No. 17-16783

In the United States Court of Appeals for the Ninth Circuit

HIQ LABS, INC., APPELLEE

v.

LINKEDIN CORPORATION, APPELLANT

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA (NO. 17-CV-03301)
(THE HONORABLE EDWARD M. CHEN, J.)

BRIEF OF *AMICUS CURIAE* COSTAR GROUP, INC., IN SUPPORT OF APPELLANT AND REVERSAL

NICHOLAS J. BOYLE
JOHN S. WILLIAMS
ERIC J. HAMILTON
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
(202) 434-5000
nboyle@wc.com

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, counsel for *amicus curiae* certifies that CoStar Group, Inc., has no parent corporation, and no publicly held corporation owns 10 percent or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND RULE

Page

Statutes and Rule—continued:

MISCELLANEOUS

Page

Miscellaneous—continued:

INTEREST OF *AMICUS CURIAE*

CoStar Group, Inc. ("CoStar"), provides information to over 37 million unique visitors every month.[1] These users include subscribers to CoStar's online services offering commercial real estate information and analytics, and visitors to CoStar's online real estate marketplaces. To provide information and analytics, CoStar conducts expansive, ongoing research to produce and maintain a proprietary database that is the largest and most comprehensive database of commercial real estate information in the United States. The database contains data generated, and original photographs taken, by professional CoStar researchers, as well as information identified and curated through proactive research. This information serves not only as the basis for CoStar's online information products; it also flows into CoStar's commercial real estate marketplaces, including LoopNet (www.loopnet.com). In addition to its commercial real estate products and marketplaces, CoStar also operates leading apartment marketplaces, including Apartments.com, among other websites.

[1] In connection with Rule 29 of the Federal Rules of Appellate Procedure, both parties have consented to CoStar filing this brief as an *amicus curiae*. CoStar affirms that no counsel for a party authored this brief in whole or in part and that no person other than *amicus curiae* or its counsel has made any monetary contributions intended to fund the preparation or submission of this brief.

Among CoStar's millions of online users are 200,000 commercial real estate information subscribers, which include state, local, and federal government agencies; major financial institutions; real estate investment trusts; all 100 of the top commercial brokerage firms; and hundreds of smaller commercial brokerages. Facilitated by CoStar's database of information, users engage in one trillion dollars' worth of transactions every year.

One of the significant value propositions that CoStar is able to offer brokerages is the ability to populate their listings automatically on LoopNet with proprietary data and copyrighted images from the CoStar subscription database. This provides the broker with a better user experience by streamlining the listing submission process; and it provides the end-consumer, *e.g.*, the real estate purchaser or renter, with a richer information set. Both broker and end user benefit from the arrangement. And CoStar is able to make that database content available on LoopNet, its marketplace website, because the Computer Fraud and Abuse Act ("CFAA") (and other laws, such as the Copyright Act) protects CoStar's database content from competitor free-riding. In addition to its legal remedies, CoStar relies on technological barriers, such as IP blocks, to fight database thieves who knowingly violate the terms of use for CoStar's websites or ignore cease-and-desist letters.

In the decision below, the district court held the CFAA did not protect LinkedIn's public-facing, user-generated content and barred LinkedIn from

using technological barriers to block the misappropriation of its database. Such reasoning, if extended to cover the proprietary and curated content that composes CoStar's databases, would weaken essential protections for businesses like CoStar that make proprietary information and copyrighted content available on the Internet. Accordingly, CoStar has a substantial interest in LinkedIn's appeal.

