

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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

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

## 8 **II. FACTUAL AND PROCEDURAL BACKGROUND**

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

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

19 hiQ was founded in 2012 and has, to date, received \$14.5 million in funding. hiQ sells to  
20 its client businesses information about their workforces that hiQ generates through analysis of data  
21 on LinkedIn users’ publicly available profiles. It offers two products: “Keeper,” which tells  
22 employers which of their employees are at the greatest risk of being recruited away; and “Skill  
23 Mapper,” which provides a summary of the skills possessed by individual workers. Docket No.  
24 23-4 (Weidick Decl.) ¶¶ 4-6. hiQ gathers the workforce data that forms the foundation of its  
25 analytics by automatically collecting it, or harvesting or “scraping” it, from publicly available  
26 LinkedIn profiles. hiQ’s model is predicated entirely on access to data LinkedIn users have opted  
27 to publish publicly. hiQ relies on LinkedIn data because LinkedIn is the dominant player in the  
28 field of professional networking.

1           On May 23, 2017, LinkedIn sent a letter demanding that hiQ “immediately cease and  
2 desist unauthorized data scraping and other violations of LinkedIn’s User Agreement.” Docket  
3 No. 23-1 (“Gupta Decl.”) Ex. J. In the letter, LinkedIn demanded that hiQ cease using software to  
4 “scrape,” or automatically collect, data from LinkedIn’s public profiles. LinkedIn noted that its  
5 User Agreement prohibits various methods of data collection from its website, and stated that hiQ  
6 was in violation of those provisions. LinkedIn also stated that it had restricted hiQ’s company  
7 page on LinkedIn and that “[a]ny future access of any kind” to LinkedIn by hiQ would be  
8 “without permission and without authorization from LinkedIn.” LinkedIn further stated that it had  
9 “implemented technical measures to prevent hiQ from accessing, and assisting other to access,  
10 LinkedIn’s site, through systems that detects, monitor, and block scraping activity.” LinkedIn  
11 stated that any further access to LinkedIn’s data would violate state and federal law, including  
12 California Penal Code § 502(c), the federal Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C.  
13 § 1030, state common law of trespass, and the Digital Millennium Copyright Act. LinkedIn  
14 reserved the right to pursue litigation, should hiQ fail to cease and desist from accessing  
15 LinkedIn’s website, computer systems, and data.

16           After hiQ and LinkedIn were unable to agree on an amicable resolution, and LinkedIn  
17 declined to permit hiQ’s continued access in the interim, hiQ filed the complaint in this action,  
18 which asserts affirmative rights against the denial of access to publicly available LinkedIn profiles  
19 based on California common law, the UCL, and the California Constitution. hiQ also seeks a  
20 declaration that hiQ has not and will not violate the CFAA, the DMCA, California Penal Code  
21 § 502(c), and the common law of trespass to chattels, by accessing LinkedIn public profiles.  
22 Docket No. 1. At the same time, hiQ also filed a request for a temporary restraining order and an  
23 order to show cause why a preliminary injunction should not be issued against LinkedIn. Docket  
24 No. 23. After a hearing on the TRO request, the parties entered into a standstill agreement  
25 preserving hiQ’s access to the data and converting hiQ’s initial motion into a motion for a  
26 preliminary injunction. A hearing on the motion for preliminary injunction was held on July 27,  
27 2017.

1 **III. DISCUSSION**

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

21 A. **Irreparable Harm and Balance of Hardships**

22 hiQ states that absent injunctive relief, it will suffer immediate and irreparable harm  
23 because its entire business model depends on access to LinkedIn’s data. If LinkedIn prevails, hiQ  
24 will simply go out of business; it “will have to breach its agreements with its customers, stop  
25 discussions with its long list of prospective customers, lay off most if not all its employees, and  
26 shutter its operations.” Docket No. 24 (“Motion”) at 24. These are credible assertions, given the  
27  
28

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

10 For its part, LinkedIn argues that it faces significant harm because hiQ’s data collection  
11 threatens the privacy of LinkedIn users, because even members who opt to make their profiles  
12 publicly viewable retain a significant interest in controlling the use and visibility of their data.<sup>2</sup> In  
13 particular, LinkedIn points to the interest that some users may have in preventing employers or  
14 other parties from tracking *changes* they have made to their profiles. LinkedIn posits that when a  
15 user updates his profile, that action may signal to his employer that he is looking for a new  
16 position. LinkedIn states that over 50 million LinkedIn members have used a “Do Not Broadcast”  
17 feature that prevents the site from notifying other users when a member makes profile changes.  
18 This feature is available even when a profile is set to public. LinkedIn also points to specific user  
19 complaints it has received objecting to the use of data by third parties. In particular, two users  
20 complained that information that they had *previously* featured on their profile, but subsequently  
21

---

22 <sup>1</sup> At the hearing, LinkedIn pointed to the fact that other companies operate in the data analytics  
23 field without making use of LinkedIn’s member data. But as hiQ pointed out, these companies  
24 employ entirely different business models. For example, one company highlighted by LinkedIn,  
25 Glint, creates its own data by taking surveys of employees working for its clients. Requiring hiQ  
26 to rebuild its business on an entirely different business model, such as that employed by Glint,  
27 from scratch would constitute harm comparable to simply going out of business. LinkedIn also  
28 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.

