Case No. 17-cv-03301-EMC
United States District Court, N.D. California.

HIQ Labs, Inc. v. Linkedin Corp.

273 F. Supp. 3d 1099 (N.D. Cal. 2017)
Decided Aug 14, 2017

Case No. 17–cv–03301–EMC

08-14-2017

HIQ LABS, INC., Plaintiff, v. LINKEDIN CORPORATION, Defendant.

Carl Brandon Wisoff, Deepak Gupta, Jeffrey G. Lau, Rebecca Hilary Stephens, Farella Braun & Martel LLP, San Francisco, CA, Laurence Tribe, Harvard Law School, Cambridge, MA, for Plaintiff. Jonathan Hugh Blavin, Laura K. Lin, Nicholas Daniel Fram, Rosemarie T. Ring, Munger, Tolles & Olson, LLP, San Francisco, Donald B. Verrilli, Jr., Munger, Tolles and Olson LLP, Washington, Tamerlin J. Godley, Munger, Tolles & Olson LLP, Los Angeles, CA, for Defendant.

EDWARD M. CHEN, United States District Judge

1103 *1103

Carl Brandon Wisoff, Deepak Gupta, Jeffrey G. Lau, Rebecca Hilary Stephens, Farella Braun & Martel LLP, San Francisco, CA, Laurence Tribe, Harvard Law School, Cambridge, MA, for Plaintiff.

Jonathan Hugh Blavin, Laura K. Lin, Nicholas Daniel Fram, Rosemarie T. Ring, Munger, Tolles & Olson, LLP, San Francisco, Donald B. Verrilli, Jr., Munger, Tolles and Olson LLP, Washington, Tamerlin J. Godley, Munger, Tolles & Olson LLP, Los Angeles, CA, for Defendant.

ORDER GRANTING PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

Docket No. 23

EDWARD M. CHEN, United States District Judge

I. INTRODUCTION

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

hiQ's business involves providing information to businesses about their workforces based on statistical analysis of publicly available data. Its data analytics business is wholly dependent on LinkedIn's public data. hiQ contends that LinkedIn's actions constitute unfair business practices under Cal. Bus. & Prof. Code §§ 17200 *et*

seq. hiQ also raises a number of common law tort and contract claims, including intentional interference with contract and promissory estoppel, and further contends that LinkedIn's actions constitute a violation of free speech under the California Constitution.

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

II. FACTUAL AND PROCEDURAL BACKGROUND

Founded in 2002, LinkedIn is a social networking site focused on business and professional networking. It
1104 currently has over 500 million users; it was acquired by Microsoft in December 2016 for $26.2 billion.*1104 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
1105 the data and converting hiQ's initial motion into a motion for a preliminary *1105 injunction. A hearing on the motion for preliminary injunction was held on July 27, 2017.

III. DISCUSSION

"A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Nat. Res. Def. Council, Inc.* , 555 U.S. 7, 20, 129 S.Ct. 365, 172 L.Ed.2d 249 (2008). In evaluating these factors, courts in the Ninth Circuit employ a "sliding scale" approach, according to which "the elements of the preliminary injunction test are balanced, so that a stronger showing of one element may offset a weaker showing of another. For example, a stronger showing of irreparable harm to plaintiff might offset a lesser showing of likelihood of success on the merits." *All. for the Wild Rockies v. Cottrell* , 632 F.3d 1127, 1131 (9th Cir. 2011). At minimum, "[u]nder *Winter* , plaintiffs must establish that irreparable harm is *likely,* not just possible, in order to obtain a preliminary injunction." *Id.* (emphasis in original). Specifically, the Ninth Circuit "has adopted and applied a version of the sliding scale approach under which a preliminary injunction could issue where the likelihood of success is such that 'serious questions going to the merits were raised and the balance of hardships tips sharply in [plaintiff's] favor.' " *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*
1106 *Commc'ns, Inc.* , 750 F.2d 1470, 1474 (9th Cir. 1985) ; *see also* *1106 *Doran v. Salem Inn, Inc.* , 422 U.S. 922, 932, 95 S.Ct. 2561, 45 L.Ed.2d 648 (1975) (holding that "a substantial loss of business and perhaps even bankruptcy" constitutes irreparable harm sufficient to warrant interim relief). Similarly, "[e]vidence of threatened loss of prospective customers or goodwill certainly supports a finding of the possibility of irreparable harm." *Stuhlbarg Int'l Sales Co. v. John D. Brush & Co.* , 240 F.3d 832, 841 (9th Cir. 2001).

