No. 19-783

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

BRIEF OF THE R STREET INSTITUTE, PUBLIC KNOWLEDGE, LINCOLN NETWORK, ENGINE ADVOCACY, THE INNOVATION DEFENSE FOUNDATION, AND THE AMERICAN ANTITRUST INSTITUTE AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

JOHN BERGMAYER
PUBLIC KNOWLEDGE
1818 N St NW Ste 410
Washington, DC 20036

J. SCOTT MCKAIG
LINCOLN NETWORK
44 Tehama St
San Francisco, CA 94105

ABBY RIVES
ENGINE ADVOCACY
700 Pennsylvania Ave SE
Washington, DC 20003

CHARLES DUAN
Counsel of Record
R STREET INSTITUTE
1212 New York Ave NW Ste 900
Washington, DC 20005
(202) 525-5717
cduan@rstreet.org

RANDY M. STUTZ
AMERICAN ANTITRUST INSTITUTE
1025 Connecticut Ave NW Ste 1000
Washington, DC 20036

Counsel for amici curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

Constitutional Provision

Statutes

Other Sources

In the Supreme Court of the United States

No. 19-783

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

BRIEF OF THE R STREET INSTITUTE, PUBLIC KNOWLEDGE, LINCOLN NETWORK, ENGINE ADVOCACY, THE INNOVATION DEFENSE FOUNDATION, AND THE AMERICAN ANTITRUST INSTITUTE AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

INTEREST OF *AMICI CURIAE*

The R Street Institute[1] is a nonprofit, nonpartisan public policy research organization. R Street's mission is to engage in policy research and educational outreach that promotes free markets, as well as limited yet effective government, including properly calibrated legal and

[1]Pursuant to Supreme Court Rule 37.3(a), all parties received appropriate notice of and consented to the filing of this brief. Pursuant to Rule 37.6, no counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of the brief. No person or entity, other than *amici*, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief.

regulatory frameworks that support Internet economic growth and individual liberty. R Street's particular focus on Internet law and policy is one of offering research and analysis that show the advantages of a more market-oriented society and of more effective, more efficient laws and regulations that protect freedom of expression and privacy.

Public Knowledge is a nonprofit organization dedicated to preserving an open Internet and the public's access to knowledge, promoting creativity through balanced intellectual property rights, and upholding and protecting the rights of consumers to use innovative technology lawfully. As part of this mission, Public Knowledge advocates on behalf of the public interest for a balanced copyright system, particularly with respect to new, emerging technologies.

Lincoln Network is a nonprofit organization that seeks to bridge the often siloed discussions between policy makers in Washington, D.C. and technologists in Silicon Valley so as to advance smart policy that encourages innovation. The organization regularly hosts policy panels, hackathons, and conferences convening influencers and technologists to address challenges facing political institutions and the nation.

Engine Advocacy is a nonprofit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups, working with government and a community of high-technology, growth-oriented startups across the nation to support the development of technology entrepreneurship. Engine conducts research, organizes events, and spearheads campaigns to educate elected officials, the entrepreneur com-

munity, and the general public on issues vital to fostering technological innovation.

The Innovation Defense Foundation is a project of the Method Foundation, which is a nonprofit, nonpartisan research and issue-advocacy institution that advocates for "permissionless innovation," seeking to repeal, relax, or replace unnecessary regulations that stand in the way of innovation. Through a combination of research, advocacy, and regulatory filings, the IDF pushes back against risk-averse, regressive, and precautionary policies that both threaten America's innovators and limit our society's ability to cope with new and existing challenges.

The American Antitrust Institute is an independent nonprofit organization devoted to promoting competition that protects consumers, businesses, and society. It serves the public through research, education, and advocacy on the benefits of competition and the use of antitrust enforcement as a vital component of national and international competition policy. AAI enjoys the input of an Advisory Board that consists of over 130 prominent antitrust lawyers, law professors, economists, and business leaders.[2]

[2]Individual views of members of AAI's Board of Directors or Advisory Board may differ from AAI's positions.

SUMMARY OF ARGUMENT

Laws generally do not aim to suppress competition, entrench monopolies, or reduce consumer choice and welfare. Yet the Computer Fraud and Abuse Act, under a broad construction applied by the Court of Appeals, embraces these adverse, anticompetitive results. Firms can wield the broad construction, under which access to computer information is "unauthorized" whenever the accessor violates a contractual or other stated term for how the information may be used, in multiple ways that do not merely injure competitors but rather impede competition as a whole. That this broad construction turns the CFAA from a computer trespass statute into a business tool for blocking competition shows that the construction is wrong.

I. Recent uses of the CFAA reveal the many ways to invoke the statute to suppress competition. Dominant social media firms have invoked the CFAA to prevent users from transferring their information over to competitor services, cementing network effects that protect those dominant firms from competition. Platform services, ones that serve as bases upon which innovative startups can build new products, have cut off startup products on their platforms to favor their own clones. And companies have sought to restrict price comparison tools from accessing pricing data, limiting consumer choice and raising prices in the process.