SUMMARY OF ARGUMENT

The district court's ruling undermines protections that innovators have depended on to build and protect some of the most useful online resources in the world. Here, the affected innovator is LinkedIn, which has built the largest online database of professional information on Earth by encouraging and facilitating 500 million individual users' sharing of data about their careers and lives. 1ER-2.

hiQ acquired massive quantities of LinkedIn's database without the permission of LinkedIn so that it can sell analyses of stolen LinkedIn content. *Id.* To accomplish this unauthorized download of the LinkedIn database, hiQ employed a sophisticated computer technique called scraping that uses automated "bots" to bombard a target's website servers with information requests at speeds that human website users could never achieve. 1ER-3. Scraping is a preferred tool among data thieves, and it is prohibited by LinkedIn. *Id.* After discovering hiQ's misappropriation of the LinkedIn database and violation

of the rules for use of LinkedIn, LinkedIn contacted hiQ to ask it to cease and desist and used a technological barrier, called an IP block, to close its website to the automated hiQ bots. *Id.*

In this litigation, hiQ claims entitlement to free-ride on LinkedIn's 15-year effort to build its database because LinkedIn makes much of its database generally available to the public, subject to any user's agreement, *inter alia*, not to scrape LinkedIn's data. *Id.* The district court agreed with hiQ, granting a preliminary injunction that held the CFAA's prohibition against unauthorized access did not apply to the portions of LinkedIn's website that do not require a password to access. *See* 1ER-8-17. Next, relying on California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*, the district court ordered LinkedIn to open its website to hiQ's bot traffic because of LinkedIn's competitive advantage in professional data analytics. *See* 1ER-21-23.

As LinkedIn explains in its brief, the district court's decision is deeply flawed. CoStar submits this brief to underscore the dangers created by the district court's reasoning for companies that, like LinkedIn and CoStar, have invested tremendous resources to create and aggregate information for the benefit of users and consumers. If affirmed, the district court's decision would worsen online information access. It is in the interest of neither end-user consumers nor providers of information, like CoStar, for a company's ability to share this information with the general public to be threatened.

Worse yet, the district court's decision threatens to stunt technological progress. The district court has imposed an authentication requirement—*i.e.*, a password gate—into the CFAA. Without the perverse incentives created by rulings like the district court's, password walls would soon become obsolete, because "active authentication" will run in the background of our devices. In other words, while the district court dismissed the CFAA as an antiquated statute written for another era, it is the district court's reasoning that encourages information providers to use antiquated means to protect their data.

Lastly, the district court's injunction against LinkedIn's efforts to protect itself from hiQ's scraper bots turns competition law on its head. Antitrust rules are not intended to encourage free-riding. In forcing LinkedIn to open its website to hiQ's theft, the district court has obligated a company to share valuable infrastructure with a competitor despite that competitor's access to alternatives to compete in the market.

CoStar respectfully urges this Court to vacate the district court's order.

ARGUMENT

I. MANY VALUABLE PUBLIC DATABASES ARE CREATED AT GREAT EFFORT AND EXPENSE AND REQUIRE PROTECTION

The Internet is the greatest disseminator of information in human history. The amount, and variety, of information that is now available to anyone whenever he or she opens a browser window is staggering. *See Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 849-53 (1997). Much of that information, however, is available only because innovators have incentives to present it in the most user-friendly manner possible. And much of that information is further only available because innovators have gone out into the world and created, collated, and synthesized data so that it is useable and useful to consumers. CoStar hopes that some background regarding the lengths to which it goes to create and provide information to its users illustrates to the Court the risks inherent in allowing other firms to scrape a company's collected information and repackage it for commercial gain.

A. CoStar's Database Is The Result Of Information Created And Curated By Professional CoStar Researchers

Like many information providers, CoStar built its database through the efforts of thousands of professional researchers who created or curated the information CoStar shares with the public. Even as to information CoStar receives directly from users, CoStar researchers sort, organize, and verify the information.

To do this, CoStar's research force scours the country—on the phone, by foot, and even by plane—to populate and refresh the CoStar database. On any given day, hundreds of CoStar researchers place 10,000 phone calls to brokers, owners, developers, and other commercial real estate professionals. In addition to the 700 employees at its research headquarters in Virginia and hundreds more in research centers in California, Georgia, Maryland, and the District of Columbia, CoStar conducts nationwide field research, utilizing 200 research vehicles that drive city, suburban, and rural streets to collect information on commercial real estate, including logging for-lease and for-sale availabilities, performing physical inspections of properties, and locating land available for development. In one year, for example, CoStar professional researchers canvass 500,000 properties and take one million photographs. The efforts of CoStar's researchers yield 5.1 million data updates every day.