<sup>2</sup> LinkedIn does not claim a proprietary interest in its users’ profiles.

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

11         These considerations are not without merit, but there are a number of reasons to discount  
12 to some extent the harm claimed by LinkedIn. First, LinkedIn emphasizes that the fact that 50  
13 million users have opted into the “Do Not Broadcast” feature indicates that a vast number of its  
14 users are fearful that their employer may monitor their accounts for possible changes. But there  
15 are other potential reasons why a user may opt for that setting. For instance, users may be  
16 cognizant that their profile changes are generating a large volume of unwanted notifications  
17 broadcasted to their connections on the site. They may wish to limit annoying intrusions into their  
18 contacts.<sup>3</sup> Second, LinkedIn has presented little evidence of users’ actual privacy expectation; out  
19 of its hundreds of millions of users, including 50 million using Do Not Broadcast, LinkedIn has  
20 only identified *three* individual complaints specifically raising concerns about data privacy related  
21 to third-party data collection. Docket No. 49-1 Exs. A-C. None actually discuss hiQ or the “Do  
22 Not Broadcast” setting. Third, LinkedIn’s professed privacy concerns are somewhat undermined  
23 by the fact that LinkedIn allows other third-parties to access user data without its members’  
24 knowledge or consent. LinkedIn offers a product called “Recruiter” that allows professional  
25 recruiters to identify possible candidates for other job opportunities. LinkedIn avers that when  
26

---

27 <sup>3</sup> Though the “Do Not Broadcast” feature makes it less likely to draw immediate attention to a  
28 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.

1 users have selected the Do Not Broadcast option, the Recruiter product respects this choice and  
2 does not update recruiters of profile changes. However, hiQ presented marketing materials at the  
3 hearing which indicate that regardless of other privacy settings, information including profile  
4 changes are conveyed to third parties who subscribe to Recruiter. Indeed, these materials inform  
5 potential customers that when they “follow” another user, “[f]rom now on, when they update their  
6 profile or celebrate a work anniversary, you’ll receive an update on your homepage. And don’t  
7 worry – they don’t know you’re following them.” LinkedIn thus trumpets its own product in a  
8 way that seems to afford little deference to the very privacy concerns it professes to be protecting  
9 in this case.

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

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

23 Furthermore, despite the fact that hiQ has been aggregating LinkedIn’s public data for five  
24

---

25 <sup>4</sup> LinkedIn argues hiQ signed up as a LinkedIn user and is thus bound by the User Agreement.  
26 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.

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

1 years with LinkedIn’s knowledge, LinkedIn has presented no evidence of harm, financial or  
2 otherwise resulting from hiQ’s activities. Indeed, LinkedIn has not explained why suddenly it has  
3 now chosen to revoke its consent (or at least tolerance) of hiQ’s use of that data.

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

7 B.  Serious Questions Going to the Merits

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

14 1.  CFAA

15 Whether hiQ’s continued access to the LinkedIn public profiles violates the CFAA  
16 constitutes a key threshold question in this case. The CFAA creates civil and criminal liability for  
17 any person who “intentionally accesses a computer without authorization or exceeds authorized  
18 access, and thereby obtains . . . information from any protected computer.”<sup>6</sup> 18 U.S.C. §  
19 1030(a)(2)(C). As the Supreme Court has explained, the statute “provides two ways of  
20 committing the crime of improperly accessing a protected computer: (1) obtaining access without  
21 authorization; and (2) obtaining access with authorization but then using that access improperly.”  
22 *Musacchio v. United States*, 136 S. Ct. 709, 713 (2016).

23 The key question regarding the applicability of the CFAA in this case is whether, by  
24 continuing to access public LinkedIn profiles after LinkedIn has explicitly revoked permission to  
25 do so, hiQ has “accesse[d] a computer without authorization” within the meaning of the CFAA.

26  
27 \_\_\_\_\_  
28 <sup>6</sup> 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.



1 LinkedIn argues that under the plain meaning of “without authorization,” as well as under relevant  
2 Ninth Circuit authority, hiQ has. LinkedIn relies primarily on two cases.