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.

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

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

These considerations are not without merit, but there are a number of reasons to discount to some extent the harm claimed by LinkedIn. First, LinkedIn emphasizes that the fact that 50 million users have opted into the "Do Not Broadcast" feature indicates that a vast number of its users are fearful that their employer may monitor their accounts for possible changes. But there are other potential reasons why a user may opt for that setting. For instance, users may be cognizant that their profile changes are generating a large volume of unwanted notifications broadcasted to their connections on the site. They may wish to limit annoying intrusions into their contacts.[3] Second, LinkedIn has presented little evidence of users' actual privacy expectation; out of its hundreds of millions of users, including 50 million using Do Not Broadcast, LinkedIn has only identified *three* individual complaints specifically raising concerns about data privacy related to third-party data collection. 1107 Docket No. 49–1 Exs. A–C. *1107 None actually discuss hiQ or the "Do Not Broadcast" setting. Third, LinkedIn's professed privacy concerns are somewhat undermined by the fact that LinkedIn allows other third-parties to access user data without its members' knowledge or consent. LinkedIn offers a product called "Recruiter" that allows professional recruiters to identify possible candidates for other job opportunities. LinkedIn avers that when users have selected the Do Not Broadcast option, the Recruiter product respects this choice and does not update recruiters of profile changes. However, hiQ presented marketing materials at the hearing which indicate that regardless of other privacy settings, information including profile changes are

conveyed to third parties who subscribe to Recruiter. Indeed, these materials inform potential customers that when they "follow" another user, "[f]rom now on, when they update their profile or celebrate a work anniversary, you'll receive an update on your homepage. And don't worry—they don't know you're following them." LinkedIn thus trumpets its own product in a way that seems to afford little deference to the very privacy concerns it professes to be protecting in this case.

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

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

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

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

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

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

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

B. Serious Questions Going to the Merits

hiQ argues that it is likely to prevail on the merits—or at least raises serious questions going to the merits—on each of its *1108 claims. For its part, LinkedIn argues that all of hiQ's claims necessarily fail because hiQ's unauthorized access to LinkedIn's computers violates the CFAA. Thus, not only is LinkedIn's cease and desist letter backed by the CFAA, to the extent that any of hiQ's state claims have merit, they would be preempted by the CFAA. The Court thus first addresses the likelihood that the CFAA applies.

1108

1. CFAA

Whether hiQ's continued access to the LinkedIn public profiles violates the CFAA constitutes a key threshold question in this case. The CFAA creates civil and criminal liability for any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer."[6] 18 U.S.C. § 1030(a)(2)(C). As the Supreme Court has explained, the statute "provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Musacchio v. United States* , ––– U.S. ––––, 136 S.Ct. 709, 713, 193 L.Ed.2d 639 (2016).

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

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

First, in *Facebook, Inc. v. Power Ventures, Inc.* , the Ninth Circuit held that "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or *when such permission has been revoked explicitly* ." 844 F.3d 1058, 1067 (9th Cir. 2016) (emphasis added). In *Power Ventures* , the defendant operated a site that extracted and aggregated users' social networking information from Facebook and other sites on a single page. The defendant gained access to password-protected Facebook member profiles when its users supplied their Facebook login credentials. When users selected certain options on the defendant's site, the defendant, in many instances, "caused a message to be transmitted to the user's friends within the Facebook system." *Id.* at 1063. Facebook had sent a cease and desist letter demanding that Power Ventures cease accessing information on users' pages. The Ninth Circuit found a CFAA violation where "after receiving written notification from Facebook" Power Ventures "circumvented IP barriers" and continued to access Facebook servers. *Id.* at 1068. In short, Power Ventures accessed Facebook computers "without authorization."