That commitment to providing its users with comprehensive data caused CoStar in 2015 to form an aerial research unit, which flies a specially-equipped research airplane for about 50 hours every week over real estate markets in the United States. Since its inception, the CoStar aerial unit has logged 290,000 miles—enough to fly to the Moon—and has visited 224 markets (some repeatedly). In so doing, the unit has captured data and images on 500 million square feet of construction projects and added 5,000 new construction projects to the CoStar database.

B. The Entire Real Estate Market Benefits From The Database CoStar Has Created

Before CoStar's founder, Andrew Florance, set out to create one, there was no centralized database of commercial real estate information. Instead, commercial real estate brokers depended on large office guide directories. Agents faxed listings to publishing companies that issued guides on a quarterly basis. These guides had incomplete and inevitably dated information. And, because they were paper directories, they were inefficient, with no way to sort or focus the results a broker would be able to find.

Today, by contrast, CoStar researchers centralize listing information, photographs, and more in a searchable database. They also continuously monitor commercial real estate properties to ensure the accuracy of information regarding the listings in the database. And, because CoStar has followed a business model of making proprietary data and copyrighted images from its proprietary database available to the public within LoopNet, when they are automatically populated into broker listings, this information is available to buyers and sellers (or lessees and lessors) simultaneously. No login or password is required to browse this proprietary and copyrighted CoStar content within LoopNet. This removal of informational asymmetries has benefited all participants in the market and reduced wasted time and effort in researching commercial real estate.

Nor are the benefits from CoStar's investment in its research limited to the commercial real estate marketplace. CoStar has paid millions of dollars in salaries to its researchers. When, for example, CoStar announced its decision to build its research headquarters in Richmond, Virginia, the Governor of Virginia forecasted a $250 million total economic impact for the state and called it "a transformational project" and "huge milestone for Richmond." "Governor McAuliffe Announces 732 New Jobs and $8 Million Investment in City of Richmond," Office of the Virginia Governor (Oct. 24, 2016), *available at* goo.gl/THDS5k.[2] Accordingly, both the actors in the commercial real estate market, and the economy more broadly, benefit from CoStar's investment in its database.

C. CoStar's Ability To Protect Its Content Enables It To Make Its Database Available To The Public

The benefits to the commercial real estate market and the United States economy resulting from CoStar's choice to make its proprietary database publicly available are premised on CoStar's ability to protect its database from theft. The Copyright Act protects the photographs taken by CoStar researchers, who visit over 100,000 buildings, construction sites, and plots of vacant

[2] CoStar's growth has drawn national attention and earned it recognition including as one of *Forbes*'s Most Innovative Growth Companies and as one of *Fortune* Magazine's Top 100 Fastest Growing Companies.

land every year and professionally photograph what they see. But the professional photographs registered by CoStar with the U.S. Copyright Office are just one of several types of proprietary information created by CoStar's researchers.

If other companies could copy and use the other information found on CoStar's websites, CoStar would have much less incentive to create or collate the information. That information is the result of extensive work done by CoStar researchers, including approximately 10,000 phone calls made every day.

For these reasons, providers of commercial real estate information seek to prevent others from copying and utilizing the information contained on their databases. As the Chief Executive Officer of one of CoStar's competitors, Xceligent, Inc. ("Xceligent"), put it: "We don't want people downloading our aggregate data set we've spent over $100 million building and sending it off." Jennifer LeClaire, "Xceligent Demonstrates The Power of Big Data at CCIM Thrive," *GlobeSt.com* (Oct. 31, 2016), *available at* goo.gl/C7rVBj. Such practices harm the company in question as well as "the industry."[3] Accordingly, the terms of use for CoStar and its competitors reflect these accepted rules:

[3] Xceligent does not always practice what its CEO preaches, unfortunately. Last year, CoStar's anti-piracy staff traced ongoing, massive data theft to Xceligent agents in Southeast Asia. After Xceligent bypassed CoStar's technological blocks, CoStar filed suit against Xceligent in the U.S. District Court for the Western District of Missouri. The case is pending. *See CoStar Group, Inc. v. Xceligent, Inc.*, No. 4:16-cv-01288-FJG (W.D. Mo.).