These uses of the CFAA are far from the intended purpose of that statute, namely to prevent abusive intrusion and trespassing into computers. The information accessed in the aforementioned cases was public or generally available, and the basis for invoking the CFAA was not illicit trespass but rather contractual terms that

prohibit competitive uses of information. Broad construction of the CFAA, which renders these anticompetitive contractual terms powerfully enforceable, thus turns the law into a weapon against competition.

II. Intellectual property laws further demonstrate problems with the broad construction of the CFAA. Both trade secret and copyright law embody careful balances intended to ensure that they do not overstep on legitimate competition: Trade secrets protect only nonpublic information where reasonable measures are taken to ensure secrecy; copyright does not protect facts and includes limitations such as the fair use doctrine.

The CFAA lacks any balances commensurate with those intellectual property laws. As such, the broad construction of the CFAA enables firms to construct ad hoc trade secret protections without complying with the secrecy requirements of trade secret law, and enables firms to invent copyright-like protections on uncopyrightable facts with none of the competition-preserving limitations of copyright law. The legislative history confirms that the CFAA was not intended to override intellectual property regimes, and the statute should not be construed to do so.

III. While the broad construction of the CFAA produces these anticompetitive effects, narrower constructions do not. The construction proffered by Petitioner, based on entitlement to access information, would prevent anticompetitive terms of use from being actionable under the CFAA. More specific constructions proposed by several *amici*, which would require technical access control measures before the CFAA could be invoked, would further prevent the law from being used for anticompetitive purposes, while still precluding actual instances of computer intrusion or trespass. These inter-

pretations should be adopted to prevent further misuse of the CFAA to hinder competition.

To the extent that businesses wish to limit uses of their computer information, contract law is their vehicle for doing so; computer operators always have the option of bringing suit for breach of contract. But long-established rules of contract law balance proprietary interests and the general preference for competition; the CFAA's powerful remedies exceed those balanced rules of contracts.

In these ways, the broad construction of the CFAA exemplifies what then-Professor Easterbrook warned against in his 1983 work *Statutes' Domains*: a statute, intended to deal with computer trespass, now applied to stymie competition and supplant contract and intellectual property laws.[3] The statute was never meant to have such an expansive domain, and this Court should construe it narrowly to return it to its proper scope.

ARGUMENT

I. Broad Construction of the CFAA Enables Anticompetitive Conduct

In addition to being a criminal statute, the Computer Fraud and Abuse Act includes extensive civil liability and remedies. *See* 18 U.S.C. § 1030(g). In view of the broad interpretation of the statute embraced by the Court of Appeals and other courts, businesses have frequently invoked the CFAA not to prevent computer intrusion or trespass but to suppress competition by "restrict[ing]

[3] *See* Frank H. Easterbrook, *Statutes' Domains*, 50 U. Chi. L. Rev. 533, 544 (1983).

their competitors' access to information they've published publicly online for the rest of the world to see." Jamie L. Williams, *Automation Is Not "Hacking": Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 B.U. J. Sci. & Tech. L. 416, 420 (2018).

In particular, the CFAA has been used in at least three anticompetitive contexts: to stymie direct competitors, to close off platforms to new startups, and to interfere with tools that advance consumer choice.

A. Incumbent Companies Can Directly Block Competitors from Entering the Market

Most directly, the broad reading of the CFAA enables companies, social media platforms in particular, to stop competitors from building competing services. A review of judicial opinions under that law found that "a tremendous number of these opinions concern claims brought by direct commercial competitors or companies in closely adjacent markets to each other." Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. Sci. & Tech. L. 372, 390 (2018) (footnote omitted).

In a striking example found in *Facebook, Inc. v. Power Ventures, Inc.*, a startup social networking service called Power.com enabled individuals to aggregate their content and relationships from multiple existing services onto a simple, unified system. *See* 844 F.3d 1058, 1062 (9th Cir. 2016). To enable this aggregation, a user would authorize Power.com to collect information from those existing social media services by accessing the user's account on each service. *See id.* at 1067. One of these

existing services, Facebook, demanded that Power.com cease and desist from accessing data this way, and subsequently sued under the CFAA. *See id.* at 1063.

While the Ninth Circuit recognized that Power.com had initial authorization to access Facebook data, it held that the cease-and-desist letter revoked any further access, rendering Power.com in violation of the CFAA. *See id.* at 1067. To reach that conclusion, the court applied a broad reading of that statute, under which a mere letter that "warned Power that it may have violated federal and state law" was sufficient to render access unauthorized. *See id.* at 1067 n.3. As a result, Facebook was able to leverage the CFAA to prevent a competitor from accessing otherwise-available data to start a business.