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

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

27 Each of these cases is distinguishable in an important respect: none of the data in *Facebook*  
28 or *Nosal II* was *public* data. Rather, the defendants in those cases gained access to a computer

1 network (in *Nosal II*) and a portion of a website (in *Power Ventures*) that were protected by a  
2 password authentication system. In short, the unauthorized intruders reached into what would  
3 fairly be characterized as the private interior of a computer system not visible to the public.  
4 Neither of those cases confronted the precise issue presented here: whether visiting and collecting  
5 information from a publicly available website may be deemed “access” to a computer “without  
6 authorization” within the meaning of the CFAA where the owner of the web site has selectively  
7 revoked permission.

8 To be sure, LinkedIn’s construction of the CFAA is not without basis. Visiting a website  
9 accesses the host computer in one literal sense, and where authorization has been revoked by the  
10 website host, that “access” can be said to be “without authorization.” *See Craigslist Inc. v. 3Taps*  
11 *Inc.*, 942 F. Supp. 2d 962 (N.D. Cal. 2013). However, whether “access” to a publicly viewable  
12 site may be deemed “without authorization” under the CFAA where the website host purports to  
13 revoke permission is not free from ambiguity. The Supreme Court has cautioned that “[w]hether a  
14 statutory term is unambiguous . . . does not turn solely on dictionary definitions of its component  
15 words. Rather, ‘the plainness or ambiguity of statutory language is determined [not only] by  
16 reference to the language itself, [but as well by] the specific context in which that language is  
17 used, and the broader context of the statute as a whole.’” *Yates v. United States*, 135 S. Ct. 1074,  
18 1082 (2015) (quoting *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997)) (holding that a fish is  
19 not a “tangible object” within the meaning of the Sarbanes-Oxley Act). *See also Bond v. U.S.*, 134  
20 S.Ct. 2077, 2090 (2014) (rejecting literal reading of Chemical Weapons Convention  
21 Implementation Act that would have permitted prosecution of woman who caused minor chemical  
22 burns to spouse’s lover’s thumb because “[p]art of a fair reading of statutory text is recognizing  
23 that ‘Congress legislates against the backdrop’ of certain unexpressed presumptions”) (quoting  
24 *EEOC v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991)).

25 The CFAA must be interpreted in its historical context, mindful of Congress’ purpose.  
26 The CFAA was not intended to police traffic to publicly available websites on the Internet – the  
27 Internet did not exist in 1984. The CFAA was intended instead to deal with “hacking” or  
28 “trespass” onto private, often password-protected mainframe computers. *See H.R. Rep. No. 98-*

1 894, 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.  
2 2479, 2480 (1986). The Ninth Circuit has recognized this statutory purpose, explaining that  
3 “Congress enacted the CFAA in 1984 primarily to address the growing problem of computer  
4 hacking, recognizing that, “[i]n intentionally trespassing into someone else’s computer files, the  
5 offender obtains at the very least information as to how to break into that computer system.”  
6 *United States v. Nosal (Nosal I)*, 676 F.3d 854, 858 (9th Cir. 2012) (quoting S.Rep. No. 99–432, at  
7 9 (1986), 1986 U.S.C.C.A.N. 2479, 2487 (Conf. Rep.)). It was originally enacted to protect  
8 government computers from hacking; it was expanded in 1986 to protect commercial computer  
9 systems. *See* S.Rep. No. 99–432, at 2 (1986), 1986 U.S.C.C.A.N. 2479, 2480 (Conf. Rep.)). The  
10 Ninth Circuit, in considering a related provision of the statute, cautioned against an overbroad  
11 interpretation that would “expand its scope far beyond computer hacking to criminalize any  
12 unauthorized use of information obtained from a computer,” thereby “mak[ing] criminals of large  
13 groups of people who would have little reason to suspect they are committing a federal crime.”  
14 *Nosal I*, 676 F.3d at 859.

15 As hiQ points out, application of the CFAA to the accessing of websites open to the public  
16 would have sweeping consequences well beyond anything Congress could have contemplated; it  
17 would “expand its scope well beyond computer hacking.” *Nosal I*, 676 F.3d at 859. Under  
18 LinkedIn’s interpretation of the CFAA, a website would be free to revoke “authorization” with  
19 respect to any person, at any time, for any reason, and invoke the CFAA for enforcement,  
20 potentially subjecting an Internet user to criminal, as well as civil, liability. Indeed, because the  
21 Ninth Circuit has specifically rejected the argument that “the CFAA only criminalizes access  
22 where the party circumvents a technological access barrier,” *Nosal II*, 844 F.3d at 1038, merely  
23 *viewing* a website in contravention of a unilateral directive from a private entity would be a crime,  
24 effectuating the digital equivalence of Medusa. The potential for such exercise of power over  
25 access to publicly viewable information by a private entity weaponized by the potential of criminal  
26 sanctions is deeply concerning.<sup>7</sup> This effect would be particularly pernicious because once it is

