2021

Hacking Antitrust: Competition Policy and the Computer Fraud and Abuse Act

Charles Duan

HACKING ANTITRUST: COMPETITION POLICY AND THE COMPUTER FRAUD AND ABUSE ACT

CHARLES DUAN*

The Computer Fraud and Abuse Act, a federal computer trespass statute that prohibits accessing a computer "without authorization or exceeding authorized access," has often been criticized for clashing with online norms, over-criminalizing common behavior, and infringing freedom-of-expression interests. These controversies over the CFAA have raised difficult questions about how the statute is to be interpreted, with courts of appeals split on the proper construction and the Supreme Court set to consider the law in its current October Term 2020.

This article considers the CFAA in a new light, namely its effects on competition. Rather than merely preventing injurious trespass upon computers, the CFAA has become a favorite legal tool for dominant firms in the computer services industry to suppress competition, expand their market control, and impose transaction costs that limit consumer choice. To explore how the CFAA implicates competition, two novel approaches are used. First, this article compares prior uses of the CFAA to competition issues identified in the computer industry and other fields. This comparison reveals that the CFAA has the ability to insulate from legal scrutiny activity that at a minimum raises serious questions about negative effects on competition. Second, the article draws upon the theory and law of intellectual property, in particular trade secrets and copyright. Because it protects information but lacks the competition-protective features of copyrights and trade secrets, the

 Senior Policy Fellow, Program on Information Justice and Intellectual Property, American University Washington College of Law; Senior Fellow for Technology and Innovation Policy, R Street Institute, Washington, D.C. This article is based in part on an *amicus curiae* brief that the author filed with the Supreme Court in *Van Buren v. United States*, No. 19-783 (July 7, 2020), on behalf of the R Street Institute and others. The author would like to thank John Bergmayer, Wayne Brough, Andrew Crocker, Avery Gardiner, Zach Graves, Blake Reid, Abby Rives, Randy Stutz, several counsel involved with the *Van Buren* litigation, and the editors of the *Colorado Technology Law Journal* for their valuable thoughts and assistance that contributed to this article.

CFAA essentially creates an ad hoc intellectual property regime that enables the improper suppression of competition.

The legislative history of the CFAA suggests that Congress did not intend the computer intrusion statute to supplant intellectual property law or to be a tool for suppressing competition. To ensure consistency with this legislative intent, then, this article posits that the CFAA should be narrowly construed such that access "without authorization" does not include violations of restrictions on how accessed data is subsequently used. At least from a competition policy perspective, a narrow construction is favorable over the broad one.

INTRODUCTION

As originally drawn, the Computer Fraud and Abuse Act prohibits malicious trespass upon and intrusion into computer systems,[1] an activity colloquially called "computer hacking."[2]

1. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) (West, Westlaw through Pub. L. No. 116–259).

2. The term "hacking" is notoriously problematic in that it more properly refers to the salutary behavior of devising unexpected, often efficient ways of achieving a desired result, particularly on a computer. *See generally* Ben Yagoda, *A Short History of "Hack,"* NEW YORKER (Mar. 6, 2014), https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack [https://perma.cc/HPZ3-EJ9M]. Its negative connotation, as computer intrusion, is a semantic narrowing likely resulting from mainstream media portrayals of teenage computer malfeasants around the 1980s. *See id.*; Orly Turgeman-Goldschmidt, *Meanings that Hackers Assign to Their Being a Hacker*, 2 INT'L J. CYBER CRIMINOLOGY 382, 383 (2008) (available at: http://www.cybercrimejournal.com/Orlyijccdec2008.pdf [https://perma.cc/KAS9-2WXF]). For example, the film *WarGames* is often credited for spurring passage of the CFAA. Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 175 (2000) (discussing cultural impact of *WarGames* and relationship

Enacted in 1984 and subsequently amended several times,[3] the CFAA imposes criminal and civil penalties upon anyone who "intentionally accesses a computer without authorization or exceeds authorized access" and thus causes any "damage and loss."[4]

