FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

HIQ LABS, INC., *Plaintiff-Appellee*, v. LINKEDIN CORPORATION, *Defendant-Appellant.*	No. 17-16783 D.C. No. 3:17-cv-03301-EMC OPINION

On Remand from the United States Supreme Court

Argued and Submitted October 18, 2021
San Francisco, California

Filed April 18, 2022

Before: J. Clifford Wallace and Marsha S. Berzon, Circuit Judges, and Terrence Berg,[*] District Judge.

Opinion by Judge Berzon

[*] The Honorable Terrence Berg, United States District Judge for the Eastern District of Michigan, sitting by designation.

SUMMARY[**]

Preliminary Injunction / Computer Fraud and Abuse Act

On remand from the United States Supreme Court, the panel affirmed the district court's order preliminarily enjoining LinkedIn Corp. from denying hiQ Labs, Inc., a data analytics company, access to publicly available member profiles on LinkedIn's professional networking website.

The panel previously affirmed the preliminary injunction. The Supreme Court granted certiorari, vacated the panel's judgment, and remanded for further consideration in light of *Van Buren v. United States*, 141 S. Ct. 1648 (2021). On remand, the panel again affirmed the preliminary injunction, concluding that *Van Buren* reinforced its determination that hiQ had raised serious questions about whether LinkedIn may invoke the Computer Fraud and Abuse Act ("CFAA") to preempt hiQ's possibly meritorious tortious interference claim.

The panel held that a plaintiff seeking a preliminary injunction must establish that it is likely to succeed on the merits, that it is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in its favor, and that an injunction is in the public interest. The court uses a "sliding scale" approach to these factors, so that when the balance of hardships tips sharply in the plaintiff's favor, it need demonstrate only serious questions going to the merits. Applying this approach, the district

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

court concluded that the balance of hardships tipped sharply in hiQ's favor and that hiQ raised serious questions on the merits.

The panel held that the district court did not abuse its discretion in concluding on the preliminary injunction record that hiQ currently had no viable way to remain in business other than using LinkedIn public profile data for its "Keeper" and "Skill Mapper" analytics services, and that hiQ therefore had demonstrated a likelihood of irreparable harm absent a preliminary injunction.

The panel concluded that the district court properly determined that the balance of hardships tipped sharply in hiQ's favor, when weighing the likelihood that hiQ would go out of business against LinkedIn's assertion that an injunction threatened its members' privacy and therefore put at risk the goodwill that LinkedIn had developed with its members.

The panel concluded that hiQ showed a sufficient likelihood of establishing the elements of its claim for intentional interference with contract, and it raised a serious question on the merits of LinkedIn's affirmative justification defense. Further, hiQ raised serious questions about whether LinkedIn could invoke the CFAA to preempt hiQ's possibly meritorious tortious interference claim. The CFAA prohibits accessing a "protected computer" without authorization. The panel concluded that to scrape LinkedIn data, hiQ needed to access LinkedIn servers, which were "protected computers." At issue was whether, once hiQ received LinkedIn's cease-and-desist letter, any further scraping and use of LinkedIn's data was "without authorization" within the meaning of the CFAA. The panel concluded that hiQ raised a serious question as to whether

the CFAA "without authorization" concept is inapplicable where, as here, prior authorization is not generally required but a particular person—or bot—is refused access. The panel concluded that the reasoning of *Van Buren* reinforced its interpretation of the CFAA, although *Van Buren* did not directly address the CFAA's "without authorization" clause, but rather considered the statute's "exceeds authorized access" clause.

Finally, the panel concluded that the district court properly determined that, on balance, the public interest favored hiQ's position.

The panel affirmed the district court's determination that hiQ had established the elements required for a preliminary injunction and remanded for further proceedings.

COUNSEL

Donald B. Verrilli Jr. (argued), Chad I. Golder, Rosemarie T. Ring, and Jonathan S. Meltzer, Munger Tolles & Olson LLP, Washington, D.C.; Jonathan H. Blavin, Nicholas Fram, and Elia Herrera, Munger Tolles & Olson LLP, San Francisco, California; E. Joshua Rosenkranz, Orrick Herrington & Sutcliffe LLP, New York, New York; Eric A. Shumsky, Orrick Herrington & Sutcliffe LLP, Washington, D.C.; for Defendant-Appellant.

Renita Sharma (argued) and Richard Corey, Quinn Emmanuel Urquhart & Sullivan LLP, New York, New York; Terry Wit, Quinn Emmanuel Urquhart & Sullivan LLP, San Francisco, California; Aaron M. Panner, Gregory G. Rapawy, and T. Dietrich Hill, Kellogg Hansen Todd Figel & Frederick PLLC, Washington, D.C.; C. Brandon Wisoff, Deepak Gupta, Jeffrey G. Lau, and Rebecca H. Stephens, Farella Braun & Martell LLP, San Francisco, California; Laurence H. Tribe, Cambridge, Massachusetts; for Plaintiff-Appellee.

Nicholas J. Boyle, John S. Williams, and Eric J. Hamilton, Williams & Connolly LLP, Washington, D.C., for Amicus Curiae CoStar Group Inc.

Perry J. Viscounty, Latham & Watkins LLP, San Francisco, California; Gregory G. Garre, Latham & Watkins LLP, Washington, D.C.; for Amicus Curiae Craigslist Inc.

Alan J. Butler and Marc Rotenberg, Electronic Privacy Information Center, Washington, D.C., for Amicus Curiae Electronic Privacy Information Center (EPIC).

Mukund Rathi, Aaron Mackey, Kurt Opsahl, Jamie Williams, Corynne McSherry, Cindy Cohn, Nathan Cardozo, Electronic Frontier Foundation, San Francisco, California, for Amici Curiae Electronic Frontier Foundation, DuckDuckGo, and Internet Archive.

Thomas V. Christopher, Law Offices of Thomas V. Christopher, San Francisco, California, for Amicus Curiae 3taps Inc.

Kenneth L. Wilton and James M. Harris, Seyfarth Shaw LLP, Los Angeles, California; Carrie P. Price, Seyfarth Shaw LLP, San Francisco, California; for Amicus Curiae Scraping Hub Ltd.

Katie Townsend, Bruce D. Brown, Gabe Rottman, Grayson Clary, and Mailyn Fidler, Reporters Committee for Freedom of the Press, Washington, D.C., for Amici Curiae Reporters Committee for Freedom of the Press and 30 News Media Organizations.

OPINION

BERZON, Circuit Judge:

We first issued an opinion in this case in September 2019, addressing the question whether LinkedIn, the professional networking website, could prevent a competitor, hiQ, from collecting and using information that LinkedIn users had shared on their public profiles, available for viewing by anyone with a web browser. *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019). HiQ, a data analytics company, had obtained a preliminary injunction forbidding LinkedIn from denying hiQ access to publicly available LinkedIn member profiles. At the preliminary injunction stage, we did not resolve the companies' legal dispute definitively, nor did we address all the claims and defenses they had pleaded in the district court. Instead, we focused on whether hiQ had raised serious questions on the merits of the factual and legal issues presented to us, as well as on the other requisites for preliminary relief. We concluded that hiQ had done so, and we therefore upheld the preliminary injunction.