- CoStar: "You shall not use the LoopNet Service as part of any effort to compete with LoopNet . . . . You shall not use any robot, spider or other automated process to . . . data mine or copy LoopNet products, services or information." *See* Terms & Conditions, LoopNet, *available at* goo.gl/B3DmmU.

- Xceligent: "You agree that you shall not . . . use CommercialSearch as part of any effort by you or any third party to directly or indirectly compete with CommercialSearch or Xceligent . . . ; use spiders, robots, or other automated services to monitor, data mine or copy CommercialSearch products, services or information." *See* Terms of Use, CommercialSearch, *available at* goo.gl/3eJLMu.

- RealMassive: "We own our intellectual property. You may not use our intellectual property unless we give you permission. . . . Except as stated herein, none of the Content may be reproduced, distributed, published, displayed, downloaded, or transmitted." *See* Terms of Use, RealMassive, *available at* goo.gl/SVmbPN.

These terms of use enable CoStar and its competitors to deliver valuable information to the public and, indeed, to generate that information to begin with. Almost without exception, the competitors or would-be competitors caught stealing CoStar's content have sufficient sophistication to understand their conduct violates the rules that apply to websites run by CoStar and its peers. What doubt exists is removed by "access denied" messages triggered by security software, other technological barriers, or cease-and-desist letters.

For CoStar and other generators/providers of information, the CFAA gives federal law support to their pro-consumer choice to make data publicly

available. The unauthorized-access remedy allows CoStar to enforce the uncontroversial data-access rules accepted among data providers, which undergird database owners' ability to publicly publish information. And the freedom to employ technological barriers, such as IP blocks, against data thieves allows CoStar to fight piracy without recourse to the courts. Everyday legitimate consumers of CoStar's information do not receive CoStar's "access denied" messages or cease-and-desist letters.

Rather, the targets of CoStar's anti-piracy unit are unashamed free-riders who set out to profit off the hard work of hundreds of professional researchers. Accordingly, it is difficult to identify the harm that is created if these free-riders are not able to scrape information that another company invested hundreds of millions of dollars to create. There is certainly no harm to consumers, who are able to access information that is useful to them and their transactions because companies like CoStar have the means and incentives to provide it to them.

II. THE DISTRICT COURT'S ADDITION OF A PASSWORD-WALL LIMITATION TO THE CFAA HARMS INTERNET USERS AND INNOVATORS

The district court suggested that LinkedIn's data could be protected under the CFAA if it was put behind a password wall. But limiting CFAA protections to a website's password-protected content would jeopardize the substantial investments made by CoStar and other data providers and put at risk

the benefits from these companies' investments in their databases. Such a rule would harm Internet users, and in any event, is an incorrect interpretation of the statute.

First, the effect of such a rule is obvious; it would encourage firms to make less information publicly available and move information behind password walls to obtain CFAA protection. Such an outcome would unquestionably worsen consumers' Internet experiences. *Second*, by writing an authentication rule into the CFAA, the district court has tied the statute to a mode of technology that will soon be obsolete. The future is "active authentication," and the district court's embrace of outmoded technology could require valuable information and websites to be stuck in the past. *Third*, the district court misinterprets "access without authorization" by anchoring its rule in an ill-fitting analogy. Physical-world analogies do not easily fit the virtual problems that the CFAA was designed to address but, even if they did, a company's exclusion of scrapers is similar to how businesses routinely exclude from their premises visitors who engage in inappropriate conduct, such as stealing.