In the four decades since, the CFAA has left open a question that courts have not been able to resolve: what is the scope of "without authorization" under the statute; that is, when does a person's access to a computer violate the statute?[5] In general, the law is amenable to two constructions. Under the "narrow" construction, violation occurs only when the person has no permission to access the computer at all and uses technical circumvention or fraudulent credentials; under the "broad" construction, even a person with permission to access the computer may violate the CFAA if that person subsequently uses information from the computer contrary to a contractual provision or terms of use.[6] The federal appeals courts have split on these two

---

to the CFAA); *see also Counterfeit Access Device and Computer Fraud and Abuse Act: Hearings on H.R. 3181, H.R. 3570, and H.R. 5112 Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 98th Cong. 185 (1983–1984), https://catalog.hathitrust.org/Record/011341755 [https://perma.cc/829M-E7GN] (testimony of Peter Waal, Vice President of Marketing, GTE-Telenet describing *WarGames* as a "realistic representation" of computer intrusion), *quoted in* COUNTERFEIT ACCESS DEVICE AND COMPUTER FRAUD AND ABUSE ACT OF 1984, H.R. REP. NO. 98-894, at 10 (1984). This ambiguity is serendipitously apt for the title of this article, which contends that the CFAA is an unexpected way to circumvent competition policy, but for purposes of clarity the term is not used henceforth in this article.

3. *See infra* note 147 and accompanying text.

4. 18 U.S.C. § 1030(a)(5)(C). The statute also contains several other pathways giving rise to liability. *See, e.g., id.* § 1030(a)(5)(B) (liability for recklessly causing damage). Civil penalties further require a showing of specific losses, such as losses within one year totaling $5000 in value. *See id.* § 1030(g), (c)(4)(A)(i)(I). This threshold is generally easily met. *See* Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1197 (E.D. Wash. 2003) (discussing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001)).

5. For an early significant treatment of this question, *see* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003) [hereinafter Kerr 2003]. The statutory phrase "exceeds unauthorized access" raises similar questions, but since both phrases contain the undefined term "authorization," courts have generally construed the two in tandem. *See, e.g.*, LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (using "exceeds unauthorized access" to interpret "without authorization"). The difference is not relevant to this article, which focuses on what qualifies as a lack of authorization under the statute.

6. *See* United States v. Valle, 807 F.3d 508, 525–28 (2d Cir. 2015) (discussing alternative constructions of the CFAA). Obviously, this is a simplification; commentators recognize a variety of diverse approaches. *See generally* Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1446–60 (2016) [hereinafter Bellia 2016]. For purposes of this article, however, the above distinction suffices since the relevant tensions between the CFAA and competition policy largely align with conditions on subsequent use of data. *See infra* Section III.

constructions,[7] and the Supreme Court recently granted a petition for a writ of certiorari on the issue.[8]

Commentators have vigorously analyzed these competing interpretations of the CFAA from a variety of perspectives, including norms of openness on the Internet,[9] the business of website scraping,[10] employer–employee relationships and employee mobility,[11] overcriminalization of everyday behavior,[12] analogy to criminal law doctrines such as authorization and

---

7. *See Valle*, 807 F.3d at 524–25. For cases favoring the narrower construction, *see id.* at 528; WEC Carolina Energy Sols., LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012) (en banc). For cases favoring the broader construction, *see* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); Explorica Inc., 274 F.3d 577, 582–83; Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

8. *See* See Van Buren v. United States, No. 19-783 (June 3, 2021). After this article was written but before it went to press, the Supreme Court issued its decision in the case, which is discussed infra notes 174–181..

9. *See, e.g.*, Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1161 (2016) [hereinafter Kerr 2016] (arguing that the CFAA ought to mirror the "presumptively open norms for the Web"); 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, 446 (2018) ("[I]t is necessary to ensure that the CFAA cannot be used to undermine open access to publicly available information online . . . ."); 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, 324 (2004) ("[A] sweeping reading of prohibited acts under the CFAA threatens the free flow of information that belongs in the public domain. As a result, the continued openness of the Internet, along with its attendant benefits, is at risk.").

10. *See, e.g.*, Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 412–13 (2018) (discussing implications of the CFAA for web scraping technologies, which provide important benefits to consumers and the public).