The Supreme Court granted LinkedIn's petition for writ of certiorari, vacated the judgment, and remanded this case for further consideration in light of *Van Buren v. United States*, 141 S. Ct. 1648 (2021). *LinkedIn Corp. v. hiQ Labs, Inc.*, 141 S. Ct. 2752 (2021). We ordered supplemental briefing and held oral argument on the effect of *Van Buren* on this appeal. Having concluded that *Van Buren* reinforces our determination that hiQ has raised serious questions about whether LinkedIn may invoke the Computer Fraud and Abuse Act ("CFAA") to preempt hiQ's possibly meritorious tortious interference claim, we once again affirm the preliminary injunction.

I.

Founded in 2002, LinkedIn is a professional networking website with over 500 million members.[1] Members post resumes and job listings and build professional "connections" with other members. LinkedIn specifically disclaims ownership of the information users post to their personal profiles: according to LinkedIn's User Agreement, members own the content and information they submit or post to LinkedIn and grant LinkedIn only a non-exclusive license to "use, copy, modify, distribute, publish, and process" that information.

LinkedIn allows its members to choose among various privacy settings. Members can specify which portions of their profile are visible to the general public (that is, to both LinkedIn members and nonmembers), and which portions are visible only to direct connections, to the member's "network" (consisting of LinkedIn members within three degrees of connectivity), or to all LinkedIn members.[2] This

[1] Our recitation of the facts reflects the record before us when this appeal was initially submitted in 2018. Given the speed at which the Internet evolves, we do not doubt that some of the facts presented here became obsolete while this case traveled to the Supreme Court and back. In addition, LinkedIn recently filed a motion in the district court to dissolve the preliminary injunction on the ground that hiQ is "out of business." Order Deferring Ruling on Defendant's Motion to Dissolve Preliminary Injunction, No. 17-cv-03301-EMC, at 2 (N.D. Cal. Oct. 5, 2021), ECF 224. HiQ responded that it remains an intact business entity and has been approached by "prospective business partners" interested in "its technology that allows for automated access of public profiles on LinkedIn's website." *Id.* The district court deferred ruling on the motion pending our decision in this appeal. *Id.* at 3.

[2] Direct connections (or first-degree connections) are people to whom a LinkedIn member is connected by virtue of having invited them

case deals only with profiles made visible to the general public.

LinkedIn also offers all members—whatever their profile privacy settings—a "Do Not Broadcast" option with respect to every change they make to their profiles. If a LinkedIn member selects this option, her connections will not be notified when she updates her profile information, although the updated information will still appear on her profile page (and thus be visible to anyone permitted to view her profile under her general privacy setting). More than 50 million LinkedIn members have, at some point, elected to employ the "Do Not Broadcast" feature, and approximately 20 percent of all active users who updated their profiles between July 2016 and July 2017—whatever their privacy setting—employed the "Do Not Broadcast" setting.

LinkedIn has taken steps to protect the data on its website from what it perceives as misuse or misappropriation. The instructions in LinkedIn's "robots.txt" file—a text file used by website owners to communicate with search engine crawlers and other web robots—prohibit access to LinkedIn servers via automated bots, except that certain entities, like the Google search engine, have express permission from

to connect and had the invitation accepted, or of having accepted their invitation to connect. Second-degree connections are people connected to a member's first-degree connections. Third-degree connections are people connected to a member's second-degree connections. A LinkedIn member's network consists of the member's first-degree, second-degree, and third-degree connections, as well as fellow members of the same LinkedIn Groups (groups of members in the same industry or with similar interests that any member can request to join).

LinkedIn for bot access.[3] LinkedIn also employs several technological systems to detect suspicious activity and restrict automated scraping.[4] For example, LinkedIn's Quicksand system detects non-human activity indicative of scraping; its Sentinel system throttles (slows or limits) or even blocks activity from suspicious IP addresses;[5] and its

[3] A web robot (or "bot") is an application that performs automated tasks such as retrieving and analyzing information. *See Definition of "bot,"* Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/bot (last visited March 15, 2022). A web crawler is one common type of bot that systematically searches the Internet and downloads copies of web pages, which can then be indexed by a search engine. *See Assoc. Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 544 (S.D.N.Y. 2013); *Definition of "web crawler,"* Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/web%20crawler (last visited March 15, 2022). A robots.txt file, also known as the robots exclusion protocol, is a widely used standard for stating the rules that a web server has adopted to govern a bot's behavior on that server. *See About /robots.txt*, http://www.robotstxt.org/robotstxt.html (last visited March 15, 2022). For example, a robots.txt file might instruct specified robots to ignore certain files when crawling a site, so that the files do not appear in search engine results. Adherence to the rules in a robots.txt file is voluntary; malicious bots may deliberately choose not to honor robots.txt rules and may in turn be punished with a denial of access to the website in question. *See Can I Block Just Bad Robots?*, http://www.robotstxt.org/faq/blockjustbad.html (last visited March 15, 2022); *cf. Assoc. Press*, 931 F. Supp. 2d at 563.

[4] Scraping involves extracting data from a website and copying it into a structured format, allowing for data manipulation or analysis. *See, e.g.*, *What Is a Screen Scraper?*, WiseGeek, http://www.wisegeek.com/what-is-a-screen-scraper.htm (last visited March 15, 2022). Scraping can be done manually, but as in this case, it is typically done by a web robot or "bot." *See supra* note 3.

[5] "IP address" is an abbreviation for Internet protocol address, which is a numerical identifier for each computer or network connected to the Internet. *See Definition of "IP Address,"* Merriam-Webster

Org Block system generates a list of known "bad" IP addresses serving as large-scale scrapers. In total, LinkedIn blocks approximately 95 million automated attempts to scrape data every day, and has restricted over 11 million accounts suspected of violating its User Agreement,[6] including through scraping.

HiQ is a data analytics company founded in 2012. Using automated bots, it scrapes information that LinkedIn users have included on public LinkedIn profiles, including name, job title, work history, and skills. It then uses that information, along with a proprietary predictive algorithm, to yield "people analytics," which it sells to business clients.

HiQ offers two such analytics. The first, Keeper, purports to identify employees at the greatest risk of being recruited away. According to hiQ, the product enables employers to offer career development opportunities, retention bonuses, or other perks to retain valuable employees. The second, Skill Mapper, summarizes employees' skills in the aggregate. Among other things, the tool is supposed to help employers identify skill gaps in their

---

Dictionary, https://www.merriam-webster.com/dictionary/IP%20address (last visited March 15, 2022).

[6] Section 8.2 of the LinkedIn User Agreement to which hiQ agreed states that users agree not to "[s]crape or copy profiles and information of others through any means (including crawlers, browser plugins and add-ons, and any other technology or manual work)," "[c]opy or use the information, content or data on LinkedIn in connection with a competitive service (as determined by LinkedIn)," "[u]se manual or automated software, devices, scripts robots, other means or processes to access, 'scrape,' 'crawl' or 'spider' the Services or any related data or information," or "[u]se bots or other automated methods to access the Services." HiQ is no longer bound by the User Agreement, as LinkedIn has terminated hiQ's user status.

workforces so that they can offer internal training in those areas, promoting internal mobility and reducing the expense of external recruitment.