A. The District Court's Decision Would Make Less Information Available To The Public

It is ironic that the district court was concerned about the effect a company's efforts to prevent its data from being scraped could have on "open access to the Internet," 1ER-2, as the district court then went on to encourage providers to hide information behind an authentication requirement, such as a

password wall. No one needs to guess at the effect of such a rule. If federal law does not back companies that want to give easy access to valuable information to the public, then fewer companies will do so. This harms everyone, and consumers most of all. Password gates decrease end users' ability to connect with information and hamper their online experience.

Password gates make websites less accessible. Because they stand between a user and the data that the user has gone onto the Internet to locate, some of the effects of password gates are obvious. At best, a password gate only slows the user's access to the information that he or she seeks.[4] And, at worst, a password gate can prevent access entirely, in those situations in which a password has been lost and a work-around is not available, either because of malfunctions in the website's systems or because the user has forgotten which answer he or she supplied to the website's security question.

[4] The burdensomeness of password gates has been studied and shown. One survey showed 60 percent of consumers say password requirements are "cumbersome." Sami Luukkonen, "Are Passwords Becoming Obsolete?" *Forbes* (Oct. 12, 2015), *available at* goo.gl/BoFUcA. Another survey revealed that one third of consumers have exited a website because it required them to login, and more than half of consumers have left a website because they forgot their username, password, or the answer to a password-reset security question. "Businesses Should Begin Preparing for the Death of the Password," *Gigya* (2016), *available at* goo.gl/wKBhXA.

Passwords strain the host as well. It is estimated that password resets consume between 20 and 30 percent of all help desk support calls to corporations. Robert McMillan, "Tech Firms Push Toward a Future Without Passwords," *Wall St. J.* (Feb. 8, 2016), *available at* goo.gl/ZC4ViM. CoStar and other Internet-based businesses seek to avoid password requirements as much as possible because they harm the user experience, and the CFAA should not incentivize firms to clutter their websites with such authentication requirements.

B. Password Gates Will Soon Be Obsolete

The district court's authentication requirement also will hold the Internet back. The password gate is on its way out; and in the not-too-distant future, the district court's description of a clear barrier separating the closed spaces of the Internet from the open spaces of the Internet will read as an antiquity. *See* 1ER-14.

Website innovators are building an "active authentication" future that continuously verifies identity based on "the rhythm of our keyboard taps, our attitude on the touchpad, or even how rapidly we scan a page." Rachel Swaby, "The Password Fallacy: Why Our Security System Is Broken, and How to Fix It," *The Atlantic* (Sept. 10, 2012), *available at* goo.gl/RmU9kT. Google is testing active authentication that recognizes patterns of speech. McMillan, *supra*. That is, in the future, login screens will no longer separate the "private interior

of a computer system" from public-facing content. 1ER-10. Instead, websites will confirm their users' identity in the background without their conscious knowledge of it. Does an end user pass through an authentication gate if the end user is never confronted with it?

At a minimum, the district court's decision to write an authentication requirement into the CFAA invites new, difficult questions for protection and could stifle technological progress for firms that want to embrace an active authentication future without risking the loss of CFAA protection. The danger from this rule is especially pronounced here in the Ninth Circuit, where many of the country's leading innovators reside. As recently as this year, the Supreme Court has warned against rules such as these: "The forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow." *Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (2017).

If nothing else, the district court's order risks pitting providers of useful information, such as LinkedIn, *amici*, and CoStar, against the wave of Internet innovation. Affirming it would encourage providers to not provide users with the best possible experience or the best technology.

C. The District Court's Rule Misinterprets The CFAA

The district court's rule would harm the Internet and those who access public databases on it, but the district court's decision also depends on a flawed

reading of the CFAA to import the authentication requirement into its text. The district court believes Congress could not have imagined a future with password-controlled information, and so it could not have written this limitation into Section 1030 itself. 1ER-12-13.

