorized access under the CFAA? – that may well have an impact on the instant case. *See United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019), *certiorari granted by* 140 S. Ct. 2667 (2020). These circumstances counsel against a ruling on the CFAA counterclaim at this point in the proceedings. The Court will be in a better position to address the counterclaim once the Supreme Court has issued its decision in *Van Buren* and/or the instant case.

C. Violation of the California Comprehensive Computer Access and Fraud Act, Cal. Pen. Code § 502 *et seq.*

LinkedIn has also asserted a counterclaim for violation of the California Comprehensive Computer Access and Fraud Act. The relevant provision in the Act can be found in California Penal Code § 502(c), which provides in relevant part as follows:

> [A]ny person who commits any of the following acts is guilty of a public offense:
>
> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> . . . .
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

Cal. Pen. Code § 502(c). Section 502(c)(7) bears similarity to the CFAA, focusing on unauthorized access. However, §§ 502(c)(1) and (2) are different from the CFAA (at least as interpreted by the Ninth Circuit), focusing instead on unauthorized use. *See also United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2016) (noting that, "[i]n contrast to the CFAA, the California statute does not require *unauthorized* access" but rather "*knowing* access[;] [w]hat makes that access unlawful is that the person 'without permission takes, copies, or makes use of' data on the computer"); *Power Ventures*, 844 F.3d at 1069 (noting that, *e.g.*, § 502(c)(2) is different from the CFAA).

Although § 502 is not on all fours with the CFAA, the Court nevertheless finds it prudent to defer ruling on the § 502 counterclaim as well. The Supreme Court's decision in *Van Buren* and/or the instant case may still affect the § 502 analysis – *e.g.*, whether, as a matter of policy, the use of public information should be deemed criminal conduct.

D. Breach of Contract

LinkedIn's breach-of-contract counterclaim is predicated on the User Agreement which "prohibits accessing LinkedIn's website through automated means" and "prohibits scraping data from LinkedIn's website using automated means." Countercl. ¶¶ 115-16. According to LinkedIn, "hiQ's conduct has damaged LinkedIn, and caused *and continues to cause* irreparable harm and injury to LinkedIn." Countercl. ¶ 125 (emphasis added).

In its motion, hiQ seeks to dismiss only part of the counterclaim. hiQ points out that, in its order granting a preliminary injunction, this Court stated: "hiQ signed up as a LinkedIn user and is thus bound by the User Agreement[,] [b]ut LinkedIn has since terminated hiQ's user status." *hiQ I*, 273 F. Supp. at 1107 n.4. Similarly, the Ninth Circuit in affirming the preliminary injunction order stated: "[h]iQ is no longer bound by the User Agreement, as LinkedIn has terminated hiQ's user status." *hiQ II*, 983 F.3d at 991 n.5. Based on these statements, hiQ argues: "LinkedIn's claim that hiQ '*continues* to' breach the User Agreement is precluded by the findings of this Court and the Ninth Circuit," and, "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." Mot. at 12 (emphasis added).

The problem with hiQ's position is that, even if LinkedIn terminated hiQ as a LinkedIn *member* subject to the User Agreement (a fact that LinkedIn disputes), that does not necessarily mean that hiQ is not subject to the User Agreement. In its counterclaim, LinkedIn alleges that "[a]ny future use of LinkedIn's website by hiQ is subject to the terms of the User Agreement," Countercl. ¶ 126, because, "[b]y its terms, the User Agreement applies not only to LinkedIn members, which hiQ was, *but to anybody who uses LinkedIn's website*." Countercl. ¶ 51 (emphasis added). According to LinkedIn, "[a]t all relevant times, LinkedIn . . . prominently displayed a link to the User Agreement on LinkedIn's homepage. Those who use LinkedIn's website with actual knowledge of the terms of the User Agreement are required to abide by those terms if they choose to access LinkedIn's website." Countercl. ¶ 109. In support, LinkedIn cites *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171 (9th Cir. 2014).