LinkedIn also relies on *United States v. Nosal* (*Nosal II*), 844 F.3d 1024 (9th Cir. 2016). There, the Ninth Circuit held that an employee "whose computer access credentials were affirmatively revoked by [his employer] acted 'without authorization' in violation of the CFAA when he or his former employee coconspirators used the login credentials of a current employee" to gain access to the employer's computer systems. *Id.* at 1038. Specifically, the defendant persuaded current employees of the company to use their login credentials to access and collect confidential information, including trade secrets that Nosal and the employees planned to use to start *1109 a competing business. *Id.* at 1028–29. The court held "that 'without authorization" is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission." *Id.* at 1028. Defendant's authorization had been revoked when he left the company.

1109

Each of these cases is distinguishable in an important respect: none of the data in *Facebook* or *Nosal II* was *public* data. Rather, the defendants in those cases gained access to a computer network (in *Nosal II*) and a portion of a website (in *Power Ventures*) that were protected by a password authentication system. In short, the unauthorized intruders reached into what would fairly be characterized as the private interior of a computer system not visible to the public. Neither of those cases confronted the precise issue presented here: whether

visiting and collecting information from a publicly available website may be deemed "access" to a computer "without authorization" within the meaning of the CFAA where the owner of the web site has selectively revoked permission.

To be sure, LinkedIn's construction of the CFAA is not without basis. Visiting a website accesses the host computer in one literal sense, and where authorization has been revoked by the website host, that "access" can be said to be "without authorization." *See Craigslist Inc. v. 3Taps Inc.* , 942 F.Supp.2d 962 (N.D. Cal. 2013). However, whether "access" to a publicly viewable site may be deemed "without authorization" under the CFAA where the website host purports to revoke permission is not free from ambiguity. The Supreme Court has cautioned that "[w]hether a statutory term is unambiguous ... does not turn solely on dictionary definitions of its component words. Rather, 'the plainness or ambiguity of statutory language is determined [not only] by reference to the language itself, [but as well by] the specific context in which that language is used, and the broader context of the statute as a whole.' " *Yates v. United States* , —— U.S. ——, 135 S.Ct. 1074, 1082, 191 L.Ed.2d 64 (2015) (quoting *Robinson v. Shell Oil Co.* , 519 U.S. 337, 341, 117 S.Ct. 843, 136 L.Ed.2d 808 (1997)) (holding that a fish is not a "tangible object" within the meaning of the Sarbanes–Oxley Act). *See also Bond v. U.S.* , —— U.S. ——, 134 S.Ct. 2077, 2090, 189 L.Ed.2d 1 (2014) (rejecting literal reading of Chemical Weapons Convention Implementation Act that would have permitted prosecution of woman who caused minor chemical burns to spouse's lover's thumb because "[p]art of a fair reading of statutory text is recognizing that 'Congress legislates against the backdrop' of certain unexpressed presumptions") (quoting *EEOC v. Arabian American Oil Co.* , 499 U.S. 244, 248, 111 S.Ct. 1227, 113 L.Ed.2d 274 (1991)).

The CFAA must be interpreted in its historical context, mindful of Congress' purpose. The CFAA was not intended to police traffic to publicly available websites on the Internet—the Internet did not exist in 1984. The CFAA was intended instead to deal with "hacking" or "trespass" onto private, often password-protected mainframe computers. *See* H.R. Rep. No. 98–894, 1984 U.S.C.C.A.N. 3689, 3691–92, 3695–97 (1984); S. Rep. No. 99–432, 1986 U.S.C.C.A.N. 2479, 2480 (1986). The Ninth Circuit has recognized this statutory purpose, explaining that "Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking, recognizing that, '[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system.' " *United States v. Nosal* (*Nosal I*), 676 F.3d 854, 858 (9th Cir. 2012) (quoting S.Rep. No. 99–432, a 9 (1986), 1986 U.S.C.C.A.N. 2479, 2487 (Conf. Rep.)). It was originally enacted to protect *1110 government computers from hacking; it was expanded in 1986 to protect commercial computer systems. *See* S.Rep. No. 99–432, at 2 (1986), 1986 U.S.C.C.A.N. 2479, 2480 (Conf. Rep.)). The Ninth Circuit, in considering a related provision of the statute, cautioned against an overbroad interpretation that would "expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer," thereby "mak[ing] criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *Nosal I* , 676 F.3d at 859.