HiQ regularly organizes "Elevate" conferences, during which participants discuss hiQ's business model and share best practices in the people analytics field. LinkedIn representatives participated in Elevate conferences beginning in October 2015. At least ten LinkedIn representatives attended the conferences. LinkedIn employees have also spoken at Elevate conferences. In 2016, a LinkedIn employee was awarded the Elevate "Impact Award." LinkedIn employees thus had an opportunity to learn about hiQ's products, including "that [one of] hiQ's product[s] used data from a variety of sources—internal and external—to predict employee attrition" and that hiQ "collected skills data from public professional profiles in order to provide hiQ's customers information about their employees' skill sets."

In recent years, LinkedIn has explored ways to capitalize on the vast amounts of data contained in LinkedIn profiles by marketing new products. In June 2017, LinkedIn's Chief Executive Officer ("CEO"), Jeff Weiner, appearing on CBS, explained that LinkedIn hoped to "leverage all this extraordinary data we've been able to collect by virtue of having 500 million people join the site." Weiner mentioned as possibilities providing employers with data-driven insights about what skills they will need to grow and where they can find employees with those skills. Since then, LinkedIn has announced a new product, Talent Insights,

which analyzes LinkedIn data to provide companies with such data-driven information.[7]

In May 2017, LinkedIn sent hiQ a cease-and-desist letter, asserting that hiQ was in violation of LinkedIn's User Agreement and demanding that hiQ stop accessing and copying data from LinkedIn's server. The letter stated that if hiQ accessed LinkedIn's data in the future, it would be violating state and federal law, including the CFAA, the Digital Millennium Copyright Act ("DMCA"), California Penal Code § 502(c), and the California common law of trespass. The letter further stated that LinkedIn had "implemented technical measures to prevent hiQ from accessing, and assisting others to access, LinkedIn's site, through systems that detect, monitor, and block scraping activity."

HiQ's response was to demand that LinkedIn recognize hiQ's right to access LinkedIn's public pages and to threaten to seek an injunction if LinkedIn refused. A week later, hiQ filed an action, seeking injunctive relief based on California law and a declaratory judgment that LinkedIn could not lawfully invoke the CFAA, the DMCA, California Penal Code § 502(c), or the common law of trespass against it. HiQ

[7] The record does not specifically name Talent Insights, but at a district court hearing on June 29, 2017, counsel for hiQ referenced Mr. Weiner's statements on CBS and stated that "in the past 24 hours we've received word . . . that LinkedIn is launching a product that is essentially the same or very similar to [hiQ's] Skill Mapper, and trying to market it head-to-head against us." LinkedIn has since launched Talent Insights, which, among other things, promises to help employers "understand the . . . skills that are growing fastest at your company." *See* https://business.linkedin.com/talent-solutions/blog/product-updates/2018/linkedin-talent-insights-now-available (last visited March 15, 2022).

also filed a request for a temporary restraining order, which the parties subsequently agreed to convert into a motion for a preliminary injunction.

The district court granted hiQ's motion. It ordered LinkedIn to withdraw its cease-and-desist letter, to remove any existing technical barriers to hiQ's access to public profiles, and to refrain from putting in place any legal or technical measures with the effect of blocking hiQ's access to public profiles. LinkedIn timely appealed.

II.

"A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). All four elements must be satisfied. *See, e.g.*, *Am. Trucking Ass'n v. City of Los Angeles*, 559 F.3d 1046, 1057 (9th Cir. 2009). We use a "sliding scale" approach to these factors, according to which "a stronger showing of one element may offset a weaker showing of another." *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011). So, when the balance of hardships tips sharply in the plaintiff's favor, the plaintiff need demonstrate only "serious questions going to the merits." *Id.* at 1135.

Applying that sliding scale approach, the district court granted hiQ a preliminary injunction, concluding that the balance of hardships tips sharply in hiQ's favor and that hiQ raised serious questions on the merits. We review the district court's decision to grant a preliminary injunction for abuse of discretion. The grant of a preliminary injunction constitutes an abuse of discretion if the district court's

evaluation or balancing of the pertinent factors is "illogical, implausible, or without support in the record." *Doe v. Kelly*, 878 F.3d 710, 713 (9th Cir. 2017).

A. Irreparable Harm

We begin with the likelihood of irreparable injury to hiQ if preliminary relief were not granted.

"[M]onetary injury is not normally considered irreparable." *Los Angeles Mem'l Coliseum Comm'n v. Nat'l Football League*, 634 F.2d 1197, 1202 (9th Cir. 1980). Nonetheless, "[t]he threat of being driven out of business is sufficient to establish irreparable harm." *Am. Passage Media Corp. v. Cass Commc'ns, Inc.*, 750 F.2d 1470, 1474 (9th Cir. 1985). As the Second Circuit has explained, "[t]he loss of . . . an ongoing business representing many years of effort and the livelihood of its . . . owners, constitutes irreparable harm. What plaintiff stands to lose cannot be fully compensated by subsequent monetary damages." *Roso Lino Beverage Distributors, Inc. v. Coca Cola Bottling Co. of New York, Inc.*, 749 F.2d 124, 125–26 (2d Cir. 1984) (per curiam). Thus, showing a threat of "extinction" is enough to establish irreparable harm, even when damages may be available and the amount of direct financial harm is ascertainable. *Am. Passage Media Corp.*, 750 F.2d at 1474.

The district court found credible hiQ's assertion that the survival of its business is threatened absent a preliminary injunction. The record provides ample support for that finding.

According to hiQ's CEO, "hiQ's entire business depends on being able to access public LinkedIn member profiles," as "there is no current viable alternative to LinkedIn's member database to obtain data for hiQ's Keeper and Skill

Mapper services." Without access to LinkedIn public profile data, the CEO averred, hiQ will likely be forced to breach its existing contracts with clients such as eBay, Capital One, and GoDaddy, and to pass up pending deals with prospective clients. The harm hiQ faces absent a preliminary injunction is not purely hypothetical. HiQ was in the middle of a financing round when it received LinkedIn's cease-and-desist letter. The CEO reported that, in light of the uncertainty about the future viability of hiQ's business, that financing round stalled, and several employees left the company. If LinkedIn prevails, hiQ's CEO further asserted, hiQ would have to "lay off most if not all its employees, and shutter its operations."

LinkedIn maintains that hiQ's business model does not depend on access to LinkedIn data. It insists that alternatives to LinkedIn data exist, and points in particular to the professional data some users post on Facebook. But hiQ's model depends on access to publicly available data from people who choose to share their information with the world. Facebook data, by contrast, is not generally accessible, *see infra* pp. 37, and therefore is not an equivalent alternative source of data.

LinkedIn also urges that even if there is no adequate alternative database, hiQ could collect its own data through employee surveys. But hiQ is a data analytics company, not a data collection company. Suggesting that hiQ could fundamentally change the nature of its business, not simply the manner in which it conducts its current business, is a recognition that hiQ's current business could not survive without access to LinkedIn public profile data. Creating a data collection system would undoubtedly require a considerable amount of time and expense. That hiQ could feasibly remain in business with no products to sell while

raising the required capital and devising and implementing an entirely new data collection system is at least highly dubious.

In short, the district court did not abuse its discretion in concluding on the preliminary injunction record that hiQ currently has no viable way to remain in business other than using LinkedIn public profile data for its Keeper and Skill Mapper services, and that HiQ therefore has demonstrated a likelihood of irreparable harm absent a preliminary injunction.