11. *See, e.g.*, Pamela Taylor, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 HOUS. L. REV. 201, 203 (2012); Katherine M. Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 821–22 (2009) (discussing application of the CFAA to employment cases); Glenn R. Schieck, *Undercutting Employee Mobility: The Computer Fraud and Abuse Act in the Trade Secret Context*, 79 BROOK. L. REV. 831, 844 (2014) ("Further, the CFAA allows employers to effectively enforce non-compete agreements that would be otherwise unenforceable under state law in cases where former employees use misappropriated information to compete in a new position.").

12. *See, e.g.*, Sarah A. Constant, *The Computer Fraud and Abuse Act: A Prosecutor's Dream and a Hacker's Worst Nightmare—The Case Against Aaron Swartz and the Need to Reform the CFAA*, 16 TUL. J. TECH. & INTELL. PROP. 231, 248 (2013) (describing the CFAA as "the ultimate catchall for computer infractions" that "gives prosecutors the power to pile charges onto unsuspecting Internet and computer users"); 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, ¶ 11, at 306 (2015) (noting that broad construction of the CFAA "inadvertently increased potential for many of us to be categorized as hackers").

consent,[13] reference to technical computer security measures,[14] and effects on "white hat" cybersecurity research.[15] The broad construction of the statute has been criticized as inconsistent with the rule of lenity in criminal law,[16] the Due Process Clause's prohibition on vagueness in criminal statutes,[17] equal protection under the Constitution,[18] freedom of expression under the First Amendment,[19] and the statute's legislative history.[20]

This article approaches interpretation of the CFAA and in particular the "without authorization" question from a different perspective, namely competition policy. Powerful remedies and broad civil enforcement abilities[21] have turned the federal computer trespass statute into a forceful tool for dominant firms,

---

13. *See, e.g.*, Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477, 1479 (2016) (authorization under the CFAA should mirror physical trespass law's authorization doctrine); James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500, 1521 (2016) (proposing construction of "authorization" under the CFAA "as incorporating the traditional legal understanding of consent, as seen, for example, in the criminal law of trespass, theft, battery, and rape").

14. *See, e.g.*, Kerr 2003, *supra* note 5, at 1649 (proposing that "without authorization" be limited to "access that circumvents restrictions by code"); Cyrus Y. Chung, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233, 250 (2010) (suggesting analogy to computer filesystem access control lists to define authorization under the CFAA).

15. *See, e.g.*, Trevor A. Thompson, *Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the "White Hats" Under the CFAA*, 36 FLA. ST. U. L. REV. 537, 567–68 (2009) (discussing the CFAA's deterrent effect on computer security researchers); Komal S. Patel, Note, *Testing the Limits of the First Amendment: How Online Civil Rights Testing Is Protected Speech Activity*, 118 COLUM. L. REV. 1473, 1477–83 (2018) (describing computer testing research to uncover algorithmic discrimination).

16. *See, e.g.*, Taylor, *supra* note 11, at 218–19 (favoring narrow construction of the CFAA in view of "logical application of the criminal lenity rule").

17. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1562 (2010) [hereinafter Kerr 2010] (contending that broad construction of the CFAA is unconstitutionally vague because it "would either provide insufficient notice of what is prohibited or fail to provide guidelines for law enforcement in violation of the constitutional requirement of Due Process of Law"); Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2258 (2004) [hereinafter Bellia 2004] (broad interpretation of the CFAA "might raise due process concerns, in that criminal liability would attach without a user having fair notice of the prohibited conduct").

18. *See* Laurent Sacharoff, *Criminal Trespass and Computer Crime*, 62 WM. & MARY L. REV. 571, 645–46 (comparing effects of the CFAA to racial discrimination based on physical trespass law).

19. *See* Patel, *supra* note 15, at 1475–76 (considering First Amendment violations resulting from the CFAA's application to testing of online services for civil rights violations); Galbraith, *supra* note 9, at 323 ("Recent court decisions have allowed website owners to utilize the CFAA to override the carefully balanced provisions of the copyright laws and improperly restrict speech in violation of the First Amendment.").