27 \_\_\_\_\_  
28 <sup>7</sup> 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

1 found to apply, the CFAA as interpreted by LinkedIn would not leave any room for the  
2 consideration of either a website owner’s reasons for denying authorization or an individual’s  
3 possible justification for ignoring such a denial. Website owners could, for example, block access  
4 by individuals or groups on the basis of race or gender discrimination. Political campaigns could  
5 block selected news media, or supporters of rival candidates, from accessing their websites.  
6 Companies could prevent competitors or consumer groups from visiting their websites to learn  
7 about their products or analyze pricing. Further, in addition to criminalizing any attempt to obtain  
8 access to information otherwise viewable by the public at large, the CFAA would preempt all state  
9 and local laws that might otherwise afford a legal right of access (e.g., state law rights asserted by  
10 hiQ herein). A broad reading of the CFAA could stifle the dynamic evolution and incremental  
11 development of state and local laws addressing the delicate balance between open access to  
12 information and privacy – all in the name of a federal statute enacted in 1984 before the advent of  
13 the World Wide Web.<sup>8</sup>

---

15 the CFAA must take into account the fact the statute may be enforced criminally and that its  
16 interpretation would apply uniformly to criminal as well as civil enforcement. *See, e.g., Ratzlaf v.*  
17 *United States*, 510 U.S. 135, 143 (1994) (“A term appearing in several places in a statutory text is  
18 generally read the same way each time it appears. We have even stronger cause to construe a  
19 *single* formulation . . . the same way each time it is called into play.”); *F.C.C. v. American*  
20 *Broadcasting Co.*, 347 U.S. 284, 296 (1954) (rejecting notion that “the same substantive language  
21 has one meaning if criminal prosecutions are brought . . . and quite a different meaning” in civil  
22 action by private party); *U.S. v. Charnay*, 537 F.2d 341, 348 (9th Cir. 1976) (agreeing there was  
23 “no reasonable basis that some different interpretation [of Rule 10b-5] should apply to a criminal  
24 action than in a civil action” for meaning of “deceptive device” under 15 U.S.C. § 78j(b)).

21 <sup>8</sup> LinkedIn argued at the hearing on this motion that the likelihood of these negative consequences  
22 is lessened because violation of the CFAA may be invoked only where the alleged violation  
23 “caused . . . loss . . . aggregating at least \$5,000 in value.” 18 U.S.C. § 1030(c)(4)(A)(i)(1).  
24 However, a violation of § 1030(a)(2) is punishable as a misdemeanor without regard to amount of  
25 loss. 18 U.S.C. § 1030(c)(2)(A). Although felony charges or a civil action may not be brought  
26 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  
27 CFAA defines “loss” broadly as “any reasonable cost to any victim, including the cost of  
28 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.

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

4 Construction of the CFAA, including the terms “access” and “without authorization,”  
5 should be informed not only by Congress’ intent but also by the Act’s theoretical underpinning.  
6 The CFAA’s origin as a statute addressing the problem of computer “trespass” suggests an  
7 interpretation of the statute informed by examining general principles which govern trespass laws.  
8 In an article cited approvingly by the Ninth Circuit in both *Nosal II* and *Power Ventures*, Professor  
9 Orin Kerr argues the analogy to trespass laws is key to understanding the appropriate scope of the  
10 “without authorization” provision of the CFAA. *See* Orin S. Kerr, *Norms of Computer Trespass*,  
11 116 Colum. L. Rev. 1143 (2016). Kerr argues that in the context of physical space, whether or not  
12 an action constitutes a trespass depends on a set of shared social norms that “tell us, at an intuitive  
13 level, when entry to property is forbidden and when it is permitted.” *Id.* at 1149. Thus, the Court  
14 understands that it is generally impermissible to enter into a private home without permission in  
15 any circumstances. By contrast, it is presumptively *not* trespassing to open the unlocked door of a  
16 business during daytime hours because “the shared understanding is that shop owners are normally  
17 open to potential customers.” *Id.* at 1151. These norms, moreover, govern not only the time of  
18 entry but the manner; entering a business through the back window might be a trespass even when  
19 entering through the door is not.