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

digital equivalence of Medusa. The potential for such exercise of power over access to publicly viewable information by a private entity weaponized by the potential of criminal sanctions is deeply concerning.[7] This effect would be particularly pernicious because once it is found to apply, the CFAA as interpreted by LinkedIn would not leave any room for the consideration of either a website owner's reasons for denying authorization or an individual's possible justification for ignoring such a denial. Website owners could, for example, block access by individuals or groups on the basis of race or gender discrimination. Political campaigns could block selected news media, or supporters of rival candidates, from accessing their websites. Companies could prevent competitors or consumer groups from visiting their websites to learn about their products or analyze pricing. Further, in addition to criminalizing any attempt to obtain access to information otherwise viewable by the public at large, the CFAA would preempt all state and local laws that might otherwise afford a legal right of access (*e.g.* , state law rights asserted by hiQ herein). A broad reading of the CFAA could stifle the dynamic evolution and incremental development of state and local laws addressing the delicate balance between open
1111 access to information and privacy—all in the name of a *1111 federal statute enacted in 1984 before the advent of the World Wide Web.[8]

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

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

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

Construction of the CFAA, including the terms "access" and "without authorization," should be informed not only by Congress' intent but also by the Act's theoretical underpinning. The CFAA's origin as a statute addressing the problem of computer "trespass" suggests an interpretation of the statute informed by examining

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

Kerr argues that the process of discerning and applying similar norms should govern "trespass" in the digital realm, and that because the Web is generally perceived as "inherently open," in that it "allows anyone in the world to publish information that can be accessed by anyone else without requiring authentication," courts should incorporate this norm by "adopt[ing] presumptively open norms for the Web." *Id.* at 1162. This general understanding of the open nature of the Web squares with language used in a recent Supreme Court decision relied on by hiQ. In *Packingham v. North Carolina* , ––– U.S. ––––, 137 S.Ct. 1730, 198 L.Ed.2d 273 (2017), the Court struck down a North Carolina law making it a felony for a registered sex offender to access social
1112 media *1112 websites like Facebook and Twitter. The Court explained that at present, social media sites are for many people "the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge." *Id.* at 1737. The Court's analogy of the Internet in general, and social networking sites in particular, to the "modern public square," *id.* , embraces the social norm that assumes the openness and accessibility of that forum to all comers. *Cf. Ampex Corp. v. Cargle* , 128 Cal.App.4th 1569, 1576, 27 Cal.Rptr.3d 863 (2005) ("Web sites that are accessible free of charge to any member of the public where members of the public may read the views and information posted, and post their own opinions, meet the definition of a public forum for purposes of section 425.16 [the California anti–SLAPP statute].").

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

> The authorization line should be deemed crossed only when access is gained by bypassing an authentication requirement. An authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web. This line achieves an appropriate balance for computer trespass law. It protects privacy when meaningful steps are taken to seal off access from the public while also creating public rights to use the Internet free from fear of prosecution.

Id. at 1161. This approach would square with the results in both *Nosal II* and *Power Ventures* while avoiding the negative consequences of an overly broad reading of "authorization." In both *Nosal II* and *Power Ventures* , the defendants had bypassed a password authentication system. In that sense, their "access" was, as *Nosal II* explained, clearly "without authorization" within the meaning of the CFAA. And while *Nosal II* stated that the term "authorization" has a plain and ordinary meaning, that meaning was in the context of determining whether

a former employer could control "access" to its *private* data protected by an authentication process. The plain meaning of "authorization" of "access" as analyzed in *Nosal II* is not so plain when viewed in the context of presumptively open public page on the Internet.

Where a website or computer owner has imposed a password authentication system to regulate access, it makes sense to apply a plain meaning reading of "access" "without authorization" such that "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly." *Power Ventures* , 844 F.3d at 1067. But, as noted above, in the context of a publicly viewable web page open to all on the Internet, the "plainness" of the meaning of "access" "without authorization" is less obvious. Context matters.