Nguyen is an arbitration-related case; nevertheless, it contains principles relevant to the instant case because the defendant there argued, *inter alia*, that the plaintiff was subject to an arbitration provision based on Terms of Use posted as a hyperlink on the defendant's website. The Ninth Circuit noted that

> [c]ontracts formed on the Internet come primarily in two flavors: "clickwrap" (or "click-through") agreements, in which website users are required to click on an "I agree" box after being presented with a list of terms and conditions of use; and "browsewrap" agreements, where a website's terms and conditions of use are generally posted on the website via a hyperlink at the bottom of the screen. . . .
>
> "Unlike a clickwrap agreement, a browsewrap agreement does not require the user to manifest assent to the terms and conditions expressly . . . [a] party instead gives his assent simply by using the website." Indeed, "in a pure-form browsewrap agreement, 'the website will contain a notice that – by merely using the services of, obtaining information from, or initiating applications within the website – the user is agreeing to and is bound by the site's terms of service.'" Thus, "by visiting the website – something that the user has already done – the user agrees to the Terms of Use not listed on the site itself but available only by clicking a hyperlink." "The defining feature of browsewrap agreements is that the user can continue to use the website or its services without visiting the page hosting the browsewrap agreement or even knowing that such a webpage exists." "Because no affirmative action is required by the website user to agree to the terms of a contract other than his or her use of the website, the determination of the validity of the browsewrap contract depends on whether the user has actual or constructive knowledge of a website's terms and conditions."

Id. at 1175-76.

The Ninth Circuit continued by noting that "courts have consistently enforced browsewrap agreements where the user had actual notice of the agreement"; in contrast, "where . . . there is no evidence that the website user had actual knowledge of the agreement, the validity of the browsewrap agreement turns on whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract." *Id.* at 1176-77.

Thus, under *Nguyen*, LinkedIn has a basis for arguing that, if hiQ has actual notice of the terms of the User Agreement (which contains, *e.g.*, a prohibition against scraping), it can be subject to those terms. Although currently hiQ is allowed access to the LinkedIn website and to copy or use public profiles posted thereon under the preliminary injunction, this does not mean that hiQ is entitled to a permanent injunction. Based on the counterclaim as pled, LinkedIn has a basis for asserting that *it* is entitled to a permanent injunction – or at least a declaration – that hiQ is subject to the User Agreement in the future. Because whether hiQ can be bound to the User Agreement raises a factual question, the counterclaim cannot be dismissed at this juncture.

E. Misappropriation

The California Court of Appeal has explained that

> [c]ommon law misappropriation is one of a number of doctrines subsumed under the umbrella of unfair competition. It is normally invoked in an effort to protect something of value not otherwise covered by patent or copyright law, trade secret law, breach of confidential relationship, or some other form of unfair competition. 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 the plaintiff's property at little or no cost to the 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 Ass'n v. Arroyo Software Corp., 69 Cal. App. 4th 607, 618 (1999) [hereinafter *USGA*].

In its counterclaim, LinkedIn alleges that hiQ engaged in misappropriation because, "without authorization, [it] wrongfully accessed LinkedIn's website, computer systems and servers, and obtained data from the LinkedIn site. The data that hiQ took included time-sensitive updates to member profiles." Countercl. ¶ 130. In response, hiQ makes two arguments: (1) LinkedIn has no ownership interest in the data allegedly misappropriated (rather, that data belongs to LinkedIn members) and (2) any misappropriation counterclaim here would be preempted by the California Uniform Trade Secret Act ("CUTSA").

1. <u>Property Rights</u>

hiQ's first argument is, in essence, that LinkedIn has no property rights at issue in the instant case. hiQ is corrected that LinkedIn's members, and not LinkedIn itself, owns the information in their public profiles. However, that does not mean that LinkedIn has no property rights. As LinkedIn points out, there may be "quasi-property" rights that are protected. For example, one company can misappropriate "another's commercial advantage" by misappropriating the "'expenditure of labor, skill, and money' of another." *Am. Cyanamid Co. v. Am. Home Assurance Co.*, 30 Cal. App. 4th 969, 976-77 (1994) (quoting *International News Service v. Associated Press*, 248 U.S. 215, 239 (1918) [hereinafter *INS*]).