Not so. When Congress expanded the CFAA in 1986 to cover commercial access without authorization, it added a proscription against trading in passwords used to gain access without authorization. Section 1030(a)(6) forbids "traffic[king] . . . in any password or similar information through which a computer may be accessed without authorization." Congress's explicit treatment of passwords in subsection (a)(6) and exclusion of them from subsection (a)(2) belie the district court's importation of this limitation. *See* Brief of Appellant at 42-44 (arguing the district court's interpretation contravenes the structure of the CFAA).

The district court has instead anchored its rule in an analogy to the physical world. But Congress, when it enacted the CFAA, recognized physical-world norms could not settle the hard questions of computer-access law. This is because "[c]omputer technology simply does not fit some of the older, more traditional legal approaches to theft or abuse of property." S. Rep. 99-432, at 13 (1986). As one example of the difference between classic trespass and digital database theft, Congress's report observed "*computer data may be 'stolen' in the sense that it is copied by an unauthorized user*, even though the original

data has not been removed or altered in any way." *Id.* (emphasis added). The CFAA "recogniz[es] computerized information as property," *id.* at 14, and it does not distinguish between computerized information made freely available subject to a prohibition against competitor theft and information that requires authentication to access.

In the district court's analogy, "a business display[s] a sign in its store-front window visible to all on a public street and sidewalk." 1ER-15. The storeowner, the district court observes, cannot ban individuals from looking at the sign, photographing the sign, or viewing the sign with sunglasses. 1ER-15, 16 & n.9.

But that is not what is going on here, and the analogy is particularly inapt. *First*, the analogy wrongfully equates valuable databases with the storefront sign. The shop owner's sign may advertise a product for sale inside or communicate special holiday hours, but no one visits the store to have a look at the sign and probably few who did even remember it was there. The shop's customers care about access to the interior of the store. As applied to LinkedIn and other providers of information on the Internet, the website and its database are the store. And, as the district court recognized, a storeowner can exercise control over whom he allows to enter the store. 1ER-15.

Second, the analogy ignores that the user-generated content published by LinkedIn is valuable data that another company is seeking to take and monetize. The LinkedIn database is worth billions of dollars, and hiQ's business model is to analyze that information for profit. *See* 1ER-4-5, 22. And LinkedIn still makes generally available the information on its website; it is merely trying to prevent someone from stealing that information.

Third, the analogy does not account for hiQ's admitted knowledge that LinkedIn forbids its scraping of the LinkedIn database. In the storefront-window analogy, the competitor has no reason to believe copying the sign would violate the storeowner's rules, and the storeowner would have no way to enforce any such rules. Not so for hiQ. hiQ operates in a field where data-protection norms exist; LinkedIn's terms of use forbid hiQ's theft; and, most importantly, LinkedIn has directly communicated its prohibition of piracy to hiQ.

Accordingly, to the extent there is any physical-world analogy to the present circumstance, a more apt one would involve businesses that actually make valuable information publicly available in the physical world subject to conditions. In these analogies, competitors are, to no one's surprise, forbidden from using cameras to make copies of what they see. For example, many sports teams hold "open practices" in which fans or members of the news media can watch the team practice for games subject to restrictions that prevent

guests from making copies that could end up in an opponent's hands. In the NFL, the San Francisco 49ers, among other teams, invite fans to open practices but ban them from bringing video cameras that could film the team executing its plays. "Fans Guide to 49ers 2017 Open Practice," S.F. 49ers, *available at* goo.gl/ijbTRw.[5] The University of Oregon's football team has limited the amount of media access to practices since 1997, when it learned that opponents had used news media footage from Oregon's practices to scout the team. *See* Kenny Jacoby, "Reporters Pleased As Oregon's New Open Football Practice Policy Goes Into Effect," *Univ. of Oregon Daily Emerald* (April 5, 2017), *available at* goo.gl/zBn99d. Today, Oregon allows reporters' cameras for just the first thirty minutes of practice. *Id.*

As another example, some manufacturers open their factories or plants to the public for tours, but cameras are strictly prohibited so that tourists cannot create a copy of what they see. Members of the public who visit Boeing's