B. Balance of the Equities

Next, the district court "balance[d] the interests of all parties and weigh[ed] the damage to each in determining the balance of the equities." *CTIA - The Wireless Ass'n v. City of Berkeley, Calif.*, 928 F.3d 832, 852 (9th Cir. 2019) (internal quotation marks and citation omitted). Again, it did not abuse its discretion in doing so.

On one side of the scale is the harm to hiQ just discussed: the likelihood that, without an injunction, it will go out of business. On the other side, LinkedIn asserts that the injunction threatens its members' privacy and therefore puts at risk the goodwill LinkedIn has developed with its members. As the district court observed, "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." LinkedIn points in particular to the more than 50 million members who have used the "Do Not Broadcast" feature to ensure that other users are not notified when the member makes a profile change. According to LinkedIn, the popularity of the "Do Not Broadcast" feature indicates that many members—including members who choose to share their information publicly—do not want their employers to

know they may be searching for a new job. An employer who learns that an employee may be planning to leave will not necessarily reward that employee with a retention bonus. Instead, the employer could decide to limit the employee's access to sensitive information or even to terminate the employee.

There is support in the record for the district court's connected conclusions that (1) LinkedIn's assertions have some merit; and (2) there are reasons to discount them to some extent. First, there is little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly, and it is doubtful that they do. LinkedIn's privacy policy clearly states that "[a]ny information you put on your profile and any content you post on LinkedIn may be seen by others" and instructs users not to "post or add personal data to your profile that you would not want to be public."

Second, there is no evidence in the record to suggest that most people who select the "Do Not Broadcast" option do so to prevent their employers from being alerted to profile changes made in anticipation of a job search. As the district court stated, there are other reasons why users may choose that option—most notably, many users may simply wish to avoid sending their connections annoying notifications each time there is a profile change. In any event, employers can always directly consult the profiles of users who chose to make their profiles public to see if any recent changes have been made. Employees intent on keeping such information from their employers can do so by rejecting public exposure of their profiles and eliminating their employers as contacts.

Finally, LinkedIn's own actions undercut its argument that users have an expectation of privacy in public profiles.

LinkedIn's "Recruiter" product enables recruiters to "follow" prospects, get "alert[ed] when prospects make changes to their profiles," and "use those [alerts] as signals to reach out at just the right moment," without the prospect's knowledge.[8] And subscribers to LinkedIn's "talent recruiting, marketing and sales solutions" can export data from members' public profiles, such as "name, headline, current company, current title, and location."

In short, even if some users retain some privacy interests in their information notwithstanding their decision to make their profiles public, we cannot, on the record before us, conclude that those interests—or more specifically, LinkedIn's interest in preventing hiQ from scraping those profiles—are significant enough to outweigh hiQ's interest in continuing its business, which depends on accessing, analyzing, and communicating information derived from public LinkedIn profiles.

Nor do the other harms asserted by LinkedIn tip the balance of harms with regard to preliminary relief. LinkedIn invokes an interest in preventing "free riders" from using profiles posted on its platform. But LinkedIn has no protected property interest in the data contributed by its users, as the users retain ownership over their profiles. And as to the publicly available profiles, the users quite evidently intend them to be accessed by others, including for commercial purposes—for example, by employers seeking to hire individuals with certain credentials. Of course, LinkedIn could satisfy its "free rider" concern by eliminating

[8] Recruiter does not provide alerts about profile changes made by LinkedIn members who select the "Do Not Broadcast" setting.

the public access option, albeit at a cost to the preferences of many users and, possibly, to its own bottom line.

We conclude that the district court's determination that the balance of hardships tips sharply in hiQ's favor is not "illogical, implausible, or without support in the record." *Kelly*, 878 F.3d at 713.

C. Likelihood of Success

Because hiQ has established that the balance of hardships tips decidedly in its favor, the likelihood-of-success prong of the preliminary injunction inquiry focuses on whether hiQ has raised "serious questions going to the merits." *Alliance for the Wild Rockies*, 632 F.3d at 1131. It has.

As usual, we consider only the claims and defenses that the parties press on appeal. We recognize that the companies have invoked additional claims and defenses in the district court, and we express no opinion as to whether any of those claims or defenses might ultimately prove meritorious. Thus, while hiQ advanced several affirmative claims in support of its request for preliminary injunctive relief, here we consider only whether hiQ has raised serious questions on the merits of its claims either for intentional interference with contract or unfair competition, under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* Likewise, while LinkedIn has asserted that it has "claims under the Digital Millennium Copyright Act and under trespass and misappropriation doctrines," it has chosen for present purposes to focus on a defense based on the CFAA, so that is the sole defense to hiQ's claims that we address here.

1. Tortious Interference with Contract

HiQ alleges that LinkedIn intentionally interfered with hiQ's contracts with third parties. "The elements which a plaintiff must plead to state the cause of action for intentional interference with contractual relations are (1) a valid contract between plaintiff and a third party; (2) defendant's knowledge of this contract; (3) defendant's intentional acts designed to induce a breach or disruption of the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5) resulting damage." *Pac. Gas & Elec. Co. v. Bear Stearns & Co.*, 50 Cal. 3d 1118, 1126 (1990).[9]

HiQ has shown a sufficient likelihood of establishing each of these elements. First, LinkedIn does not contest hiQ's evidence that contracts exist between hiQ and some customers, including eBay, Capital One, and GoDaddy.

Second, hiQ will likely be able to establish that LinkedIn knew of hiQ's scraping activity and products for some time.

[9] Under California law, tortious interference with contract claims are not limited to circumstances in which the defendant has caused the third party with whom the plaintiff has contracted to breach the agreement. "The most general application of the rule is to cases where the party with whom the plaintiff has entered into an agreement has been induced to breach it, but the rule is also applicable where the plaintiff's performance has been prevented or rendered more expensive or burdensome and where he has been induced to breach the contract by conduct of the defendant, such as threats of economic reprisals." *Lipman v. Brisbane Elementary Sch. Dist.*, 55 Cal. 2d 224, 232 (1961), *abrogated on other grounds by Brown v. Kelly Broad. Co.*, 48 Cal. 3d 711, 753 n.37 (1989); *see also Pac. Gas & Elec. Co.*, 50 Cal. 3d at 1129 ("We have recognized that interference with the plaintiff's performance may give rise to a claim for interference with contractual relations if plaintiff's performance is made more costly or more burdensome.").

LinkedIn began sending representatives to hiQ's Elevate conferences in October 2015. At those conferences, hiQ discussed its business model, including its use of data from external sources to predict employee attrition. LinkedIn's director of business operations and analytics, who attended several Elevate conferences, specifically "recall[s] someone from hiQ stating [at the April 2017 conference] that they collected skills data from public professional profiles in order to provide hiQ's customers information about their employees' skill sets." Additionally, LinkedIn acknowledged in its cease-and-desist letter that "hiQ has stated during marketing presentations that its Skill Mapper product is built on profile data from LinkedIn." Finally, at a minimum, LinkedIn knew of hiQ's contracts as of May 31, 2017, when hiQ responded to LinkedIn's cease-and-desist letter and identified both current and prospective hiQ clients.