An analogy to physical space, while inevitably imperfect when analyzing the digital world, may be helpful. With respect to a closed space (*e.g.* , behind a locked door which requires a key to pass), the Court intuitively understands that where an individual does not have permission to enter, he would be trespassing if he did so. Even if the door is open to the public for business, the shop owner may impose limits to the manner and scope of access (*e.g.* , by restricting access to a storage or employees-only area). But if a business displayed a sign in its storefront window visible to all on a public street and sidewalk, it could *1113 not ban an individual from looking at the sign and subject such person to trespass for violating such a ban. LinkedIn, here, essentially seeks to prohibit hiQ from viewing a sign publicly visible to all.

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

Lastly, with respect to the CFAA, LinkedIn argues in part that what it objects to is not merely hiQ's access to the site, but hiQ's automated scraping of user data. But "authorization," as used in CFAA § 1030(a)(2), is most naturally read in reference to the *identity* of the person accessing the computer or website, not *how* access occurs. *Cf. Nosal I* , 676 F.3d at 857–59 (distinguishing between unauthorized access to versus use of data). Thus, Professor Kerr persuasively argues that where an individual employs an automated program that bypasses a CAPTCHA—a program designed to allow humans but to block "bots" from accessing a site—he has still not entered the website "without authorization." Unlike a password gate, a CAPTCHA does not limit access to certain individuals; it is instead intended "as a way to slow[ ] a user's access rather than as a way to deny authorization to access." Kerr, *supra* , at 1170. Other measures taken by website owners to block or limit access to bots may be thought of in the same way. A user does not "access" a computer "without authorization" by using bots, even in the face of technical countermeasures, when the data it accesses is otherwise open to the public.[9] Thus, under Professor Kerr's analysis, hiQ's circumvention of LinkedIn's measures to prevent use of bots and implementation of IP address blocks does not violate the CFAA because hiQ accessed only publicly viewable data not protected by an authentication gateway.[10]

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

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

This is not to say that a website like LinkedIn cannot employ, *e.g.* , anti-bot measures to prevent, *e.g.* , harmful intrusions or attacks on its server. Finding the CFAA inapplicable to hiQ's actions does not remove all arrows from LinkedIn's legal quiver against malicious attacks.[11] *1114 The Court therefore concludes that hiQ has, at the very least, raised serious questions as to applicability of the CFAA to its conduct.[12] Accordingly, the Court cannot *1115 conclude, at this stage, that the CFAA preempts hiQ's affirmative claims under state law. The question then is whether hiQ is entitled to preliminary injunctive relief not only against enforcement of the CFAA but also against the use of technological barriers. To obtain such relief, hiQ would have to raise at least serious questions as to whether it has rights under state laws which are violated by LinkedIn's conduct. The Court thus turns to those state claims.[13]

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

12 hiQ also argues that the interpretation of the CFAA that LinkedIn urges should be rejected under the canon of constitutional avoidance, because it raises potentially serious problems under the First Amendment. *See Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council* , 485 U.S. 568, 575, 108 S.Ct. 1392, 99 L.Ed.2d 645 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress."). Because the Court rejects LinkedIn's interpretation on the grounds discussed above, it need not reach hiQ's First Amendment arguments. The Court observes, however, that the threshold issue of state action presents a serious hurdle to any direct First Amendment claim against LinkedIn in this case. *See, e.g., Brunette v. Humane Society of Ventura County* , 294 F.3d 1205, 1210 (9th Cir. 2002) (private party may be deemed to have engaged in state action if it is a willful participant in joint action with the government; if the government has insinuated itself into a position of interdependence with it; and if it performs functions traditionally and exclusively reserved to the states); *Brentwood Academy v. Tennessee Secondary School Athletic Ass'n* , 531 U.S. 288, 300–301, 121 S.Ct. 924, 148 L.Ed.2d 807 (2001) (state action may be found where private entity is controlled by an agency of the state, when its activity results from the state's exercise of coercive power, when the state provides encouragement, or when government is "entwined" in the entity's policies, management, or control). LinkedIn is not a state official or governmental agency; it is a private party and there is no evidence that the CFAA has served to compel or encourage LinkedIn to withdraw hiQ's authorization to access its website. Compare *Brentwood Academy* , 531 U.S. at 300, 121 S.Ct. 924 (private party's actions may be characterized as state action "when the State provides significant encouragement, either overt or covert") (citation and quotation omitted) with *Blum v. Yaretsky* , 457 U.S. 991, 1005, 102 S.Ct. 2777, 73 L.Ed.2d 534 (1982) (nursing homes' decisions to discharge patients were not state action because they were made by private parties according to professional standards not established by the state, and the simple fact "[t]hat the State responds to such actions by adjusting benefits does not render it *responsible* for those actions"). However, the same interpretation of the statute would apply uniformly to both civil and criminal actions, *see supra* n.7, and a criminal prosecution under the CFAA would undoubtedly constitute state action. Thus, because the act of viewing a publicly accessible website is likely protected by the First Amendment (*see, e.g., Packingham* , 137 S.Ct. at 1737 (statute's prohibition on sex