Facebook's CFAA success against Power.com comes at a time of controversy over the dominance of social media companies, including Facebook itself. Scholars often attribute the lack of competition in the social media market to lock-in caused by network effects—Facebook users face difficulty switching to new platforms because their photos, writings, and friend relationships are already stuck within Facebook.[4] Policymakers and experts have thus looked to measures to increase "interoperability," that is, to enable users to migrate to competing social networks without loss of data or key functionalities like

[4]*See, e.g.*, Spencer Weber Waller, *Antitrust and Social Networking*, 90 N.C. L. Rev. 1771, 1787–88 (2012). Many social media companies now allow users to retrieve some of their data, but that retrievable fraction of data appears to be less than useful. *See* Gabriel Nicholas & Michael Weinberg, *Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?* 15–17 (2019), *available online*. Locations of authorities available online are shown in the Table of Authorities.

messaging.[5] There have been calls to encourage or even require data sharing or interoperability, to enable new competitor entry.[6]

To be sure, "there is no consensus" as to how antitrust law should account for "technologically dynamic markets characterized by network effects." *See United States v. Microsoft Corp.*, 253 F.2d 34, 50 (D.C. Cir. 2001). Nevertheless, these important antitrust questions should not be preempted by an unrelated law of computer trespass. If potentially anticompetitive terms of service are enforceable under the CFAA, as they apparently were in *Power Ventures*, then that law becomes a powerful tool for companies to preserve market share and suppress competition.

Experience shows that companies will wield such competition-suppressing power to the fullest extent. *See* Cory Doctorow, *Adversarial Interoperability*, Electronic Frontier Found. (Oct. 2, 2019). For example, brand-name drug manufacturers have asserted safety regulations to withhold samples from generic competitors, thereby preventing the competitors from completing the regulatory process prerequisite to entering the market. *See* Michael A. Carrier, *Sharing, Samples, and Generics: An Antitrust Framework*, 103 Cornell L. Rev. 1, 9–12 (2017); Henry N. Butler, *REMS-Restricted Drug Distribution Programs and the Antitrust Economics of Refusals to Deal with Potential General Competitors*, 67 Fla. L. Rev. 977, 979 (2016). This behavior, which courts and federal

[5] *See, e.g.*, Gus Rossi & Charlotte Slaiman, *Interoperability = Privacy + Competition*, Pub. Knowledge (Apr. 26, 2019).

[6] *See* Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2019, S. 2658, 116th Cong. sec. 4(a) (Oct. 22, 2019).

authorities have described as a "significant threat to competition," Butler, *supra*, at 991 (quoting FTC assistant director Markus Meier), is much like Facebook's invocation of the CFAA against Power.com: A dominant firm making a resource publicly available except to competitors, and citing an unrelated safety law to justify this anticompetitive act.

Use of the CFAA to hamstring direct competition thus illustrates how "[m]isuse of courts and governmental agencies is a particularly effective means of delaying or stifling competition." Robert H. Bork, *The Antitrust Paradox* 159 (1978). In particular, CFAA assertion is a form of "cheap exclusionary behavior": It is virtually costless for a dominant firm to write terms of service invoking the CFAA to exclude competition, and the broad construction renders that cheap exclusionary tactic powerfully effective. Susan A. Creighton et al., *Cheap Exclusion*, 72 Antitrust L.J. 975, 992 (2005). It is difficult to imagine Congress intending a computer trespass law to have this sort of exclusionary effect.

B. Online Platform Operators Can Copy and Then Foreclose Innovative Startups

The broad construction of the CFAA also impedes competition in a different circumstance, where a computer service operates a platform upon which other tools or services are built. Using the CFAA, a monopoly-minded platform provider can knock out innovative startups or other services on the platform, even while subsuming their businesses for the platform's own.

An example is found in *HiQ Labs, Inc. v. LinkedIn Corp.*, which involved well-known website LinkedIn, a

platform for professionals to share their resumes and career information. *See* 938 F.3d 985, 991 (9th Cir. 2019). A startup firm, hiQ, used LinkedIn's public data platform as a basis for analysis to provide companies with novel insights such as identifying career opportunities, recommending bonuses, or identifying needed training. *See id.*

Initially, LinkedIn offered no analogous service to hiQ and in fact embraced a relationship with the company for several years, perhaps because hiQ's services were a value-add atop LinkedIn's platform. *See id.* Yet in May 2017, LinkedIn demanded that hiQ cease and desist from accessing any further LinkedIn data, threatening to invoke the CFAA and essentially putting an end to hiQ's business. *See id.* at 992. Just months later, LinkedIn announced its own new product, Talent Insights, which offered data insights highly similar to hiQ's. *See id.* at 991–92 & n.7. In other words, LinkedIn positioned itself to absorb hiQ's business just as LinkedIn invoked the CFAA to shut hiQ down.

LinkedIn's introducing an alternative service to hiQ may well have been procompetitive, but forcibly excluding hiQ was almost certainly not. Indeed, the Ninth Circuit stated that "LinkedIn's conduct may well not be 'within the realm of fair competition.'" *See id.* at 998 (quoting *Inst. of Veterinary Pathology, Inc. v. Cal. Health Labs., Inc.*, 116 Cal. App. 3d 111, 127 (Ct. App. 1981)).[7] Specifically, a platform company favoring its own platform-using product by denying competitors access to the platform is a form of "input foreclosure," which

[7]The court ultimately relied on a separate claim for tortious interference and did not reach the unfair competition claim directly. *See id.* at 999 & n.11.

antitrust scholars and enforcement agencies have long wrestled with and often found to be problematic.[8]

In *Microsoft*, for example, the dominant operating system maker took a variety of actions to inhibit use of a third-party web browser Netscape Navigator, relative to Microsoft's own Internet Explorer, including use of contracts to foreclose installation of Netscape on the operating system to an extent. *See* 253 F.2d at 59–64. The D.C. Circuit held many of those actions, including the contract-based foreclosure, to violate § 2 of the Sherman Act. *See id.* at 63–78. Similarly, LinkedIn foreclosed its data platform to hiQ, thereby favoring its own Talent Insights product; to the extent that LinkedIn had market power in its data, its acts would have fallen within the logic of *Microsoft*.