Third, LinkedIn's threats to invoke the CFAA and implementation of technical measures selectively to ban hiQ bots could well constitute "intentional acts designed to induce a breach or disruption" of hiQ's contractual relationships with third parties. *Pac. Gas & Elec. Co.*, 50 Cal. 3d at 1126; *cf. Winchester Mystery House, LLC v. Global Asylum, Inc.*, 210 Cal. App. 4th 579, 597 (2012) (indicating that "cease-and-desist letters . . . refer[ring] to a[] contractual or other economic relationship between plaintiff and any third party" could "establish . . . the . . . intent element[] of the interference claim[]").

Fourth, the contractual relationships between hiQ and third parties have been disrupted and "now hang[] in the balance." Without access to LinkedIn data, hiQ will likely be unable to deliver its services to its existing customers as promised.

Last, hiQ is harmed by the disruption to its existing contracts and interference with its pending contracts. Without the revenue from sale of its products, hiQ will likely go out of business. *See supra* pp. 15–17.

LinkedIn does not specifically challenge hiQ's ability to make out any of these elements of a tortious interference claim. Instead, LinkedIn maintains that it has a "legitimate business purpose" defense to any such claim. *Cf. Quelimane Co. v. Stewart Title Guar. Co.*, 19 Cal. 4th 26, 57 (1998), *as modified* (Sept. 23, 1998). That contention is an affirmative justification defense for which LinkedIn bears the burden of proof. *See id.*

Under California law, a legitimate business purpose can indeed justify interference with contract, but not just any such purpose suffices. *See id.* at 55–56. Where a contractual relationship exists, the societal interest in "contractual stability is generally accepted as of greater importance than competitive freedom." *Imperial Ice Co. v. Rossier*, 18 Cal. 2d 33, 36 (1941). Emphasizing the "distinction between claims for the tortious disruption of an existing contract and claims that a prospective contractual or economic relationship has been interfered with by the defendant," the California Supreme Court instructs that we must "bring[] a greater solicitude to those relationships that have ripened into agreements." *Della Penna v. Toyota Motor Sales, U.S.A., Inc.*, 11 Cal. 4th 376, 392 (1995). Thus, interference with an existing contract is not justified simply because a competitor "seeks to further his own economic advantage at the expense of another." *Imperial Ice*, 18 Cal. 2d at 36; *see id.* at 37 ("A party may not . . . under the guise of competition . . . induce the breach of a competitor's contract in order to secure an economic advantage."). Rather, interference with contract is justified only when the party

alleged to have interfered acted "to protect an interest that has greater social value than insuring the stability of the contract" interfered with. *Id.* at 35.

Accordingly, California courts apply a balancing test to determine whether the interests advanced by interference with contract outweigh the societal interest in contractual stability:

> Whether an intentional interference by a third party is justifiable depends upon a balancing of the importance, social and private, of the objective advanced by the interference against the importance of the interest interfered with, considering all circumstances including the nature of the actor's conduct and the relationship between the parties.

Herron v. State Farm Mut. Ins. Co., 56 Cal. 2d 202, 206 (1961). Considerations include whether "the means of interference involve no more than recognized trade practices," *Buxbom v. Smith*, 23 Cal. 2d 535, 546 (1944), and whether the conduct is "within the realm of fair competition," *Inst. of Veterinary Pathology, Inc. v. Cal. Health Labs., Inc.*, 116 Cal. App. 3d 111, 127 (Cal. Ct. App. 1981). The "determinative question" is whether the business interest is pretextual or "asserted in good faith." *Richardson v. La Rancherita*, 98 Cal. App. 3d 73, 81 (Cal. Ct. App. 1979).

Balancing the interest in contractual stability and the specific interests interfered with against the interests advanced by the interference, we agree with the district court that hiQ has at least raised a serious question on the merits of LinkedIn's affirmative justification defense. First, hiQ has a strong commercial interest in fulfilling its contractual

obligations to large clients like eBay and Capital One. Those companies benefit from hiQ's ability to access, aggregate, and analyze data from LinkedIn profiles.

Second, LinkedIn's means of interference is likely not a "recognized trade practice" as California courts have understood that term. "Recognized trade practices" include such activities as "advertising," "price-cutting," and "hir[ing] the employees of another for use in the hirer's business," *Buxbom*, 23 Cal. 2d at 546–47—all practices which may indirectly interfere with a competitor's contracts but do not fundamentally undermine a competitor's basic business model. LinkedIn's proactive technical measures to selectively block hiQ's access to the data on its site are not similar to trade practices previously recognized as acceptable justifications for contract interference.

Further, LinkedIn's conduct may well not be "within the realm of fair competition." *Inst. of Veterinary Pathology*, 116 Cal. App. 3d at 127. HiQ has raised serious questions about whether LinkedIn's actions to ban hiQ's bots were taken in furtherance of LinkedIn's own plans to introduce a competing professional data analytics tool. There is evidence from which it can be inferred that LinkedIn knew about hiQ and its reliance on external data for several years before the present controversy. Its decision to send a cease-and-desist letter occurred within a month of the announcement by LinkedIn's CEO that LinkedIn planned to leverage the data on its platform to create a new product for employers with some similarities to hiQ's Skill Mapper product. If companies like LinkedIn, whose servers hold vast amounts of public data, are permitted selectively to ban only potential competitors from accessing and using that otherwise public data, the result—complete exclusion of the original innovator in aggregating and analyzing the public

information—may well be considered unfair competition under California law.[10]

Finally, LinkedIn's asserted private business interests—"protecting its members' data and the investment made in developing its platform" and "enforcing its User Agreements' prohibitions on automated scraping"—are relatively weak. LinkedIn has only a non-exclusive license to the data shared on its platform, not an ownership interest. Its core business model—providing a platform to share professional information—does not require prohibiting hiQ's use of that information, as evidenced by the fact that hiQ used LinkedIn data for some time before LinkedIn sent its cease-and-desist letter. As to its members' interests in their data, for the reasons already explained, *see supra* pp. 17–20, we agree with the district court that members' privacy expectations regarding information they have shared in their public profiles are "uncertain at best." Further, there is evidence that LinkedIn has itself developed a data analytics tool similar to HiQ's products, undermining LinkedIn's claim that it has its members' privacy interests in mind. Finally, LinkedIn has not explained how it can enforce its user agreement against hiQ now that its user status has been terminated.

For all these reasons, LinkedIn may well not be able to demonstrate a "legitimate business purpose" that could justify the intentional inducement of a contract breach, at

[10] The district court determined that LinkedIn's legitimate business purpose defense overlapped with hiQ's claim under California's Unfair Competition Law ("UCL"), which the district court found raised serious questions on the merits: "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 UCL].'"

least on the record now before us. We therefore conclude that hiQ has raised at least serious questions going to the merits of its tortious interference with contract claim. Because such a showing on the tortious interference claim is sufficient to support an injunction prohibiting LinkedIn from selectively blocking hiQ's access to public member profiles, we do not reach hiQ's unfair competition claim.[11]

2. Computer Fraud and Abuse Act (CFAA)

Our inquiry does not end, however, with the state law tortious interference claim. LinkedIn argues that even if hiQ can show a likelihood of success on any of its state law causes of action, all those causes of action are preempted by the CFAA, 18 U.S.C. § 1030, which LinkedIn asserts that hiQ violated.