20. *See, e.g.*, Bellia 2004, *supra* note 17, at 2253–57 (narrow construction of the CFAA better aligns with statutory language and legislative history).

21. *See* 18 U.S.C. § 1030(c) (West, Westlaw through P.L. 116–259) (criminal penalties); § 1030(i)–(j) (criminal forfeiture of computer equipment); § 1030(g) (civil action).

especially firms in the information technology industry, to engage in conduct that harms not just competitors but competition in general. This article reviews multiple instances of litigation under the CFAA that fit this pattern.[22] Insofar as Congress almost certainly did not intend the CFAA to be used for anticompetitive purposes and those purposes contravene other established federal policy,[23] this article concludes that the statute should be construed to avoid anticompetitive uses and the narrower construction better does so.

To be sure, both courts and commentators have asserted that the broad construction makes the CFAA into an "anti-competitive sword," though without substantial consideration of how exactly the statute interacts with competition policy.[24] This article uncovers that interaction from two points of view. Section I compares several the CFAA cases with specific issues that have arisen in competition policy, including technological interoperability,[25] cheap exclusion,[26] input foreclosure,[27] and price obfuscation.[28] This comparison reveals that CFAA assertion, under a broad construction of the statute, enables and insulates business activity that either contravenes competition law or is at least highly questionable under it.[29]

Section II reveals the deleterious effects of the CFAA on competition from the perspective of intellectual property law, in particular copyrights and trade secrets. Others have observed

22. *See infra* Section I.

23. *See infra* Section II.C.

24. Williams, *supra* note 9, at 416, 420–21 (noting "skirmishes between competing commercial services" but focusing on Internet openness concerns instead); *see also* Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 970 n.8 (N.D. Cal. 2013) (noting that "[a]pplying the CFAA to publicly available website information presents uncomfortable possibilities," but nevertheless construing the statute to cover such information); Joseph Oat Holdings, Inc. v. RCM Digesters, Inc., 409 F. App'x 498, 506 (3d Cir. 2010) (noting in passing that "[s]ome commentators have noted that suits under anti-hacking laws have gone beyond the intended scope of such laws and are increasingly being used as a tactical tool to gain business or litigation advantages.") (quoting Andrew B. Serwin, *Poised on the Precipice: A Critical Examination of Privacy Litigation*, 25 SANTA CLARA HIGH TECH. L.J. 883, 887 (2009)); Galbraith, *supra* note 9, at 324; Breana Love, *The Chaos of the CFAA: Facebook's Successful CFAA Claim Affects Website Owners, Competitors, and You*, 50 LOY. L.A. L. REV. 831, 842–43 (2017) (criticizing major websites' use of the CFAA "not to protect their platforms, but to eradicate competing third party businesses" though focusing more on consequences for "everyday users").

25. *See infra* text accompanying notes 40–57.

26. *See infra* text accompanying notes 57–61.

27. *See infra* text accompanying notes 68–76.

28. *See infra* text accompanying notes 91–103.

29. *See infra* Section I.

tension between the CFAA and both copyrights[30] and trade secrets,[31] but the competition policy effects of the CFAA–intellectual property relationship have generally not been explored, which has led commentators to take a variety of positions on whether the CFAA as a normative matter ought to override intellectual property law.[32] Simultaneous consideration of intellectual property theory and competition policy resolves this normative question due to the observation that copyrights and trade secrets, like all forms of intellectual property, include doctrinal limitations that are specifically intended to promote competition.[33] Insofar as the CFAA enables firms to create quasi–intellectual property rights without the balancing limitations of copyrights or trade secrets, the computer trespass statute undermines competition beyond the intentions of Congress and

30. *See, e.g.*, Wolfe, *supra* note 12, ¶ 5, at 303 (describing the CFAA "as a para-copyright tool to secure exclusivity to otherwise publicly accessible data"); Galbraith, *supra* note 9, at 323; Kathleen C. Riley, *Data Scraping as a Cause of Action: Limiting Use of the CFAA and Trespass in Online Copying Cases*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 245, 305–06 (2019) (proposing application of copyright law rather than the CFAA in cases of data scraping).