20 Kerr argues that the process of discerning and applying similar norms should govern  
21 “trespass” in the digital realm, and that because the Web is generally perceived as “inherently  
22 open,” in that it “allows anyone in the world to publish information that can be accessed by  
23 anyone else without requiring authentication,” courts should incorporate this norm by “adopt[ing]  
24 presumptively open norms for the Web.” *Id.* at 1162. This general understanding of the open  
25 nature of the Web squares with language used in a recent Supreme Court decision relied on by  
26 *hiQ*. In *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017), the Court struck down a North  
27 Carolina law making it a felony for a registered sex offender to access social media websites like  
28 Facebook and Twitter. The Court explained that at present, social media sites are for many people

1 “the principal sources for knowing current events, checking ads for employment, speaking and  
2 listening in the modern public square, and otherwise exploring the vast realms of human thought  
3 and knowledge.” *Id.* at 1737. The Court’s analogy of the Internet in general, and social  
4 networking sites in particular, to the “modern public square,” *id.*, embraces the social norm that  
5 assumes the openness and accessibility of that forum to all comers. *Cf. Ampex Corp. v. Cargle*,  
6 128 Cal. App. 4th 1569, 1576 (2005) (“Web sites that are accessible free of charge to any member  
7 of the public where members of the public may read the views and information posted, and post  
8 their own opinions, meet the definition of a public forum for purposes of section 425.16 [the  
9 California anti-SLAPP statute].”).

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

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

21 *Id.* at 1161. This approach would square with the results in both *Nosal II* and *Power Ventures*  
22 while avoiding the negative consequences of an overly broad reading of “authorization.” In both  
23 *Nosal II* and *Power Ventures*, the defendants had bypassed a password authentication system. In  
24 that sense, their “access” was, as *Nosal II* explained, clearly “without authorization” within the  
25 meaning of the CFAA. And while *Nosal II* stated that the term “authorization” has a plain and  
26 ordinary meaning, that meaning was in the context of determining whether a former employer  
27 could control “access” to its *private* data protected by an authentication process. The plain  
28 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

1 authorization” such that “a defendant can run afoul of the CFAA when he or she has no  
2 permission to access a computer or when such permission has been revoked explicitly.” *Power*  
3 *Ventures*, 844 F.3d at 1067. But, as noted above, in the context of a publicly viewable web page  
4 open to all on the Internet, the “plainness” of the meaning of “access” “without authorization” is  
5 less obvious. Context matters.

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

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

19 Lastly, with respect to the CFAA, LinkedIn argues in part that what it objects to is not  
20 merely hiQ’s access to the site, but hiQ’s automated scraping of user data. But “authorization,” as  
21 used in CFAA § 1030(a)(2), is most naturally read in reference to the *identity* of the person  
22 accessing the computer or website, not *how* access occurs. *Cf. Nosal I*, 676 F.3d at 857-59  
23 (distinguishing between unauthorized access to versus use of data). Thus, Professor Kerr  
24 persuasively argues that where an individual employs an automated program that bypasses a  
25 CAPTCHA – a program designed to allow humans but to block “bots” from accessing a site – he  
26 has still not entered the website “without authorization.” Unlike a password gate, a CAPTCHA  
27 does not limit access to certain individuals; it is instead intended “as a way to slow[] a user’s  
28 access rather than as a way to deny authorization to access.” Kerr, *supra*, at 1170. Other

1 measures taken by website owners to block or limit access to bots may be thought of in the same  
2 way. A user does not “access” a computer “without authorization” by using bots, even in the face  
3 of technical countermeasures, when the data it accesses is otherwise open to the public.<sup>9</sup> Thus,  
4 under Professor Kerr’s analysis, hiQ’s circumvention of LinkedIn’s measures to prevent use of  
5 bots and implementation of IP address blocks does not violate the CFAA because hiQ accessed  
6 only publicly viewable data not protected by an authentication gateway.<sup>10</sup>

7 This is not to say that a website like LinkedIn cannot employ, *e.g.*, anti-bot measures to  
8 prevent, *e.g.*, harmful intrusions or attacks on its server. Finding the CFAA inapplicable to hiQ’s  
9 actions does not remove all arrows from LinkedIn’s legal quiver against malicious attacks.<sup>11</sup>

10 The Court therefore concludes that hiQ has, at the very least, raised serious questions as to  
11 applicability of the CFAA to its conduct.<sup>12</sup> Accordingly, the Court cannot conclude, at this stage,

---

12  
13 <sup>9</sup> To take the analogy above another step, when a business displays a sign in a storefront window  
14 for the public to view, it may not prohibit on pain of trespass a viewer from photographing that  
15 sign or viewing it with glare reducing sunglasses.

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

19 <sup>11</sup> In addition to technological self-help, LinkedIn may be able to pursue other legal remedies. For  
20 example, LinkedIn argues that if it cannot invoke the CFAA to prevent unauthorized access by  
21 bots, it may be left open to denial of service attacks. However, the CFAA creates liability against  
22 “[w]hoever” – whether access is authorized or not – “causes the transmission of a program,  
23 information, code, or command, and as a result of such conduct, intentionally causes damage  
24 without authorization, to a protected computer.” 18 U.S.C. § 1030(a)(5)(A). Additionally, such  
25 attacks are likely remediable under, *e.g.*, the common law tort of trespass to chattel. Trespass to  
26 chattel requires a plaintiff to prove that a defendant intentionally interfered with plaintiff’s use or  
27 possession of personal property, with resultant injury. *See California Civil Jury Instructions 2101*;  
28 *Itano v. Colonial Yacht Anchorage*, 267 Cal. App. 2d 84, 90 (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 (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).