But LinkedIn's potentially anticompetitive actions would have been absolved and permissible if its cease-and-desist letter triggered the CFAA. *See HiQ*, 938 F.3d at 999. While the Ninth Circuit ultimately found the CFAA inapplicable, it did so on narrow grounds: Because LinkedIn's website and thus data was "accessible to the general public" with no authentication system at all, the authorization elements of the CFAA were not invoked. *Id.* at 1003. Had LinkedIn installed even a perfunctory

[8] *See* U.S. Dep't of Justice & Fed. Trade Comm'n, *Vertical Merger Guidelines* 4–7 (June 30, 2020), *available online*. To be sure, there is substantial theoretical debate over the frequency and likelihood of foreclosure in a variety of different contexts. *See, e.g.*, Steven C. Salop, *Invigorating Vertical Merger Enforcement*, 127 Yale L.J. 1962, 1966–67 (2018) (describing differing views in merger context); Herbert J. Hovenkamp, *Robert Bork and Vertical Integration: Leverage, Foreclosure, and Efficiency*, 79 Antitrust L.J. 983, 995–96 (2014) (describing Bork, *supra*, at 236–37). But foreclosure based on invocation of the CFAA is guaranteed to occur by operation of that law's injunctive provisions.

or nominal authentication system,[9] *HiQ* suggests that the CFAA would have applied to preempt hiQ's unfair competition claims, enabling LinkedIn and other technology platforms to block competitors and strengthen their grip over the technology market. *See id.* at 1001–02. The broad construction of the CFAA could thus propel forward behavior that the antitrust laws and *Microsoft* have sought to forestall.

C. CFAA Assertion Limits Consumer Choice and Facilitates Unfair Pricing

The CFAA, broadly construed, also enables companies to restrict competition by limiting tools that enable consumer choice.

The quintessential example of a consumer choice–enhancing tool is a price comparison service, one that aggregates prices across multiple vendors to allow consumers to make optimal choices. Yet companies have invoked the CFAA to block price comparison services. In *Southwest Airlines Co. v. Farechase, Inc.*, a company called Outtask used software to collect pricing and route data from airlines in order to offer a service for comparing airfares. *See* 318 F. Supp. 2d 435, 437 (N.D. Tex. 2004). Southwest Airlines objected, claiming that the fares listed on its public website were "proprietary" and that Outtask's collection of those fares was unauthorized under the Use Agreement on Southwest's website, which prohibited automated collection of data. *See id.* at 438. On a motion to dismiss, the district court found that Southwest's Use Agreement, while perhaps not enforceable as a contract, nevertheless "directly informed Outtask that

[9]For example, it could have users create a costless, anonymous account before viewing LinkedIn data.

their access was unauthorized," and therefore Southwest had stated a claim under the CFAA. *Id.* at 440.

Other cases have similarly held that collection of computerized public pricing data can violate the CFAA where contractual terms prohibit it. *See, e.g.*, *Ryanair DAC v. Expedia Inc.*, No. 17-cv-1789, slip op. at 6 (W.D. Wash. Aug. 6, 2018) (airfares); *EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577, 583–84 (1st Cir. 2001) (travel tours service); *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 969–70 (N.D. Cal. 2013) (real estate listings).

Blocking of price comparison services damages consumer welfare. Activity that heightens the costs of searching for the best deal, which economists call "obfuscation," can "increase average markups and the fraction of consumers buying from relatively high-priced firms." Glenn Ellison & Sara Fisher Ellison, *Search, Obfuscation, and Price Elasticities on the Internet*, 77 Econometrica 427, 430 (2009). "[L]owering search costs[] will unambiguously increase social welfare," so blocking services that lower search costs will decrease welfare. Dale O. Stahl II, *Oligopolistic Pricing with Sequential Consumer Search*, 79 Am. Econ. Rev. 700, 709 (1989).

Regarding airlines specifically, a 2015 study found that blocking comparison shopping "is likely to lead to higher average airfares" and ultimately "strengthen the market power of the major airlines," with a "total net consumer welfare impact" of "potentially $7.3 billion annually." Fiona Scott Morton et al., Travel Tech. Ass'n, *Benefits of Preserving Consumers' Ability to Compare Airline Fares via OTAs and Metasearch Sites* 3, 57 (2015), *available online*. Across six different markets, cutting off online price comparison services could raise prices by 10–15%. *See id.* at 53.

