Berzon, Circuit Judge:

May LinkedIn, the professional networking website, prevent a competitor, hiQ, from collecting and using information that LinkedIn users have shared on their public profiles, available for viewing by anyone with a web browser? …

I.

Founded in 2002, LinkedIn is a professional networking website with over 500 million members. 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. This case deals only with profiles made visible to the general public. …

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 LinkedIn for bot access. LinkedIn also employs several technological systems to detect suspicious activity and restrict automated scraping. 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; and its 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,[5] 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.

---

5 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.

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

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 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 suit, seeking injunctive relief ...

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. ...

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. [The court held that hiQ had established irreparable harm and that balanced of equities tipped in its favor because the "survival of its business is threatened absent a preliminary injunction."]

C. Likelihood of Success ...

2. Computer Fraud and Abuse Act (CFAA) ...

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. ...

HiQ's position is that *Nosal II* [844 F.3d 1024 (2016)] 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 (10th ed. 2014) (defining "authorization" as "[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. ...

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). ...

We therefore look to whether the conduct at issue is analogous to "breaking and entering." 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. 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 "to increase protection for the privacy and confidentiality of computer information." S. Rep. No. 104-357, at 7. The 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). ...

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 computer information 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 information: (1) information for which access is open to the general public and permission is not required, (2) information for which authorization is required and has been given, and (3) information 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 such information, the "breaking and entering" analogue invoked so frequently during congressional consideration has no application, and the concept of "without authorization" is inapt.

Neither of the cases LinkedIn principally relies upon is to the contrary. LinkedIn first cites *Nosal II.* 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." 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 (9th Cir. 2016), the other precedent upon which 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. After Facebook sent a cease-and-desist letter, Power Ventures continued to circumvent IP barriers and gain access to password-protected Facebook member profiles. 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. 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. 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. ...

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. ...

We note that 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.[15] 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 com-

---

15 LinkedIn's cease-and-desist letter also asserted a state common law claim of trespass to chattels. Although we do not decide the question, 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, 1 Cal. Rptr. 3d 32, 71 P.3d 296 (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).

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

D. Public Interest ...

[E]ach 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 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.

Conclusion

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