<sup>12</sup> 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 (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*,



1 that the CFAA preempts hiQ’s affirmative claims under state law. The question then is whether  
2 hiQ is entitled to preliminary injunctive relief not only against enforcement of the CFAA but also  
3 against the use of technological barriers. To obtain such relief, hiQ would have to raise at least  
4 serious questions as to whether it has rights under state laws which are violated by LinkedIn’s  
5 conduct. The Court thus turns to those state claims.<sup>13</sup>

6  
7 *e.g.*, *Brunette v. Humane Society of Ventura County*, 294 F.3d 1205, 1210 (9th Cir. 2002) (private  
8 party may be deemed to have engaged in state action if it is a willful participant in joint action  
9 with the government; if the government has insinuated itself into a position of interdependence  
10 with it; and if it performs functions traditionally and exclusively reserved to the states); *Brentwood  
11 Academy v. Tennessee Secondary School Athletic Ass’n*, 531 U.S. 288, 300-301 (2001) (state  
12 action may be found where private entity is controlled by an agency of the state, when its activity  
13 results from the state’s exercise of coercive power, when the state provides encouragement, or  
14 when government is “entwined” in the entity’s policies, management, or control). LinkedIn is not  
15 a state official or governmental agency; it is a private party and there is no evidence that the  
16 CFAA has served to compel or encourage LinkedIn to withdraw hiQ’s authorization to access its  
17 website. Compare *Brentwood Academy*, 531 U.S. at 300 (private party’s actions may be  
18 characterized as state action “when the State provides significant encouragement, either overt or  
19 covert”) (citation and quotation omitted) with *Blum v. Yaretsky*, 457 U.S. 991, 1005 (1982)  
20 (nursing homes’ decisions to discharge patients were not state action because they were made by  
21 private parties according to professional standards not established by the state, and the simple fact  
22 “[t]hat the State responds to such actions by adjusting benefits does not render it *responsible* for  
23 those actions”). However, the same interpretation of the statute would apply uniformly to both  
24 civil and criminal actions, *see supra* n.7, and a criminal prosecution under the CFAA would  
25 undoubtedly constitute state action. Thus, because the act of viewing a publicly accessible website  
26 is likely protected by the First Amendment (*see, e.g., Packingham*, 137 S.Ct. at 1737 (statute’s  
27 prohibition on sex offender access to social media websites raised serious First Amendment  
28 concerns because, *inter alia*, “[s]ocial media allows users to gain access to information . . .”);  
*Kleindienst v. Mandel*, 408 U.S. 753, 762-63 (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 (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 (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 (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.

<sup>13</sup> 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 (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

1           2.       California Constitutional Claim

2           hiQ argues that LinkedIn’s actions violate California’s constitutional free speech  
3 protections. Article I, Section 2 of the California Constitution provides that “[e]very person may  
4 freely speak, write, and publish his or her sentiments on all subjects.” The California Supreme  
5 Court has long recognized that this provision confers broader free speech rights than those  
6 provided by the First Amendment. *See Dailey v. Superior Court of City & Cty. of San Francisco*,  
7 112 Cal. 94, 97-98 (1896). In particular, unlike the First Amendment, California’s provision is not  
8 limited to restraining state entities. The California Supreme Court, in its landmark decision in  
9 *Robins v. Pruneyard Shopping Ctr.*, 23 Cal. 3d 899, 905 (1979), held that the state’s guarantee of  
10 free expression may take precedence over the rights of private property owners to exclude people  
11 from their property. *Robins* concerned attempts by a large shopping mall to exclude individuals  
12 engaging in political speech. In holding that this speech was protected by the state constitution,  
13 the court emphasized the importance of the shopping mall as a public forum and center of  
14 community life, a place where “25,000 persons are induced to congregate daily to take advantage  
15 of the numerous amenities offered.” *Id.* at 910.