As indicated above, California's recognition of this kind of misappropriation is based on *INS* which recognized a property interest in "hot news." *See id.*; *see* also *Sammons & Sons v. Ladd-Fab, Inc.*, 138 Cal. App. 3d 306, 311 (1982) (noting that "*INS* expanded existing concepts of unfair competition to include protection against appropriation of competitive advantage 'acquired by complainant as the result of organization and the expenditure of labor, skill, and money' by a defendant who thereby 'is endeavoring to reap where it has not sown'"). In *INS*, the plaintiff and the defendant were competitors in the gathering and distribution of news and its publication for profit in newspapers throughout the United States." *INS*, 248 U.S. at 229. The plaintiff filed suit to stop the defendant from, *inter alia*, copying news from bulletin boards and early editions of the plaintiff's newspapers and selling it, "either bodily or after rewriting it, to defendant's customers." *Id.* at 231.

The Supreme Court noted that, while "the news of current events may be regarded as common property[,] [w]hat we are concerned with is the business of making it known to the world." *Id.* at 235. "The peculiar value of news is in the spreading of it while it is fresh." *Id.* In other words,

> although we may and do assume that neither party has any remaining property interest as against the public in uncopyrighted news matter after the moment of its first publication, it by no means

> follows that there is no remaining property interest in it as between themselves. For, to both of them alike, news matter, however little susceptible of ownership or dominion in the absolute sense, is stock in trade, *to be gathered at the cost of enterprise, organization, skill, labor, and money*, and to be distributed and sold to those who will pay money for it, as for any other merchandise. Regarding the news, therefore, as but the material out of which both parties are seeking to make profits at the same time and in the same field, we hardly can fail to recognize that for this purpose, and as between them, it must be regarded as quasi property, irrespective of the rights of either as against the public.

Id. at 236 (emphasis added). California courts have cited *INS* approvingly. *See, e.g.*, *Balboa Ins. Co. v. Trans Glob. Equities*, 218 Cal. App. 3d 1327, 1342 (1990) ("Common law misappropriation presents a final legal theory under the broad unfair competition umbrella. The doctrine originated in the United States Supreme Court's decision of [*INS*].").

hiQ suggests that, to the extent *INS* is recognized under California law, *INS* should be narrowly construed and

> limited to cases where: (i) a plaintiff generates or gathers information at a cost; (ii) the information is time-sensitive; (iii) a defendant's use of the information constitutes free-riding on the plaintiff's efforts; (iv) the defendant is in direct competition with a product or service offered by the plaintiffs; and (v) the ability of other parties to free-ride on the efforts of the plaintiff or others would so reduce the incentive to produce the product or service that its existence or quality would be substantially threatened.

Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 845 (2d Cir. 1997) [hereinafter "*NBA*"]. But hiQ has cited no California state court opinion adopting this narrow view. Rather, the elements of a common law misappropriation claim under California law have been outlined above. *See Balboa*, 218 Cal. App. 3d at 1342 (recognizing that common law misappropriation has its roots in *INS* but not limiting the claim to the hot news context and stating that "[t]he cause of action has three elements: (1) the plaintiff has invested substantial time and money in development of its . . . property; (2) the defendant has appropriated the [property] at little or no cost; and (3) the plaintiff has been injured by the defendant's conduct") (internal quotation marks omitted). Although hiQ has cited *Pollstar v. Gigmania, Ltd.*, 170 F. Supp. 2d 974, 979 (E.D. Cal. 2000), where the district court applied the Second Circuit's approach above, that case is not dispositive. hiQ has cited no California case that imposes the *NBA* restrictions, even in a case involving "hot news."

If anything, California authority rejects, at least in part, the narrow interpretation. For instance, in *USGA*, the state court expressly rejected the argument that an essential element of a misappropriation claim was direct competition between the plaintiff and the defendant. *See USGA*, 69 Cal. App. 4th at 618 ("Under the California law applicable here, . . . the essential elements of a misappropriation claim simply do not include any such requirement of proof of direct competition between the plaintiff and the defendant."). *Cf. Colo. Escrow & Title Servs., LLC v. Deinema*, No. 2012CV387, 2015 Colo. Dist. LEXIS 1802, *34-36 (Colo. Dist. Ct. Jan. 23, 2015) (noting that Colorado law recognizes a misappropriation claim "where one either wrongfully profits from another's expenditure of labor, skill or money, or capitalizes wrongfully on the commercial values of another"; rejecting the argument that such a claim requires that the plaintiff and defendant be competitors – it was enough that "ESI has profited from TCR's accumulation and organization of public records").