Nevertheless, companies face strong incentives to leverage legal tools such as the CFAA to limit price comparison shopping. *See* Glenn Ellison & Alexander Wolitzky, *A Search Cost Model of Obfuscation*, 32 RAND J. Econ. 417, 435 (2012). Southwest Airlines, for example, was able to raise its prices over competitors, sometimes by over 20%, by refusing to be listed on price comparison services. *See* Morton et al., *supra*, at 24; Volodymyr Bilotkach, *Reputation, Search Cost, and Airfares*, 16 J. Air Transport Mgmt. 251, 253 tbl.2 (2010). And the effectiveness of other price obfuscation strategies has led the Federal Trade Commission and others to consider whether such strategies constitute unfair or deceptive practices. *See* David Adam Friedman, *Regulating Drip Pricing*, 31 Stan. L. & Pol'y Rev. 51, 68–71, 86–91 (2020) (citing national authorities in United States, Canada, and Australia).

Price comparison tools are just one of many welfare-enhancing services with which the CFAA could interfere. Another example is privacy-enhancing software. The growing use of data to track and analyze Internet users for highly targeted advertising (and perhaps more nefarious reasons) has raised concerns among many.[10] In response, software developers have built tools to combat this loss of privacy by blocking Internet transactions that facilitate online tracking.[11] Such software has received

[10]*See, e.g.*, David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. Econ. Persp. No. 3, at 37, 55–58 (2009); Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 Comm. ACM No. 5, at 44, 52 (2013) (observing patterns of racial discrimination in online advertising).

[11]To explain further, many websites include hidden references to online tracking services. When a person visits any of those websites, the hidden reference instructs the person's computer to

tremendous praise and widespread usage,[12] but online advertisers unsurprisingly dislike it and have in fact used their terms of service to prohibit such privacy-enhancing software—terms of service that could be powerfully enforced under the broad construction of the CFAA.[13]

Examples such as these have led commentators to conclude that the CFAA "limit[s] the valid tools consumers need to protect themselves online." Ashkan Soltani, *Protecting Your Privacy Could Make You the Bad Guy*, Wired (July 23, 2013). Consumers and free markets benefit from services like price comparison tools and privacy-enhancing software, services that enhance competition and consumer choice. That the CFAA, broadly interpreted, can render these tools illegal demonstrates that the law has overstepped its intended bounds to anticompetitive effect.

---

send a message to the tracking service, thereby alerting the tracking service of the person's activities. In much the same way that a person can transact with a business with anonymous cash rather than a traceable credit card, privacy-enhancing software enables the person's computer to transact only with the desired website and not the tracking service. *See generally* Cory Doctorow, *Adblocking: How About Nah?*, Electronic Frontier Found. (July 25, 2019). Privacy-enhancing software is often conflated with software that blocks display of online advertisements ("ad-blockers"), but they are distinct insofar as the former focuses on invisible tracking techniques that generally display no visible advertisements. *See, e.g.*, Johan Mazel et al., *A Comparison of Web Privacy Protection Techniques*, 144 Computer Comm. 162 (2019).

[12] *See* Doc Searls, *Beyond Ad Blocking—The Biggest Boycott in Human History*, Doc Searls Weblog (Harv. Blogs) (Sept. 29, 2015).

[13] *See, e.g.*, Dami Lee, *Spotify Bans Ad Blockers in Updated Terms of Service*, The Verge (Feb. 7, 2019); *cf.* Anastasia Shuba et al., *NoMoAds: Effective and Efficient Cross-App Mobile Ad-Blocking*, Proc. on Privacy Enhancing Techs., Oct. 2018, at 125 (noting possible relevance of and lack of case law on the CFAA).

II. Conflicts with the Intellectual Property Laws Show That the Broad Construction of the CFAA Enables Anticompetitive Behavior

The broad construction of the CFAA is furthermore incorrect because it conflicts with intellectual property laws. Those laws consistently feature cautious rules of balance that limit the ability of information holders to restrict competition and preserve monopolies. The CFAA, broadly construed, lacks any such balance and instead allows firms holding computerized information to set unilateral rules of access regardless of competitive consequences. In that sense, the broad construction of the CFAA enables firms to construct ad hoc, unbalanced intellectual property regimes that Congress and this Court have long sought to avoid. A computer trespass statute ought not be interpreted in this manner, inconsistent with other statutory schemes.

A. Trade Secret Law Requires Secrecy Tradeoffs That the CFAA Disregards

Trade secret law illuminates the error of the broad construction of the CFAA, because that construction effectively allows firms to protect public information as if it were a trade secret.

Protecting proprietary information that brings value to a business by virtue of its secrecy, trade secret law offers a range of powerful remedies for unauthorized disclosure, including, like the CFAA, injunctive relief and criminal penalties. *See* 18 U.S.C. § 1836(b)(3) (damages and injunctive relief); § 1836(b)(2) (civil seizure); § 1832

(criminal penalties).[14] But trade secret law carefully balances interests between protection and competition. Information generally known to the public cannot be a trade secret. *See* 18 U.S.C. § 1839(3)(B); *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475 (1974). Public information such as airfare offers and social media profiles thus cannot be protected under trade secret law. Furthermore, a business must take "reasonable measures" to maintain the secrecy of trade secrets. 18 U.S.C. § 1839(3)(A). Courts have often held that mere contractual provisions, not backed by technical measures or substantial enforcement capacity, fail to be "reasonable measures."[15]

A narrow construction of the CFAA is likely consistent with trade secret law, since unauthorized access to information would occur only if the information is kept secret such that the accessor lacks entitlement to access it. The broad construction, however, introduces inconsistency: A firm can make information public and thus unprotectable under trade secret law, but nevertheless craft terms of use prohibiting competitive uses of that information, enjoying trade secret–like remedies without meeting the requirements for trade secret protection.