offender access to social media websites raised serious First Amendment concerns because, *inter alia* , "[s]ocial media allows users to gain access to information ...."); *Kleindienst v. Mandel* , 408 U.S. 753, 762–63, 92 S.Ct. 2576, 33 L.Ed.2d 683 (1972) (noting the "variety of contexts [in which] this Court has referred to a First Amendment right to receive information and ideas") (quotation omitted); *First Nat'l Bank of Boston v. Bellotti* , 435 U.S. 765, 782, 98 S.Ct. 1407, 55 L.Ed.2d 707 (1978) (the First Amendment plays a role to protect "not only" "individual self-expression but also ... affording public access to discussion, debate, and the dissemination of information and ideas"); *Board of Edu., Island Trees Union Free School Dist. No. 26 v. Pico* , 457 U.S. 853, 867, 102 S.Ct. 2799, 73 L.Ed.2d 435 (1982) (noting that the right to receive information "is an inherent corollary of the rights of free speech and press that are explicitly guaranteed by the Constitution"); *cf. Branzburg v. Hayes* , 408 U.S. 665, 684–85, 92 S.Ct. 2646, 33 L.Ed.2d 626 (1972) (explaining that "[n]ewsmen have no constitutional right of access to the scenes of crime or disaster when the general public is excluded," perhaps suggesting that the right extends at least to information to which the general public has access), the doctrine of constitutional avoidance might well be properly considered in interpreting the CFAA, even if the First Amendment were not directly implicated in this particular case. *See Sosa v. DIRECTV, Inc.* , 437 F.3d 923, 932, 942 (9th Cir. 2006) (statute should be construed to avoid burdening First Amendment interests where possible). The doctrine of constitutional avoidance, if applicable, would substantiate the Court's doubt about the applicability of the CFAA to hiQ's conduct.

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

2. California Constitutional Claim

hiQ argues that LinkedIn's actions violate California's constitutional free speech protections. Article I, Section 2 of the California Constitution provides that "[e]very person may freely speak, write, and publish his or her sentiments on all subjects." The California Supreme Court has long recognized that this provision confers broader free speech rights than those provided by the First Amendment. *See Dailey v. Superior Court of City & Cty. of San Francisco* , 112 Cal. 94, 97–98, 44 P. 458 (1896). In particular, unlike the First Amendment, California's provision is not limited to restraining state entities. The California Supreme Court, in its landmark decision in *Robins v. Pruneyard Shopping Ctr.* , 23 Cal.3d 899, 905, 153 Cal.Rptr. 854, 592 P.2d 341 (1979), held that the state's guarantee of free expression may take precedence over the rights of private property owners to exclude people from their property. *Robins* concerned attempts by a large shopping mall to exclude individuals engaging in political speech. In holding that this speech was protected by the state constitution, the court emphasized the importance of the shopping mall as a public forum and center of community life, a place where "25,000 persons are induced to congregate daily to take advantage of the numerous amenities offered." *Id.* at 910, 153 Cal.Rptr. 854, 592 P.2d 341.