The CFAA states that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished" by fine or

[11] LinkedIn also advances a business interest in "asserting its rights under federal and state law." That interest depends upon the scope of LinkedIn's rights under the CFAA and California's CFAA analogue, California Penal Code § 502. Similarly, LinkedIn argues that there can be no tortious interference because hiQ's contracts are premised on unauthorized access to LinkedIn data and are therefore illegal. Under California law, "[i]f the central purpose of the contract is tainted with illegality, then the contract as a whole cannot be enforced." *Marathon Ent., Inc. v. Blasi*, 42 Cal. 4th 974, 996 (2008), *as modified* (Mar. 12, 2008); *see also* Cal. Civ. Code § 1598 ("Where a contract has but a single object, and such object is unlawful, whether in whole or in part, or wholly impossible of performance . . . the entire contract is void."). As we explain next, however, hiQ has raised at least serious questions in support of its position that its activities are lawful under the CFAA.

imprisonment. 18 U.S.C. § 1030(a)(2)(C).[12] The term "protected computer" refers to any computer "used in or affecting interstate or foreign commerce or communication," 18 U.S.C. § 1030(e)(2)(B)—effectively any computer connected to the Internet, *see United States v. Nosal (Nosal II)*, 844 F.3d 1024, 1050 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 314 (2017)—including servers, computers that manage network resources and provide data to other computers. LinkedIn's computer servers store the data members share on LinkedIn's platform and provide that data to users who request to visit its website. Thus, to scrape LinkedIn data, hiQ must access LinkedIn servers, which are "protected computer[s]." *See Nosal II*, 844 F.3d at 1050.

The pivotal CFAA question here is whether once hiQ received LinkedIn's cease-and-desist letter, any further scraping and use of LinkedIn's data was "without authorization" within the meaning of the CFAA and thus a violation of the statute. 18 U.S.C. § 1030(a)(2). If so, LinkedIn maintains, hiQ could have no legal right of access to LinkedIn's data and so could not succeed on any of its state law claims, including the tortious interference with

[12] Additionally, "[a]ny person who suffers damage or loss by reason of a violation" of that provision may bring a civil suit "against the violator to obtain compensatory damages and injunctive relief or other equitable relief," subject to certain conditions. 18 U.S.C. § 1030(g). *Van Buren* reviewed the statutory definitions of "damage" and "loss" and concluded that this civil remedies provision requires a showing of "technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data." 141 S. Ct. at 1659–60 (interpreting 18 U.S.C. § 1030(e)(8), (e)(11), (g)). LinkedIn has not alleged that hiQ's scraping of public profiles caused any such technological harms.

contract claim we have held otherwise sufficient for preliminary injunction purposes.

We have held in another context that the phrase "'without authorization' is a non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."[13] *Nosal II*, 844 F.3d at 1028. *Nosal II* involved an employee accessing without permission an employer's private computer for which access permissions in the form of user accounts were required. *Id.* at 1028–29. *Nosal II* did not address whether access can be "without authorization" under the CFAA where, as here, prior authorization is not generally required, but a particular person—or bot—is refused access. HiQ's position is that *Nosal II* is consistent with the conclusion that where access is open to the general public, the CFAA "without authorization" concept is inapplicable. At the very least, we conclude, hiQ has raised a serious question as to this issue.

First, the wording of the statute, forbidding "access[] . . . without authorization," 18 U.S.C. § 1030(a)(2), suggests a baseline in which access is not generally available and so permission is ordinarily required. "Authorization" is an affirmative notion, indicating that access is restricted to those specially recognized or admitted. *See, e.g.*, Black's Law Dictionary (11th ed. 2019) (defining "authorization" as

[13] *Van Buren* observed that "[w]hen interpreting statutes, courts take note of terms that carry 'technical meaning[s],'" 141 S. Ct. at 1657 (quoting A. Scalia & B. Garner, *Reading Law: The Interpretation of Legal Texts* 73 (2012)), and stated that "'[a]ccess' is one such term," which, in the "computing context, . . . references the act of entering a computer 'system itself' or a particular 'part of a computer system,' such as files, folders, or databases," *id.* Although we rely on the plain meaning of "without authorization," we apply the specialized meaning of "access" in interpreting the CFAA.

"[o]fficial permission to do something; sanction or warrant"). Where the default is free access without authorization, in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of "authorization." *Cf. Blankenhorn v. City of Orange*, 485 F.3d 463, 472 (9th Cir. 2007) (characterizing the exclusion of the plaintiff in particular from a shopping mall as "bann[ing]").

Second, even if this interpretation is debatable, the legislative history of the statute confirms our understanding. "If [a] statute's terms are ambiguous, we may use . . . legislative history[] and the statute's overall purpose to illuminate Congress's intent." *Jonah R. v. Carmona*, 446 F.3d 1000, 1005 (9th Cir. 2006).

The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking. *See United States v. Nosal (Nosal I)*, 676 F.3d 854, 858 (9th Cir. 2012) (citing S. Rep. No. 99-432, at 9 (1986) (Conf. Rep.)).

The 1984 House Report on the CFAA explicitly analogized the conduct prohibited by section 1030 to forced entry: "It is noteworthy that section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' . . . .'" H.R. Rep. No. 98-894, at 20 (1984); *see also id.* at 10 (describing the problem of "'hackers' who have been able to access (trespass into) both private and public computer systems"). Senator Jeremiah Denton similarly characterized the CFAA as a statute designed to prevent unlawful intrusion into otherwise inaccessible computers, observing that "[t]he bill makes it clear that unauthorized access to a Government computer is a trespass offense, as surely as if the offender

had entered a restricted Government compound without proper authorization."[14] 132 Cong. Rec. 27639 (1986) (emphasis added). And when considering amendments to the CFAA two years later, the House again linked computer intrusion to breaking and entering. *See* H.R. Rep. No. 99-612, at 5–6 (1986) (describing "the expanding group of electronic trespassers," who trespass "just as much as if they broke a window and crawled into a home while the occupants were away").

In recognizing that the CFAA is best understood as an anti-intrusion statute and not as a "misappropriation statute," *Nosal I*, 676 F.3d at 857–58, we rejected the contract-based interpretation of the CFAA's "without authorization" provision adopted by some of our sister circuits. *Compare Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 313 (2017) ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA."); *Nosal I*, 676 F.3d at 862 ("We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty."), *with EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583–84 (1st Cir. 2001) (holding that violations of a confidentiality agreement or other contractual restraints could give rise to a claim for unauthorized access under the CFAA); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that a defendant "exceeds authorized access" when violating policies governing authorized use of databases). *Van Buren*, interpreting the CFAA's "exceeds authorized access" clause,

[14] The CFAA originally prohibited only unauthorized access to government computers.

approved of *Nosal I* and abrogated *EF Cultural Travel* and *Rodriguez*. 141 S. Ct. at 1653–54 & n.2.

We therefore look to whether the conduct at issue is analogous to "breaking and entering." H.R. Rep. No. 98-894, at 20. Significantly, the version of the CFAA initially enacted in 1984 was limited to a narrow range of computers—namely, those containing national security information or financial data and those operated by or on behalf of the government. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102, 98 Stat. 2190, 2190–91. None of the computers to which the CFAA initially applied were accessible to the general public; affirmative authorization of some kind was presumptively required.