16           hiQ argues that LinkedIn is an internet-age equivalent to the Pruneyard Shopping Center.  
17 hiQ notes that like the shopping center, “LinkedIn opens the public profile section of its website to  
18 the public. LinkedIn promises its members that the public profiles on its site can be viewed by  
19 everyone.” Motion at 17. Moreover, LinkedIn “expressly holds itself out as a place ‘to meet,  
20 exchange ideas, [and] learn,’ . . . making it a modern-day equivalent of the shopping mall or town  
21 square, a marketplace of ideas on a previously unimaginable scale.” *Id.* For that reason, hiQ  
22 argues, it has a right under the California Constitution to access that marketplace on equal terms  
23 with all other people and that LinkedIn’s private property rights in controlling access to its  
24 computers cannot take precedence. *Cf. Nicholson v. McClatchy Newspapers*, 177 Cal.App.3d  
25 509, (1986) (concluding that under federal case-law, “[w]hile reporters are not privileged to

---

26  
27 prohibits “knowingly access[ing] and without permission tak[ing], cop[y]ing, or mak[ing] use of  
28 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.

1 commit crimes and independent torts in gathering the news, and the press has no special  
2 constitutional right of access to information, ‘news gathering is not without its First Amendment  
3 protections’”) (quoting *Branzburg*, 408 U.S. at 707). See generally *Beeman v. Anthem*  
4 *Prescription Management, LLC*, 58 Cal.4th 329, 341 (2013) (“The state Constitution’s free speech  
5 provision is at least as broad as and in some ways is broader than the comparable provision of the  
6 federal Constitution’s First Amendment.”) (citations and quotations omitted); *Dailey, supra*, 112  
7 Cal. at 97-98.

8 No court has expressly extended *Pruneyard* to the Internet generally. Although the  
9 California Supreme Court has held that, under *Pruneyard*, “the actions of a private property owner  
10 constitute state action for purposes of California’s free speech clause only if the property is freely  
11 and openly accessible to the public,” *Golden Gateway Center v. Golden Gateway Tenants Assn.*,  
12 26 Cal.4th 1013, 1033 (2001), this discussion occurred in the context of real property. Though  
13 certain spaces on the Internet share important characteristics of the traditional public square, see,  
14 e.g., *Packingham*, 137 S. Ct. at 1737 (characterizing social network sites as “the modern public  
15 square”), at this juncture, the Court has doubts about whether *Pruneyard* may be extended  
16 wholesale into the digital realm of the Internet. No court has had occasion to so hold or to  
17 consider the reach and potentially sweeping consequences of such a holding. For instance, would  
18 all publicly viewable websites on the Internet be subject to constitutional constraints regardless of  
19 size of the business? Does *Pruneyard*, which involves a single owner of the public forum (the  
20 shopping center), apply to a website which constitutes only a portion of the Internet and where  
21 there is no single controlling entity? Would the entire Internet or only a particular collection of  
22 websites constitute a public forum? If the Internet were a public forum governed by constitutional  
23 speech, would social network sites such as Facebook be prohibited from engaging in any content-  
24 based regulation of postings? The analogy between a shopping mall and the Internet is imperfect,  
25 and there are a host of potential “slippery slope” problems that are likely to surface were  
26 *Pruneyard* to apply to the Internet.

27 It is true that a number of California state courts have determined that publicly accessible  
28 websites may constitute public fora within the meaning of the state’s anti-SLAPP law. In *Ampex*

1 *Corp.*, the California Court of Appeal held that postings made on an internet message board  
2 constituted speech in a public forum for the purposes of the statute. The court explained that  
3 “[t]he term ‘public forum’ includes forms of public communication other than those occurring in a  
4 physical setting. Thus the electronic communication media may constitute public forums. Web  
5 sites that are accessible free of charge to any member of the public where members of the public  
6 may read the views and information posted, and post their own opinions, meet the definition of a  
7 public forum *for purposes of section 425.16.*” *Ampex Corp.*, 128 Cal. App. 4th at 1576 (emphasis  
8 added). The reach of the anti-SLAPP statute is broader than the scope of constitutionally  
9 protected speech; it applies to a cause of action arising from an act “in furtherance of” the person’s  
10 right of free speech under the constitution. Cal. Civ. Proc. Code § 425.16(b); *Ampex Corp.*, 128  
11 Cal. App. 4th at 1575; *cf. Lieberman v. KCOP Television, Inc.*, 110 Cal. App. 4th 156, 166, 1 Cal.  
12 Rptr. 3d 536, 542 (2003) (explaining that the anti-SLAPP law’s protections are “not limited to the  
13 exercise of [the] right of free speech, but to all conduct *in furtherance* of the exercise of the right  
14 to free speech in connection with a public issue” (emphasis in original)).