Consider, for example, the *Southwest Airlines* case described above. Southwest Airlines was free to prevent its airfares from being listed on price comparison services

[14]While trade secret law is generally a matter of state law, the recently-enacted federal law is sufficiently similar to most states' laws, so it is cited here.

[15]*See, e.g., Bison Advisors LLC v. Kessler*, No. 14-cv-3121, slip op. at 10 (D. Minn. Aug. 12, 2016); *nClosures Inc. v. Block & Co., Inc.*, 770 F.3d 598, 603 (7th Cir. 2014); *Fire 'Em Up, Inc., v. Technocarb Equip. (2004) Ltd.*, 799 F. Supp. 2d 846, 851 (N.D. Ill. 2011); *Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890, 901–02 (Minn. 1983).

by treating those airfares as trade secrets. *Sw. Stainless, LP v. Sappington*, 582 F.3d 1176, 1189 (10th Cir. 2009) (treating price lists as trade secrets). But it could do so only at the cost of not publishing those airfares on Southwest's own website and enjoying the benefits of rapid e-commerce. By invoking the broad construction of the CFAA to impede price comparison services while still listing prices on its website, Southwest effectively obtained the advantages of trade secret law without accepting the costs of secrecy.

As a second example, the Second Circuit found no trade secret misappropriation where a company's ex-employee accessed computer information without authorization, because the company, in failing to implement technical protections on a computer housing its sensitive client lists, had not taken "adequate measures" to warrant trade secret protection. *Defiance Button Mach. Co. v. C & C Metal Prods. Corp.*, 759 F.2d 1053, 1063–64 (2d Cir. 1985). Had the company been able to assert the CFAA at the time, it may have succeeded in showing a violation under the broad construction of that law, effectively circumventing the limitations of trade secret law.

The limitations of trade secret law are not arbitrary; they are designed "to strike the classic balance between free competition on one hand and the prevention of unfair competition on the other." Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 Hamline L. Rev. 493, 543 (2010). Insofar as trade secret law excludes certain information from protection, it is because that degree of protection is overly contrary to free competition. Insofar as the broad con-

struction of the CFAA offers protection for that excluded information, that construction is overly contrary to free competition as well.

B. Copyright Law Incorporates Balances and Exceptions Not Found in the CFAA

Like trade secrets, copyrights enable firms to prevent competitors from using proprietary information. Indeed, plaintiffs in CFAA cases frequently bring copyright infringement claims as well.[16] And as with trade secret law, limitations of copyright law demonstrate the overreach of the broad construction of the CFAA.

Copyright protection inheres in works of original authorship and prohibits others from copying such protected works. *See* 17 U.S.C. § 102(a). However, not all acts of copying are proscribed. Copyright protection applies only to expressive elements of works, not underlying facts. *See* § 102(b); *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 344–45 (1991) (quoting *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 556 (1985)). Copyright inures to the author of the information, even if the information is possessed by someone else. *See* 17 U.S.C. § 201(a). Furthermore, even expressive elements may be copied to the extent allowed under the doctrine of fair use, which encompasses copying for purposes such as news reporting, scholarly quotation, parody, education, and so on. *See* § 107; *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 575–78 (1994). Finally, the Constitution mandates that copyright

[16] *See, e.g., Explorica*, 274 F.3d at 580; *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 523 (S.D.N.Y. 2004).

subsist only "for limited times." U.S. Const. art. 1, § 8, cl. 8; *see* 17 U.S.C. § 302.

The CFAA, broadly construed, subverts all these elements of copyright law. Cases such as *Southwest Airlines* and *Explorica* demonstrate uses of the CFAA to prevent copying of uncopyrightable factual information such as price lists. *Power Ventures* involved assertion of the CFAA to protect data authored by third parties—indeed, third parties who consented to the copying. The CFAA contains no fair use provision. And there is no time limit on a CFAA-backed ad hoc "copyright" regime.

As a result, under the broad construction of the CFAA, a business can use cleverly crafted terms of service effectively to invent a "para-copyright tool to secure exclusivity to otherwise publicly accessible data." Nicholas A. Wolfe, *Hacking the Anti-Hacking Statute: Using the Computer Fraud and Abuse Act to Secure Public Data Exclusivity*, 13 Nw. J. Tech. & Intell. Prop. 301, ¶ 5, at 303 (2015). Since most information today is stored on computers, the computer operators need only draft terms of use specifying copyright-like rules for how their information is to be used, and may then assert the CFAA against undesirable uses, whether or not those uses would be copyright infringements.