When section 1030(a)(2)(C) was added in 1996 to extend the prohibition on unauthorized access to any "protected computer," the Senate Judiciary Committee explained that the amendment was designed "to increase protection for the privacy and confidentiality of computer information." S. Rep. No. 104-357, at 7 (emphasis added).[15] The

[15] At the same time, Congress added the word "nonpublic" to section 1030(a)(3), the section prohibiting unauthorized access of "any nonpublic computer" belonging to the United States government. LinkedIn maintains that Congress's decision not to include the word "nonpublic" in section 1030(a)(2)(C) confirms that that section's prohibition on unauthorized access applies to public websites. We disagree. The Senate Judiciary Committee explained that the "nonpublic" modifier was meant to increase protection for government computers by making clear that "a person who is permitted to access publicly available Government computers, for example, via an agency's World Wide Web site, may still be convicted under (a)(3) for accessing without authority any nonpublic Federal Government computer." S. Rep. No. 104-357, at 9. Congress's concern about protecting government computers, even though some government computers may be "publicly

legislative history of section 1030 thus makes clear that the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort. As one prominent commentator has put it, "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." Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1161 (2016). Moreover, elsewhere in the statute, password fraud is cited as a means by which a computer may be accessed without authorization, *see* 18 U.S.C. § 1030(a)(6),[16] bolstering the idea that authorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information.

We therefore conclude that hiQ has raised a serious question as to whether the reference to access "without authorization" limits the scope of the statutory coverage to computers for which authorization or access permission, such as password authentication, is generally required. Put differently, the CFAA contemplates the existence of three kinds of computer systems: (1) computers for which access is open to the general public and permission is not required,

---

available," *id.*, does not imply that Congress also intended the prohibition of unauthorized access to privately owned protected computers to extend to the publicly available websites on such computers.

[16] 18 U.S.C. § 1030(a)(6) provides: "Whoever . . . knowingly and with intent to defraud traffics . . . in any password or similar information through which a computer may be accessed without authorization, if—(A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States; . . . shall be punished as provided in subsection (c) of this section."

(2) computers for which authorization is required and has been given, and (3) computers for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed). Public LinkedIn profiles, available to anyone with an Internet connection, fall into the first category. With regard to websites made freely accessible on the Internet, the "breaking and entering" analogue invoked so frequently during congressional consideration has no application, and the concept of "without authorization" is inapt.

The reasoning of *Van Buren* reinforces our interpretation of the CFAA, although it did not directly address the statute's "without authorization" clause. *Van Buren* held that a police sergeant did not violate the CFAA when he "ran a license-plate search in a law enforcement computer database in exchange for money." 141 S. Ct. at 1652. Interpreting the "exceeds authorized access" clause of section 1030(a)(2), the Court held that the CFAA "covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them." *Id.*

Van Buren found the "interplay between the 'without authorization' and 'exceeds authorized access' clauses of subsection (a)(2) . . . particularly probative." *Id.* at 1658. "The 'without authorization' clause . . . protects computers themselves by targeting so-called outside hackers—those who 'acces[s] a computer without any permission at all.'" *Id.* (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)). The "'exceeds authorized access' clause . . . provide[s] complementary protection for certain

information within computers . . . by targeting so-called inside hackers—those who access a computer with permission, but then '"exceed" the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend.'" *Id.* (quoting *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015)). "[L]iability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Id.* at 1658–59.

Van Buren's "gates-up-or-down inquiry" is consistent with our interpretation of the CFAA as contemplating three categories of computer systems. *See supra* p. 33–34. Discussing the "without authorization" clause, *Van Buren* explained that a computer user who has "authorization" is one who "can . . . access a computer system," 141 S. Ct. at 1658, where "access" means "the act of entering a computer 'system itself,'" *id.* at 1657 (citation omitted). In other words, a user with "authorization" is not subject to "limitations on access," whether those limitations are "code-based" or "contained in contracts or policies." *Id.* at 1659 n.8. *Van Buren* stated that the CFAA's password-trafficking provision, section 1030(a)(6), which also uses the word "authorization," "contemplates a 'specific type of authorization—that is, authentication,' which turns on whether a user's credentials allow him to proceed past a computer's access gate, rather than on other, scope-based restrictions." *Id.* at 1659 n.9 (quoting Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 Geo. Wash. L. Rev. 1442, 1470 (2016)).

Van Buren's distinction between computer users who "can or cannot access a computer system," *id.* at 1658,

suggests a baseline in which there are "limitations on access" that prevent some users from accessing the system (i.e., a "gate" exists, and can be either up or down). The Court's "gates-up-or-down inquiry" thus applies to the latter two categories of computers we have identified: if authorization is required and has been given, the gates are up; if authorization is required and has *not* been given, the gates are down. As we have noted, however, a defining feature of public websites is that their publicly available sections lack limitations on access; instead, those sections are open to anyone with a web browser. In other words, applying the "gates" analogy to a computer hosting publicly available webpages, that computer has erected no gates to lift or lower in the first place.[17] *Van Buren* therefore reinforces our conclusion that the concept of "without authorization" does not apply to public websites.

Additionally, neither of the cases LinkedIn principally relies upon casts doubt on our interpretation of the statute. LinkedIn first cites *Nosal II*, 844 F.3d 1024. As we have already stated, *Nosal II* held that a former employee who used current employees' login credentials to access company computers and collect confidential information had acted "'without authorization' in violation of the CFAA." 844 F.3d at 1038. The computer information the defendant accessed in *Nosal II* was thus plainly one which no one could access without authorization.

So too with regard to the system at issue in *Power Ventures*, 844 F.3d 1058, the other precedent upon which

[17] Of course, even computers and servers hosting public websites may contain areas that require authorization to access. Accessing those areas "without authorization" would violate the CFAA. 18 U.S.C. § 1030(a)(2)(C).

LinkedIn relies. In that case, Facebook sued Power Ventures, a social networking website that aggregated social networking information from multiple platforms, for accessing Facebook users' data and using that data to send mass messages as part of a promotional campaign. *Id.* at 1062–63. After Facebook sent a cease-and-desist letter, Power Ventures continued to circumvent IP barriers and gain access to password-protected Facebook member profiles. *Id.* at 1063. We held that after receiving an individualized cease-and-desist letter, Power Ventures had accessed Facebook computers "without authorization" and was therefore liable under the CFAA. *Id.* at 1067–68. But we specifically recognized that "Facebook has tried to limit and control access to its website" as to the purposes for which Power Ventures sought to use it. *Id.* at 1063. Indeed, Facebook requires its users to register with a unique username and password, and Power Ventures required that Facebook users provide their Facebook username and password to access their Facebook data on Power Ventures' platform. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1028 (N.D. Cal. 2012). While Power Ventures was gathering user data that was protected by Facebook's username and password authentication system, the data hiQ was scraping was available to anyone with a web browser.

In sum, *Nosal II* and *Power Ventures* control situations in which authorization generally is required and has either never been given or has been revoked. As *Power Ventures* indicated, the two cases do not control the situation present here, in which information is "presumptively open to all comers." *Power Ventures*, 844 F.3d at 1067 n.2. As to the computers at issue in those cases, the authorization gate was "down."