Finally, even if the Court were inclined to adopt a narrow view of *INS*, LinkedIn has still met that standard (at least based on the allegations made by the parties). For example, regarding direct competition, hiQ itself has charged LinkedIn with blocking hiQ's access because LinkedIn "wants to monetize [its] data itself with a competing product." *hiQ I*, 273 F. Supp. 3d at 1117. Also, to the extent information must be time sensitive, LinkedIn has alleged that "[t]he data that hiQ took included time-sensitive updates to member profiles." Countercl. ¶ 130. Finally, there are questions of fact as to whether hiQ is a free rider with respect to LinkedIn and whether hiQ's use of LinkedIn's data reduces LinkedIn's incentive to invest in its infrastructure.

2. CUTSA Preemption

hiQ argues that, even if LinkedIn has a property interest to support a misappropriation counterclaim, the counterclaim must still be dismissed based on CUTSA preemption. This contention lacks merit. As LinkedIn points out, the misappropriation counterclaim is not preempted because the whole point of such a claim is to protect a property right "*not* otherwise covered by patent or copyright law, trade secret law, breach of confidential relationship, or some other form of unfair competition." *USGA*, 69 Cal. App. 4th at 618 (emphasis added).

hiQ points out that, under certain circumstances, there can be CUTSA preemption even where the property right at issue does not constitute a trade secret per se. For instance, in *Lifeline Food Co. v. Gilman Cheese Corp.*, No. 5:15-cv-00034-PSG, 2015 U.S. Dist. LEXIS 64155 (N.D. Cal. May 15, 2015), the district court noted that the "CUTSA may supersede 'claims based on the misappropriation of information that does not satisfy the definition of trade secret under CUTSA' when '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.'" *Id.* at *3. However, in the instant case, LinkedIn is not making any claim that the public profiles are confidential or not generally known to the public. Rather, the property right it is claiming is based on the labor, skill, money, etc. that it put into developing the professional networking system. There is thus no basis for CUTSA preemption.

F. <u>Trespass to Chattels</u>

"Under California law, trespass to chattels 'lies where an intentional interference with the possession of personal property has proximately caused injury.'" *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1350-51 (2003). The owner of the property may recover actual damages suffered by reason of the impairment of the property or the loss of its use.[2] *See id.* at 1351. Injunctive relief is also possible where there is threatened injury. *See id.* at 1352 (asking whether the defendant's actions "cause or threatened to cause damage to Intel's computer system, or injury to it rights in that personal property").

In its motion, hiQ argues that the trespass claim should be dismissed because LinkedIn has failed to adequately allege injury. In response, LinkedIn contends that it has adequately alleged existing injury as well as threatened future injury.

Regarding existing injury, LinkedIn contends that a small amount of harm can support trespass to chattels. *See* Opp'n at 24. In support, it cites *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App.

[2] In *Intel*, the California Supreme Court rejected the plaintiff's argument that its damages included the time its staff spent time attempting to block the defendant's email messages. "'[I]t is circular to premise the damage element of a tort solely upon the steps taken to prevent the damage. Injury can only be established by the completed tort's consequences, not by the cost of the steps taken to avoid the injury and prevent the tort; otherwise, we can create injury for every supposed tort.'" *Intel*, 30 Cal. 4th at 1359.

4th 1559 (1996). In *Thrifty-Tel*, the plaintiff was a company that provided long-distance telephone services. "Subscribers' telephones are programmed with a confidential access code and a six-digit authorization code that directs calls into Thrifty-Tel's computerized switching network. An unauthorized user who knows both an access and an authorization code can make long-distance calls without being charged for them." *Id.* at 1563. During a three-day period, the defendants' children "gained entry into Thrifty-Tel's system with [a confidential] code [that a friend knew] and conducted manual random searches for a six-digit authorization code. They made approximately 90 calls, consuming roughly 24 minutes of telephone time during the first 2 days." *Id.* at 1564. The following day, they made "72 manual attempts to identify an authorization code over an almost 16-minute period." *Id.* The state appellate court found that the plaintiff had a valid trespass claim and remanded to the trial court to determine damages. *See id.* at 1570, 1572 (holding that "the superior court erred in awarding contract or tort damages based on [a] tariff instead of requiring plaintiff to prove actual damages").