hiQ argues that LinkedIn is an internet-age equivalent to the Pruneyard Shopping Center. hiQ notes that like the shopping center, "LinkedIn opens the public profile section of its website to the public. LinkedIn promises its members that the public profiles on its site can be viewed by everyone." Motion at 17. Moreover, LinkedIn "expressly holds itself out as a place 'to meet, exchange ideas, [and] learn,' ... making it a modern-day equivalent of the shopping mall or town square, a marketplace of ideas on a previously unimaginable scale." *Id.* For that reason, hiQ argues, it has a right under the California Constitution to access that marketplace on equal terms with all other people and that LinkedIn's private property rights in controlling access to its computers

cannot take precedence. *Cf. Nicholson v. McClatchy Newspapers* , 177 Cal.App.3d 509, 223 Cal.Rptr. 58 (1986) (concluding that under federal case-law, "[w]hile reporters are not privileged to commit crimes and independent torts in gathering the news, and the press has no special constitutional right of access to
1116 information, 'news gathering is not without its First Amendment protections' ") *1116 (quoting *Branzburg* , 408 U.S. at 707, 92 S.Ct. 2646). *See generally Beeman v. Anthem Prescription Management, LLC* , 58 Cal.4th 329, 341, 165 Cal.Rptr.3d 800, 315 P.3d 71 (2013) ("The state Constitution's free speech provision is at least as broad as and in some ways is broader than the comparable provision of the federal Constitution's First Amendment.") (citations and quotations omitted); *Dailey* , *supra,* 112 Cal. at 97–98, 44 P. 458.

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

It is true that a number of California state courts have determined that publicly accessible websites may constitute public fora within the meaning of the state's anti–SLAPP law. In *AmpexCorp* ., the California Court of Appeal held that postings made on an internet message board constituted speech in a public forum for the purposes of the statute. The court explained that "[t]he term 'public forum' includes forms of public communication other than those occurring in a physical setting. Thus the electronic communication media may constitute public forums. Web sites that are accessible free of charge to any member of the public where members of the public may read the views and information posted, and post their own opinions, meet the definition of a public forum *for purposes of section 425.16* ." *Ampex Corp.* , 128 Cal.App.4th at 1576, 27 Cal.Rptr.3d 863 (emphasis added). The reach of the anti–SLAPP statute is broader than the scope of constitutionally protected speech; it applies to a cause of action arising from an act "in furtherance of" the person's right of free speech under the constitution. Cal. Civ. Proc. Code § 425.16(b) ; *Ampex Corp.* , 128 Cal.App.4th at 1575, 27 Cal.Rptr.3d 863 ; *cf. Lieberman v. KCOP Television, Inc.* , 110 Cal.App.4th 156, 166, 1 Cal.Rptr.3d 536, 542 (2003) (explaining that the anti–SLAPP law's protections are "not limited to the exercise of [the] right of free speech, but to all conduct *in furtherance* of the exercise of the right to free speech in
1117 connection with a public issue" (emphasis in original)).*1117 Similarly, in *Barrett v. Rosenthal* , 40 Cal.4th 33, 51 Cal.Rptr.3d 55, 146 P.3d 510 (2006), two physicians brought an action for libel and libel per se against a health activist who had posted messages attacking the physicians' character to publicly accessible Internet newsgroups. The California Supreme Court agreed with the Court of Appeals that "[w]eb sites accessible to the public ... are 'public forums' for the purposes of the anti–SLAPP statute." *Id.* at 41 n.4, 51 Cal.Rptr.3d 55, 146

P.3d 510. As in *Ampex* , however, this holding was limited to whether the defendant could invoke the anti–SLAPP statute's protections. Indeed, the Court of Appeals in that case had treated the speech in question as "act or acts ... taken '*in furtherance* of [her] right of petition or free speech' " under the anti–SLAPP law. *Barrett v. Rosenthal* , 114 Cal.App.4th 1379, 9 Cal.Rptr.3d 142, 149 (Ct. App. 2004) (emphasis added).