15 Similarly, in *Barrett v. Rosenthal*, 40 Cal.4th 33 (2006), two physicians brought an action  
16 for libel and libel per se against a health activist who had posted messages attacking the  
17 physicians’ character to publicly accessible Internet newsgroups. The California Supreme Court  
18 agreed with the Court of Appeals that “[w]eb sites accessible to the public . . . are ‘public forums’  
19 for the purposes of the anti-SLAPP statute.” *Id.* at 41 n.4. As in *Ampex*, however, this holding  
20 was limited to whether the defendant could invoke the anti-SLAPP statute’s protections. Indeed,  
21 the Court of Appeals in that case had treated the speech in question as “act or acts . . . taken ‘*in*  
22 *furtherance* of [her] right of petition or free speech”” under the anti-SLAPP law. *Barrett v.*  
23 *Rosenthal*, 9 Cal.Rptr.3d 142, 149 (Ct. App. 2004) (emphasis added).

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

1 its constitutional rights under the California Constitution.

2 3. UCL Claim

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

7 The UCL broadly prohibits any “unlawful, unfair or fraudulent business act or practices.”  
8 *Id.* Practices are “unfair” when grounded in “some legislatively declared policy or proof of some  
9 actual or threatened effect on competition.” *Cel-Tech Commc’ns, Inc. v. Los Angeles Cellular Tel.*  
10 *Co.*, 20 Cal. 4th 163, 187 (1999). One such set of policies are those embodied in the federal  
11 antitrust laws. *Id.*; *see also Blank v. Kirwan*, 39 Cal. 3d 311, 320 (1985) (noting that California  
12 law looks to the Sherman Act for guidance). Significantly, however, “unfair” practices under the  
13 UCL are not limited to actual antitrust violations, but also include “conduct that threatens an  
14 incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because  
15 its effects are comparable to or the same as a violation of the law, or otherwise significantly  
16 threatens or harms competition.” *Cel-Tech*, 20 Cal. 4th at 187.

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

27 The Sherman Act prohibits companies from leveraging monopoly power to “foreclose  
28 competition or gain a competitive advantage, or to destroy a competitor.” *Otter Tail Power Co. v.*

1 *United States*, 410 U.S. 366, 377 (1973). In this case, hiQ plausibly asserts that LinkedIn enjoys a  
2 position as the dominant power in the market of professional networking. Furthermore, hiQ has  
3 presented evidence that LinkedIn is seeking to compete with hiQ in the market of data analytics.  
4 In a news segment airing on national television on June 21, 2017, LinkedIn’s CEO announced that  
5 “[w]hat LinkedIn would like to do is leverage all this extraordinary data we’ve been able to collect  
6 by virtue of having 500 million people join the site . . . to make sure that each individual member  
7 has information about where those jobs are” and that “[f]or employers, [the goal is to provide] an  
8 understanding of what skills they’re gonna need to be able to continue to grow, and where that  
9 talent exists.” Docket No. 34 (Gupta Decl.) Ex. U. at 2. In other words, LinkedIn appears to be  
10 developing a product that competes directly with hiQ’s Skill Mapper product, which helps  
11 employers understand what skills the members of their workforces possess. There is thus a  
12 plausible inference that LinkedIn terminated hiQ’s access to its public member data in large part  
13 because it wanted exclusive control over that data for its own business purposes; as noted above,  
14 hiQ faces an existential threat. That inference is supported by the timing of the commencement of  
15 its employer product which appears to coincide roughly with its terminating hiQ’s access.

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

26 To be sure, LinkedIn may well be able to demonstrate it was not motivated by anti-  
27 competitive purposes and that there is in fact no threatened anti-trust violation; instead, it is  
28 motivated by a desire to preserve user privacy preferences and its users’ trust. But, hiQ has

1 presented some evidence supporting its assertion that LinkedIn’s decision to revoke hiQ’s access  
2 to its data was made for the purpose of eliminating hiQ as a competitor in the data analytics field,  
3 and thus potentially “violates the policy or spirit” of the Sherman Act. *Cel-Tech*, 20 Cal. 4th at  
4 187. While hiQ will have to do much more to prove such a claim, it has raised at least serious  
5 enough questions on the merits of its UCL claim at this juncture to support the issuance of a  
6 preliminary injunction.

7 4. Promissory Estoppel

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

20 C. Public Interest

21 At the final step of its preliminary injunction analysis, the Court must consider where the  
22 public interest lies. Here, each party contends that the public interest favors its position, because  
23 each party believes that its position will maximize the free flow of information. hiQ argues that a  
24

---

25 <sup>14</sup> hiQ also asserts a common law claim of tortious interference with contract, but the California  
26 Supreme Court has held that such a claim is foreclosed as long as the defendant “had a legitimate  
27 business purpose which justified its actions.” *Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal.  
28 4th 26, 57 (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.





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

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

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

17 3. This preliminary injunction shall take effect immediately.

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

20 This order disposes of Docket No. 23.

21

22 **IT IS SO ORDERED.**

23


24 Dated: August 14, 2017

25

26

27

28

  
EDWARD M. CHEN  
United States District Judge