[5] The same is true for the open practices at the Miami Dolphins and Tennessee Titans. *See, e.g.*, "Miami Dolphins Training Camp Guidelines," Miami Dolphins, *available at* goo.gl/ZB6Muc ("The use of any audio or video recording devices is STRICTLY prohibited and such action will result in being asked to leave Training Camp. The transmission of data during practice is also STRICTLY prohibited, which include but is not limited to blogging, tweeting and/or texting."); David Ammenheuser, "A to Z Fans Guide to Titans Training Camp," *The Tennessean* (July 29, 2015), *available at* goo.gl/9MxXMb ("[V]ideos are prohibited. While the Titans officials cannot monitor what you're doing with your cell phone, fans are discouraged from shooting videos with them. Violators will be asked to leave.").

factory in Seattle may take pictures in a museum; once inside the plant, cameras and even binoculars are explicitly prohibited. "Frequently Asked Questions," Future of Flight Aviation Center & Boeing Tour, *available at* goo.gl/YDVuwW. Toyota, Ford, and Hyundai all open their production plants in the United States for public tours, and each of them ban cameras inside.[6]

LinkedIn's and CoStar's prohibitions on the copying of public databases play the same role as the camera bans imposed by the football teams and manufacturing plants that open their property to the public. Both types of copying bans are strictly enforced; the football teams can remove a violator from the practice facility and database owners can use IP blocks to shut out violators. All of our business models permit us to share our property with the public, and society is better for it. However, to do so, we must exclude those who would use their devices—photography in the physical world, scraping techniques in the digital one—to copy our property for a competitor's use.

[6] "Cameras are allowed in the Visitor and Education Center, but must be secured in your vehicle before the plant tour. NO cameras or cell phones allowed in the manufacturing facility." Tour Guidelines, Toyota Manufacturing Texas, *available at* goo.gl/KwmSBT (emphasis in original); *see also* Ford Rogue Tour Tips & Policies, The Henry Ford, *available at* goo.gl/a69DM7; About Hyundai Motor Manufacturing Alabama (HMMA) Tours, Hyundai, *available at* goo.gl/GUaPko.

III. COMPETITION LAW DOES NOT BAR THE USE OF IP BLOCKS TO PROTECT ONLINE DATABASES

Even if LinkedIn is wrong about the applicability of the CFAA, its use of IP blocks to exclude scrapers who would steal and trade on the LinkedIn database does not constitute unfair competition. The district court concluded that hiQ had "raised serious questions" with its allegations LinkedIn had unfairly leveraged its power for an anticompetitive purpose by imposing technological barriers against hiQ's scrapers. 1ER-21. To the contrary, LinkedIn's protection of its valuable database from pirates finds ample support in antitrust law.

Forced sharing of the LinkedIn or CoStar databases would violate "'the long recognized right of [a] trader or manufacturer engaged in an entirely private business[ ] freely to exercise his own independent discretion as to parties with whom he will deal.'" *Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 408 (2004) ("*Trinko*") (quoting *United States v. Colgate & Co.*, 250 U.S. 300, 307 (1919)). A court should "exercise[ ] considerable caution in recognizing exceptions to this broad principle." *Aerotec Int'l, Inc. v. Honeywell Int'l, Inc.*, 836 F.3d 1171, 1183 (9th Cir. 2016).

As an initial matter, the district court's bar against LinkedIn's technological barriers violates an "underlying purpose of antitrust law," which is to encourage all companies to "invest in . . . economically beneficial facilities."

Trinko, 540 U.S. at 407-08; *see also Aerotec Int'l*, 836 F.3d at 1183 (citing *MetroNet Servs. Corp. v. Qwest Corp.*, 383 F.3d 1124, 1131 (9th Cir. 2004)). If LinkedIn and CoStar's databases were unprotected and subject to competitor copying, competitors could reap where they have not sown and profit on a database without having invested in it. Such a rule would destroy the incentive for firms to invest in the research required to populate valuable databases of information for the benefit of consumers. *See Novell, Inc. v. Microsoft Corp.*, 731 F.3d 1064, 1073 (10th Cir. 2013) (Gorsuch, J.).