That the CFAA, construed broadly, can overreach what Congress intended again demonstrates the anti-competitiveness of that construction. The traditional limitations of copyright law have long reflected a "balance of competing claims" between authors and the public, and between protection and competition. *Fogerty v. Fantasy, Inc.*, 510 U.S. 517, 526 (1994) (quoting *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975)). Broad constructions of the CFAA "upset the careful bal-

ance that the Copyright Act has struck between authors and society." Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 Md. L. Rev. 320, 365 (2004) (citing Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. Dayton L. Rev. 179, 182 (2001)). This Court in particular has long concerned itself with avoiding expansive intellectual property protections that go "beyond the limits of his specific grant" of copyright. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984). To allow an unrelated criminal law—a computer trespass statute, no less—to render the copyright statutes practically superfluous would effectively open a back door for circumventing this Court's precedents designed to protect competitive markets.

C. Statutory Text and Legislative History Confirm that the CFAA Was Not Intended to Supersede Intellectual Property Law

In enacting the current version of the CFAA, Congress was aware of the overlap between that law and intellectual property rules discussed above. The text and legislative history confirm that Congress did not intend the CFAA to enable companies to devise ad hoc schemes that render trade secret and copyright law superfluous.

The key provisions rendering the CFAA applicable to non-governmental computers appear in the National Information Infrastructure Protection Act of 1996. But that law did not stand alone: It was Title II of the Economic Espionage Act of 1996, of which Title I was a

comprehensive federal trade secret protection law. *See* Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491. The provisions of Title I included all of the careful balancing elements discussed above. *See, e.g.*, *id.* sec. 101, § 1839(3)(A)–(B). The proponents of the EEA specifically observed that the trade secret law included "a number of safeguards" meant to protect competition and employee mobility, and the Managers' Statement on the bill called out in more detail limitations of trade secret protection such as reasonable measures and public information. 142 Cong. Rec. 27116 (1996).

The drafters of the 1996 CFAA amendments were also keenly aware of copyright law, indeed borrowing the latter's text. *See* 18 U.S.C. § 1030(c)(2)(B)(i) (using 17 U.S.C. § 506(a)); S. Rep. No. 104-357, at 8 (1996). Importantly, they intended the two legal regimes to be distinct. Recognizing in its report that in many cases information accessed in violation of the CFAA "is also copyrighted," the Senate committee observed that unauthorized access to that information "may implicate certain rights under the copyright laws." S. Rep. No. 104-357, *supra*, at 7. Nevertheless, the committee recognized that the "crux of the offense" under the CFAA was not misuse of copyrighted material, but rather "the abuse of a computer to obtain the information." *Id.* at 7–8.

It would have made little sense for Congress to jettison the careful balancing of copyright and trade secret law with a computer trespass statute so broad as to enable ad hoc intellectual property rights. The committee report's description of the 1996 amendments as "privacy protection coverage" against "computer trespasses" confirms that Congress intended the statute to be distinct from intellectual property misappropriation

(and intended the protected information to be private, not public). *Id.* at 4; *see United States v. Nosal*, 676 F.3d 854, 857 & n.3 (9th Cir. 2012) (en banc). To be sure, the report acknowledges correctly that the CFAA provides additional causes of action for "theft of intangible information." S. Rep. No. 104-357, *supra*, at 7. No doubt the CFAA overlaps with information theft, but that phrase in the report is no warrant to *redefine* information theft, particularly in ways inconsistent with the trade secret provisions of Title I of the EEA.

None of this is to say that the intellectual property laws are perfectly sufficient to deal with all manner of proprietary business information. But to the extent that loopholes remain, the proper avenue is not the CFAA but Congress, which has repeatedly patched those laws to deal with problems such as boat hull designs and semiconductor manufacturing. *See* 17 U.S.C. § 902(a)(1); § 1301(a)(1). The statutory domain of the CFAA is technical trespass upon computers, not the manufacture of novel intellectual property interests. It should be construed to stay within that domain.

III. The CFAA Should Be Construed Narrowly to Exclude Terms of Use as Conditions of Authorization

To avoid the anticompetitive consequences thus described, the CFAA should be construed narrowly as Petitioner and others suggest. To the extent that computer-operating companies have legitimate needs to enforce their terms of use or contractual relationships with users, they ought to rely on contract law rather than the CFAA.

A. A Narrow Construction of the CFAA Better Ensures Competition

Congress did not intend for the CFAA to be a tool for blocking competition; proponents of the key 1996 amendments to that law specifically warned that they "do not want this law used to stifle the free flow of information or of people from job to job." 142 Cong. Rec. at 27116. Yet the broad construction of the CFAA, under which a computer operator's terms of use can render access to computer information "unauthorized," is the root of the anticompetitive behaviors thus described. By deeming competitive business activity to be "unauthorized" use under the CFAA, a computer operator offering a data service, such as a social media website or e-commerce platform, can restrict competition, gobble up startups, and inhibit consumer welfare–enhancing services.