But *Thrifty-Tel* is distinguishable from the instant case in that, there, an actual entry into the plaintiff's system was made, thus making the case more akin to a traditional computer hacking or "breaking and entering" claim whereas, here, there has been an alleged burden on LinkedIn's servers and/or infrastructure. Thus, more on point than *Thrifty-Tel* is the California Supreme Court opinion in *Intel* which noted that, "[s]hort of dispossession, personal injury, or physical damage . . . , intermeddling is actionable only if the chattel is impaired as to its condition, quality, or value or . . . the possessor is deprived of the use of the chattel for a substantial time" – *i.e.*, "for a time so substantial that it is possible to estimate the loss caused thereby." *Intel*, 30 Cal. 4th at 1357 (internal quotation marks omitted; adding that "'[a] mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession'"). This statement from *Intel* suggests that, at least as to impaired use, the quantum of harm cannot be negligible.

That being said, LinkedIn fairly argues that there is a question of fact as to what extent hiQ's actions burdened LinkedIn's servers/infrastructure. LinkedIn has alleged:

- "[S]craping traffic has grown substantially over the past few years." Countercl. ¶ 82.

- "LinkedIn . . . receives many millions of unauthorized requests of its servers from bots every day. The volume . . . reached 95 million requests per day by the outset of the parties' dispute, and has further increased dramatically during this litigation." Countercl. ¶ 82.
- "[T]aken in the aggregate, automated scrapers place a substantial burden on LinkedIn's infrastructure – reaching at present into hundreds of millions of blocked access requests per day." Countercl. ¶ 83. "[T]he significant volume of automated scraping activity forces LinkedIn to invest more in capital and operational resources than it otherwise would if it were able to prevent these access requests from ever happening. Scraping operations force LinkedIn to alter its priorities for use of its computing resources and impair the efficiency of such resources." Countercl. ¶ 83.
- "On information and belief, hiQ's bots made millions of calls to LinkedIn's servers prior to May 23, 2017 [the date of the cease-and-desist letter]." Countercl. ¶ 68.
- "The full extent of hiQ's illicit scraping is not currently known to LinkedIn, as hiQ has gone to substantial lengths to hide its methods from public view." Countercl. ¶ 64.

In short, the requests generated by hiQ's bots burden LinkedIn's servers.

As to future injury, LinkedIn has also alleged enough to support a request for injunctive relief. Regarding injunctive relief, the California Supreme Court took note in *Intel* of two district court decisions finding that unauthorized robotic data collection from a company's publicly accessible website was a trespass on the company's computer system in part because of "the deleterious impact this activity could have, especially if replicated by other searchers, on the functioning of a Web site's computer equipment." *Intel*, 30 Cal. 4th at 1354. Tracking *Intel*, LinkedIn makes the following allegations in support of its counterclaim for trespass to chattels: (1) "LinkedIn owns, possesses, and/or has the right to possess the servers and infrastructure used to run its business"; (2) "hiQ intentionally interfered with LinkedIn's use and possession" of such; and (3) "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." Countercl. ¶¶ 136-37, 139; *see also* Countercl. ¶ 84 ("It is only because of LinkedIn's ongoing protection efforts as well as its willingness to spend increasing amounts to maintain a high service level that it has been able to prevent a degradation in the quality of its services."); Countercl. ¶ 85 ("LinkedIn will be forced into making the choice of investing more in its infrastructure to ensure the availability of its website, or succumbing to the burden of bot-based scraping.").

III. CONCLUSION

For the foregoing reasons, the Court denies hiQ's motion to dismiss the counterclaims for breach of contract, misappropriation, and trespass to chattels. The Court defers ruling on the motion to dismiss the counterclaims for violation of the CFAA and California Penal Code § 502.

For administrative purposes only, the Court terminates hiQ's motion to dismiss, even though the CFAA and § 502 counterclaims have not yet been addressed. To be clear, this termination does not bar hiQ from renewing its motion to dismiss the CFAA and § 502 counterclaims once the Supreme Court issues its decision in *Van Buren* and/or this case.

IT IS SO ORDERED.

Dated: April 19, 2021

EDWARD M. CHEN
United States District Judge