Our understanding that the CFAA is premised on a distinction between information presumptively accessible to the general public and information for which authorization is generally required is consistent with our interpretation of a provision of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*,[18] nearly identical to the CFAA provision at issue. *Compare* 18 U.S.C. § 2701(a) ("[W]hoever—(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . unauthorized access to a wire or electronic communication . . . shall be punished . . . .") *with* 18 U.S.C. § 1030(a)(2)(C) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished . . . ."). "The similarity of language in [the SCA and the CFAA] is a strong indication that [they] should be interpreted *pari passu*." *Northcross v. Bd. of Educ. of Memphis City Schs.*, 412 U.S. 427, 428 (1973); *see also United States v. Sioux*, 362 F.3d 1241, 1246 (9th Cir. 2004).

Addressing the "without authorization" provision of the SCA, we have distinguished between public websites and non-public or "restricted" websites, such as websites that "are password-protected . . . or require the user to purchase access by entering a credit card number." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002);

[18] The Stored Communications Act, enacted as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, provides privacy protections for e-mail and other electronic communications by limiting the ability of the government to compel disclosure by internet service providers.

see also id. at 879 n.8. As we explained in *Konop*, in enacting the SCA, "Congress wanted to protect electronic communications that are configured to be private" and are "'not intended to be available to the public.'" *Id.* at 875 (quoting S. Rep. No. 99-541, at 35–36 (1986)). The House Committee on the Judiciary stated, with respect to the section of the SCA at issue, section 2701, that "[a] person may reasonably conclude that a communication is readily accessible to the general public if the . . . means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy." H.R. Rep. No. 99-647, at 62 (1986). The Committee further explained that "electronic communications which the service provider attempts to keep confidential would be protected, while the statute would impose no liability for access to features configured to be readily accessible to the general public." *Id.* at 63.

Both the legislative history of section 1030 of the CFAA and the legislative history of section 2701 of the SCA, with its similar "without authorization" provision, then, support the district court's distinction between "private" computer networks and websites, protected by a password authentication system and "not visible to the public," and websites that are accessible to the general public.

Finally, the rule of lenity favors our narrow interpretation of the "without authorization" provision in the CFAA. The statutory prohibition on unauthorized access applies both to civil actions and to criminal prosecutions—indeed, "§ 1030 is primarily a criminal statute." *LVRC Holdings*, 581 F.3d at 1134. "Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies."

Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004). As we explained in *Nosal I*, we therefore favor a narrow interpretation of the CFAA's "without authorization" provision so as not to turn a criminal hacking statute into a "sweeping Internet-policing mandate." 676 F.3d at 858; *see also id.* at 863.[19]

For all these reasons, it appears that the CFAA's prohibition on accessing a computer "without authorization" is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer. It is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA. The data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using such an authorization system. HiQ has therefore raised serious questions about whether LinkedIn may invoke the CFAA to preempt hiQ's possibly meritorious tortious interference claim.[20]

---

[19] *Van Buren* identified similar concerns, stating that "[i]f the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals." 141 S. Ct. at 1661.

[20] LinkedIn asserts that the illegality of hiQ's actions under the CFAA is also grounds for holding (1) that hiQ's injuries are not cognizable as irreparable harm, (2) that hiQ's contracts are illegal and so their breach cannot give rise to a cognizable tortious interference with contract claim, and (3) that LinkedIn has a legitimate business interest in asserting its rights under federal law that justifies its interference with hiQ's contracts. *See supra* n.11. These contentions are insufficient at this stage for the same reasons LinkedIn's CFAA preemption position does not preclude preliminary injunctive relief.

Entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply: state law trespass to chattels claims may still be available.[21] And other causes of action, such as copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy, may also lie. *See, e.g.*, *Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 561 (S.D.N.Y. 2013) (holding that a software

[21] LinkedIn's cease-and-desist letter also asserted a state common law claim of trespass to chattels. Although we do not decide the question, *see supra* p. 20, it may be that web scraping exceeding the scope of the website owner's consent gives rise to a common law tort claim for trespass to chattels, at least when it causes demonstrable harm. *Compare eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) (finding that eBay had established a likelihood of success on its trespass claim against the auction-aggregating site Bidder's Edge because, although eBay's "site is publicly accessible," "eBay's servers are private property, conditional access to which eBay grants the public," and Bidder's Edge had exceeded the scope of any consent, even if it did not cause physical harm); *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 437–38 (2d Cir. 2004) (holding that a company that scraped a competitor's website to obtain data for marketing purposes likely committed trespass to chattels, because scraping could—although it did not yet—cause physical harm to the plaintiff's computer servers); *Sw. Airlines Co. v. FareChase, Inc.*, 318 F. Supp. 2d 435, 442 (N.D. Tex. 2004) (holding that the use of a scraper to glean flight information was unauthorized as it interfered with Southwest's use and possession of its site, even if the scraping did not cause physical harm or deprivation), *with Ticketmaster Corp. v. Tickets.Com, Inc.*, No. 2:99-cv-07654-HLH-VBK, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003) (holding that the use of a web crawler to gather information from a public website, without more, is insufficient to fulfill the harm requirement of a trespass action); *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1364 (2003) (holding that "trespass to chattels is not actionable if it does not involve actual or threatened injury" to property and the defendant's actions did not damage or interfere with the operation of the computer systems at issue).

company's conduct in scraping and aggregating copyrighted news articles was not protected by fair use).

D. Public Interest

Finally, we must consider the public interest in granting or denying the preliminary injunction. Whereas the balance of equities focuses on the parties, "[t]he public interest inquiry primarily addresses impact on non-parties rather than parties," and takes into consideration "the public consequences in employing the extraordinary remedy of injunction." *Bernhardt v. Los Angeles Cnty.*, 339 F.3d 920, 931–32 (9th Cir. 2003) (citations omitted).

As the district court observed, each side asserts that its own position would benefit the public interest by maximizing the free flow of information on the Internet. HiQ points out that data scraping is a common method of gathering information, used by search engines, academic researchers, and many others. According to hiQ, letting established entities that already have accumulated large user data sets decide who can scrape that data from otherwise public websites gives those entities outsized control over how such data may be put to use.

For its part, LinkedIn argues that the preliminary injunction is against the public interest because it will invite malicious actors to access LinkedIn's computers and attack its servers. As a result, the argument goes, LinkedIn and other companies with public websites will be forced to choose between leaving their servers open to such attacks or protecting their websites with passwords, thereby cutting them off from public view.

Although there are significant public interests on both sides, the district court properly determined that, on balance,

the public interest favors hiQ's position. We agree with the district court that giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest.

Internet companies and the public do have a substantial interest in thwarting denial-of-service attacks[22] and blocking abusive users, identity thieves, and other ill-intentioned actors. But we do not view the district court's injunction as opening the door to such malicious activity. The district court made clear that the injunction does not preclude LinkedIn from continuing to engage in "technological self-help" against bad actors—for example, by employing "anti-bot measures to prevent, *e.g.*, harmful intrusions or attacks on its server." Although an injunction preventing a company from securing even the public parts of its website from malicious actors would raise serious concerns, such concerns are not present here.[23]

The district court's conclusion that the public interest favors granting the preliminary injunction was appropriate.

[22] In a denial-of-service (DoS) attack, an attacker seeks to prevent legitimate users from accessing a targeted computer or network, typically by flooding the target with requests and thereby overloading the server.

[23] We note that LinkedIn has not specifically challenged the scope of the injunction.

CONCLUSION

We **AFFIRM** the district court's determination that hiQ has established the elements required for a preliminary injunction and remand for further proceedings.