Less generally, the district court expresses special concern at a perceived connection between LinkedIn's institution of IP blocks against hiQ and LinkedIn's planned launch of analytics products that would offer services not unlike hiQ's analytics. 1ER-22-23. Even assuming such a connection exists, antitrust law backs LinkedIn's protection of its data. Although there are examples of forced cooperation after a firm's change in practices towards a competitor, they are distinguishable from LinkedIn's use of IP blocks. In a decision the Supreme Court later described as "at or near the outer boundary," *Trinko*, 540 U.S. at 409, the Supreme Court held that a ski resort that had "cooperated for years" with its rival in a profitable joint venture could face liability for terminating that venture in order to put its rival out of business. *Id.* at 408-10 (citing *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472

U.S. 585, 601 (1985)). The Court's analysis depended on the fact "the defendant's decision to cease participation in a cooperative venture . . . suggested a willingness to forsake short-term profits to achieve an anticompetitive end." *Id.* at 409.

This exception has no application here. There is no "cooperative venture" between LinkedIn and hiQ. CoStar is not aware of companies engaging in "cooperative venture[s]" with parasitic scrapers who pirate their databases. Indeed, the scraper would not even have an incentive to cooperate with the provider of the information if it could simply take whatever information it wanted whenever it wanted. No one doubts hiQ's representation that technological barriers impede its business model, but that is only because hiQ has chosen a free-riding business model that imperils LinkedIn's data. And "[t]he prevention of free-riding, which is an inherently economic motivation, provides a valid business justification." *Morris Commc'ns Corp. v. PGA Tour, Inc.*, 364 F.3d 1288, 1296–98 (11th Cir. 2004). Unfair competition law does not require LinkedIn to unlock its database for hiQ's copying.

* * * * *

The CFAA is a critical security for firms, like CoStar, that provide valuable information to consumers of all stripes through creating, collating, and categorizing commercially valuable information on the Internet. The CFAA's protection of databases containing that information inures to the great benefit

of the mine run of visitors to such websites, who are able to view information useful to their endeavors without having to pay or, in many cases, be encumbered by password protections. For the general public to continue to benefit from such databases, however, it is vital that the creators of those databases have sufficient incentives to generate the information that goes into them. And those incentives are compromised by any system in which free-riders can use and profit from the data.

The CFAA and competition laws are tools that help align those incentives properly. The district court's order, however casts those incentives into disarray.

CONCLUSION

The district court's preliminary injunction should be vacated.

Respectfully submitted.

/s/ Nicholas J. Boyle
NICHOLAS J. BOYLE
JOHN S. WILLIAMS
ERIC J. HAMILTON
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
(202) 434-5000
nboyle@wc.com

OCTOBER 10, 2017

CERTIFICATE OF COMPLIANCE
WITH TYPEFACE AND WORD-COUNT LIMITATIONS

I, Nicholas J. Boyle, counsel for *amicus curiae* CoStar Group, Inc., and a member of the Bar of this Court, certify, pursuant to Federal Rule of Appellate Procedure 32, that the attached Brief of *Amicus Curiae* is proportionately spaced, has a typeface of 14 points or more, and contains 5,618 words.

/s/ Nicholas J. Boyle
NICHOLAS J. BOYLE

OCTOBER 10, 2017

CERTIFICATE OF SERVICE

I, Nicholas J. Boyle, counsel for *amicus curiae* CoStar Group, Inc., and a member of the Bar of this Court, certify that, on October 10, 2017, a copy of the attached Brief of *Amicus Curiae* was filed with the Clerk and served on the parties through the Court's electronic filing system. I further certify that all parties required to be served have been served.

/s/ Nicholas J. Boyle
NICHOLAS J. BOYLE

OCTOBER 10, 2017