UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

HIQ LABS, INC.,

Plaintiff,

v.

LINKEDIN CORPORATION,

Defendant.

Case No. 17-cv-03301-EMC

ORDER GRANTING PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

Docket No. 23

I. INTRODUCTION

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

hiQ's business involves providing information to businesses about their workforces based on statistical analysis of publicly available data. Its data analytics business is wholly dependent on LinkedIn's public data. hiQ contends that LinkedIn's actions constitute unfair business practices under Cal. Bus. & Prof. Code § 17200 *et seq.* hiQ also raises a number of common law tort and contract claims, including intentional interference with contract and promissory estoppel, and further contends that LinkedIn's actions constitute a violation of free speech under the California Constitution.

Now pending before the Court is hiQ's motion for a preliminary injunction. For the reasons set forth in more detail below, the Court **GRANTS** the motion. In summary, the balance

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

II. FACTUAL AND PROCEDURAL BACKGROUND

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

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

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

On May 23, 2017, LinkedIn sent a letter demanding that hiQ "immediately cease and desist unauthorized data scraping and other violations of LinkedIn's User Agreement." Docket No. 23-1 ("Gupta Decl.") Ex. J. In the letter, LinkedIn demanded that hiQ cease using software to "scrape," or automatically collect, data from LinkedIn's public profiles. LinkedIn noted that its User Agreement prohibits various methods of data collection from its website, and stated that hiQ was in violation of those provisions. LinkedIn also stated that it had restricted hiQ's company page on LinkedIn and that "[a]ny future access of any kind" to LinkedIn by hiQ would be "without permission and without authorization from LinkedIn." LinkedIn further stated that it had "implemented technical measures to prevent hiQ from accessing, and assisting other to access, LinkedIn's site, through systems that detects, monitor, and block scraping activity." LinkedIn stated that any further access to LinkedIn's data would violate state and federal law, including California Penal Code § 502(c), the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, state common law of trespass, and the Digital Millennium Copyright Act. LinkedIn reserved the right to pursue litigation, should hiQ fail to cease and desist from accessing LinkedIn's website, computer systems, and data.

After hiQ and LinkedIn were unable to agree on an amicable resolution, and LinkedIn declined to permit hiQ's continued access in the interim, hiQ filed the complaint in this action, which asserts affirmative rights against the denial of access to publicly available LinkedIn profiles based on California common law, the UCL, and the California Constitution. hiQ also seeks a declaration that hiQ has not and will not violate the CFAA, the DMCA, California Penal Code § 502(c), and the common law of trespass to chattels, by accessing LinkedIn public profiles. Docket No. 1. At the same time, hiQ also filed a request for a temporary restraining order and an order to show cause why a preliminary injunction should not be issued against LinkedIn. Docket No. 23. After a hearing on the TRO request, the parties entered into a standstill agreement preserving hiQ's access to the data and converting hiQ's initial motion into a motion for a preliminary injunction. A hearing on the motion for preliminary injunction was held on July 27, 2017.

III. DISCUSSION

"A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). In evaluating these factors, courts in the Ninth Circuit employ a "sliding scale" approach, according to which "the elements of the preliminary injunction test are balanced, so that a stronger showing of one element may offset a weaker showing of another. For example, a stronger showing of irreparable harm to plaintiff might offset a lesser showing of likelihood of success on the merits." *All. for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011). At minimum, "[u]nder *Winter*, plaintiffs must establish that irreparable harm is *likely*, not just possible, in order to obtain a preliminary injunction." *Id.* (emphasis in original). Specifically, the Ninth Circuit "has adopted and applied a version of the sliding scale approach under which a preliminary injunction could issue where the likelihood of success is such that 'serious questions going to the merits were raised and the balance of hardships tips sharply in [plaintiff's] favor.'" *Id.* (quoting *Clear Channel Outdoor, Inc. v. City of Los Angeles*, 340 F.3d 810, 813 (9th Cir. 2003)). Thus, upon a showing that the balance of hardships tips sharply in its favor, a party seeking a preliminary injunction need only show that there are "serious questions going to the merits" in order to be entitled to relief. Because the balance of hardships, including the threat of irreparable harm faced by each party, informs the requisite showing on the merits, the Court addresses that prong first.

A. Irreparable Harm and Balance of Hardships

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

undisputed fact that hiQ's entire business depends on its access to LinkedIn's public profile data.[1] These potential consequences are sufficient to constitute irreparable harm. "The threat of being driven out of business is sufficient to establish irreparable harm." *Am. Passage Media Corp. v. Cass Commc'ns, Inc.*, 750 F.2d 1470, 1474 (9th Cir. 1985); *see also Doran v. Salem Inn, Inc.*, 422 U.S. 922, 932 (1975) (holding that "a substantial loss of business and perhaps even bankruptcy" constitutes irreparable harm sufficient to warrant interim relief). Similarly, "[e]vidence of threatened loss of prospective customers or goodwill certainly supports a finding of the possibility of irreparable harm." *Stuhlbarg Int'l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001).

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

[1] At the hearing, LinkedIn pointed to the fact that other companies operate in the data analytics field without making use of LinkedIn's member data. But as hiQ pointed out, these companies employ entirely different business models. For example, one company highlighted by LinkedIn, Glint, creates its own data by taking surveys of employees working for its clients. Requiring hiQ to rebuild its business on an entirely different business model, such as that employed by Glint, from scratch would constitute harm comparable to simply going out of business. LinkedIn also suggests that hiQ could make use of other sources of data, such as Facebook. But while Facebook may have a comparable number of professionals using its service, LinkedIn has not argued that the professional data available at Facebook is of a similar quality to that available at LinkedIn. Moreover, if LinkedIn's view of the law is correct, nothing would prevent Facebook from barring hiQ in the same way LinkedIn has.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.