Competition in technology markets is better protected by narrower constructions of the CFAA embraced by Petitioner, supporting *amici*, and several courts of appeals. Under Petitioner's test, a person entitled to access computer information is authorized and thus beyond the reach of the statute regardless of how that information is later used. Under this test, a computer service operator cannot differentiate under the CFAA between ordinary uses of the service (social media website visitors, airline travelers) and competitive uses of computer information (social media competitors, airfare price comparators). A firm that opens itself up for business to the former class of users cannot leverage the CFAA to nevertheless close itself off to the latter competitive uses.

Several *amici* further refine Petitioner's test such that any lack of entitlement rendering access "unauthorized" must be a computerized technical measure. This

test more strongly guards against anticompetitive behavior. As seen in the examples described above, the computer operator will frequently send a specific cease-and-desist letter to competitors or startups, thereby rendering access unauthorized under the CFAA. This post hoc revocation of access to restrict competition would not be possible under a technical measures test.

B. Existing Contract Remedies Render the Broad Construction Superfluous and Excessive

In most cases of unauthorized computer access, authorization to access the protected computer is specified in an actual or attempted contract that identifies permitted and disallowed uses of information on that computer. Regardless of how the CFAA is interpreted, an action for breach of contract often can offer remedies for improper use of information accessed on a computer. *See Ward v. TheLadders.com, Inc.*, 3 F. Supp. 3d 151, 162 (S.D.N.Y. 2014); Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1170 (2016). The broad construction of the CFAA is thus unnecessary to give computer operators the power to restrict how information on that computer is used.

Yet contract law contains important competition-preserving limitations not found in the CFAA. The remedies differ starkly: Criminal penalties are available under the CFAA but not mere breach of contract. *See United States v. D'Amato*, 39 F.3d 1249, 1261 n.8 (2d Cir. 1994). Preliminary injunctions issue routinely under the CFAA, *see* Sellars, *supra*, at 394 & n.159, despite being an "extraordinary and drastic remedy" in other areas of law. *Munaf v. Geren*, 553 U.S. 674, 689–90 (2008) (quoting 11A

Charles A. Wright, Arthur R. Miller & Mary K. Kane, *Federal Practice and Procedure* § 2948, at 129 (2d ed. 1995)).

Application of the CFAA also ignores contract formation requirements, such that mere notice of terms of use suffices to create liability regardless of whether the contractual terms were accepted. *See Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17, 31–32 (2002) (Sotomayor, J.) (discussing lack of notice and assent to website terms of use); *Sw. Airlines*, 318 F. Supp. 2d at 440 (finding possible CFAA violation "[r]egardless of whether the Use Agreement creates an enforceable contract"); Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. Rev. 2164, 2242 (2004). Contract law also provides in some cases for disregarding unconscionable terms and interpreting contracts in view of public policy; the CFAA has no such doctrines. *See* U.C.C. §§ 2–302 (2002); *Scott v. United States*, 79 U.S. (12 Wall.) 443, 445 (1871); 11 Richard A. Lord, *Williston on Contracts* § 32:19 (4th ed. 2012); Restatement (Second) of Contracts § 207 (1979). The CFAA further dispenses with privity of parties, since liability can attach to one who "conspires to commit" an offense. 18 U.S.C. § 1030(b).

And perhaps most importantly, enforcement of contracts is directly subject to the antitrust laws, most notably § 1 of the Sherman Act, which prohibits any "contract . . . in restraint of trade or commerce." 15 U.S.C. § 1. Insofar as an anticompetitive contract may be enforceable via the broad construction of the CFAA, *cf. HiQ*, 938 F.3d at 999, that construction of the law conflicts with the intent of Congress expressed in the Sherman Act.

"Statutes which invade the common law . . . are to be read with a presumption favoring the retention of long-established and familiar principles, except when a statutory purpose to the contrary is evident." *Isbrandtsen Co. v. Johnson*, 343 U.S. 779, 783 (1952); *see Impression Prods., Inc. v. Lexmark Int'l, Inc.*, 137 S. Ct. 1523, 1533 (2017); *Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519, 552–53 (2013). This is especially so where the statute that invades a common law field, such as contract law, was drafted toward an unrelated regulatory domain, such as computer trespass. *See* Frank H. Easterbrook, *Statutes' Domains*, 50 U. Chi. L. Rev. 533, 544 (1983). There is no indication that Congress sought to rewrite traditional doctrines of contract law when enacting the CFAA; this Court should not interpret it to do so.

CONCLUSION

For the foregoing reasons, the decision of the Court of Appeals should be reversed.

Respectfully submitted,

CHARLES DUAN
Counsel of Record
R STREET INSTITUTE
1212 New York Ave NW Ste 900
Washington, DC 20005
(202) 525-5717
cduan@rstreet.org

JOHN BERGMAYER
PUBLIC KNOWLEDGE
1818 N St NW Ste 410
Washington, DC 20036

J. SCOTT MCKAIG
LINCOLN NETWORK
44 Tehama St
San Francisco, CA 94105

RANDY M. STUTZ
AMERICAN ANTITRUST INSTITUTE
1025 Connecticut Ave NW Ste 1000
Washington, DC 20036

ABBY RIVES
ENGINE ADVOCACY
700 Pennsylvania Ave SE
Washington, DC 20003

Counsel for amici curiae

July 2020