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

3. UCL Claim

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

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

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

1118 *1118 The Sherman Act prohibits companies from leveraging monopoly power to "foreclose competition or gain a competitive advantage, or to destroy a competitor." *Otter Tail Power Co. v. United States* , 410 U.S. 366, 377, 93 S.Ct. 1022, 35 L.Ed.2d 359 (1973). In this case, hiQ plausibly asserts that LinkedIn enjoys a position as the dominant power in the market of professional networking. Furthermore, hiQ has presented evidence that LinkedIn is seeking to compete with hiQ in the market of data analytics. In a news segment airing on national television on June 21, 2017, LinkedIn's CEO announced that "[w]hat LinkedIn would like to do is leverage all this extraordinary data we've been able to collect by virtue of having 500 million people join the site ... to make sure that each individual member has information about where those jobs are" and that "[f]or employers, [the goal is to provide] an understanding of what skills they're gonna need to be able to continue to grow, and where that talent exists." Docket No. 34 (Gupta Decl.) Ex. U. at 2. In other words, LinkedIn appears to be developing

a product that competes directly with hiQ's Skill Mapper product, which helps employers understand what skills the members of their workforces possess. There is thus a plausible inference that LinkedIn terminated hiQ's access to its public member data in large part because it wanted exclusive control over that data for its own business purposes; as noted above, hiQ faces an existential threat. That inference is supported by the timing of the commencement of its employer product which appears to coincide roughly with its terminating hiQ's access.

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

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

4. Promissory Estoppel

Lastly, hiQ argues that it is likely to prevail on claims under the common law of promissory estoppel.[14] This
1119 claim *1119 appears meritless. hiQ bases its promissory estoppel on LinkedIn's alleged promise to its users that they control the visibility of their data. By restricting hiQ's access to public member data, hiQ contends that LinkedIn has reneged on that promise with respect to members who want their data to be publicly available to all viewers. But the fact that a user has set his profile to public does not imply that he wants any third parties to collect and use that data for all purposes, and there is no indication that LinkedIn has made any promises to users that their data may be used in that way. Thus, LinkedIn's restrictions in hiQ's collection do not violate any promise made to its users. Moreover, hiQ has not cited any authority applying promissory estoppel to a promise made to someone *other* than the party asserting that claim. For instance, hiQ does not claim to be a cognizable third party beneficiary of such promise or that even that a third party beneficiary doctrine applies to promissory estoppel.

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

C. Public Interest

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

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

For present purposes, the Court concludes that the public interest favors hiQ's position. As explained above, the actual privacy interests of LinkedIn users in their *public* data are at best uncertain. It is likely that those who opt for the public view setting expect their public profile will be subject to searches, date mining, aggregation, and analysis. On the other hand, conferring on private entities such as LinkedIn, the blanket authority to block viewers from accessing information publicly available on its website for any reason, backed by sanctions of the CFAA, could pose an ominous threat to public discourse and the free flow of information promised by the
1120 Internet.*1120 Finally, given the Court's holding that hiQ has raised serious questions that LinkedIn's behavior may be anticompetitive conduct in violation of California's Unfair Competition Law, a preliminary injunction leans further in favor of the public interest. *See* , *e.g.* , *American Exp. Co. v. Italian Colors Restaurant* , 133 U.S. 2304, 133 S.Ct. 2304, 2313, 186 L.Ed.2d 417 (2013) (noting "the public interest in vigilant enforcement of the antitrust laws").

IV. CONCLUSION

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

1. Defendant LinkedIn Corporation and its officers, agents, servants, employees, and attorneys are hereby enjoined from (1) preventing hiQ's access, copying, or use of public profiles on LinkedIn's website (*i.e.* , information which LinkedIn members have designated public, meaning it is visible not just to LinkedIn members but also to others, including those who may access LinkedIn's website via Google, Bing, other services, or by direct URL) and (2) blocking or putting in place any mechanism (whether legal or technical) with the effect of blocking hiQ's access to such member public profiles. To the extent LinkedIn has already put in place technology to prevent hiQ from accessing these public profiles, it is ordered to remove any such barriers within 24 hours of the issuance of this Order.

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

3. This preliminary injunction shall take effect immediately.

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

This order disposes of Docket No. 23.

IT IS SO ORDERED .