31. *See, e.g.*, United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) (describing how the CFAA's "general purpose is . . . not misappropriation of trade secrets"); Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429, 447–50 (2009) (describing how the CFAA "disserves the fundamental policy goals of trade secret protection"); Omri Rachum-Twaig & Ohad Somech, *Breaking into an Empty House: A Theory of Remedies for CFAA Unauthorized Access to Non-Proprietary Information*, 82 ALB. L. REV. 555, 555–56 (2019) (noting "significant tension between the CFAA unauthorized access doctrine and basic understandings of (lack of) property rights in information," including copyright and trade secrets law); Schieck, *supra* note 11, at 856 ("Beyond eroding the theoretical policy considerations of trade secret law, the CFAA's lack of a reasonably protective measures requirement may discourage employers from adequately investing in data protection, which is economically inefficient."); Field, *supra* note 11, at 846 (describing broad interpretation of the CFAA as "an arrow capable of overriding traditional trade secret liability and thus disrupting established policy preferences in employment law").

32. *Compare* references cited *supra* note 31 *with* Tiffany A. Miao, *Access Denied: How Social Media Accounts Fall Outside the Scope of Intellectual Property Law and into the Realm of the Computer Fraud and Abuse Act*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1017, 1060–61 (2013) (contending that the CFAA "better protects" social media information that is unprotectable under intellectual property law), Graham M. Liccardi, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. 155, 157 (2008) ("The CFAA . . . has a distinct advantage in that it protects *all* valuable computer data regardless of whether it is proven a trade secret under state law."), *and* Patrick J. Manion, *Two Steps Forward, One Step Back: The Defend Trade Secrets Act of 2016 and Why the Computer Fraud and Abuse Act of 1984 Still Matters for Trade Secret Misappropriation*, 43 J. LEGIS. 289, 292 (2016) ("I conclude by arguing that the Computer Fraud and Abuse Act may be a more attractive remedy for trade secret misappropriation claims considering recent state and federal trends disfavoring non-compete covenants and in light of the state non-compete carve out provisions of the Defend Trade Secrets Act").

33. *See infra* text accompanying notes 121–133 (discussing trade secrets); *infra* text accompanying notes 138–144 (discussing copyrights).

state legislators. Indeed, because relevant amendments to the CFAA were debated and enacted in tandem with a federal trade secrets law,[34] the intellectual property and competition perspective on the CFAA allows the legislative history to illuminate the proper interpretation of the statute in ways heretofore not considered in the literature.[35]

In view of this analysis of the CFAA in light of competition issues and intellectual property theory, Section III concludes that a narrower construction better effectuates congressional intent and positive competition policy compared to the broader construction. Two specific narrower constructions are considered: an entitlement-based test, where access without authorization occurs only when the accessor has no entitlement to access the data for any reason; and a code-based test, where a denial of authorization must be in the form of computer code restricting access. Both narrower constructions better serve competition policy, and while they cannot prevent all anticompetitive behavior involving the CFAA, the behaviors that remain unchecked, namely technological access restrictions designed to inhibit competition, are less problematic from a competition perspective because they are harder to implement, easier to identify, and more amenable to challenge under the antitrust laws.

I. HOW THE CFAA IS USED TO BLOCK COMPETITION

In addition to being a criminal statute, the CFAA includes extensive civil liability and remedies.[36] In view of the broad interpretation of the statute embraced by several courts of appeals,[37] businesses have frequently invoked the CFAA not to prevent computer intrusion or trespass but to suppress competition by "restrict[ing] their competitors' access to information they've published publicly online for the rest of the world to see."[38]

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.

34. *See* Economic Espionage Act of 1996 (EEA), Pub. L. No. 104-294 tit. II, 110 STAT. 3488, 3491.

35. *See infra* Section II.C.

36. *See* 18 U.S.C. § 1030(g) (West, Westlaw through P.L. 116–259).

37. *See* cases cited *supra* note 7.

38. Williams, *supra* note 9, at 420.

A. *Competitor Blocking by Incumbent Companies*

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."[39]

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.[40] To enable this aggregation, a user would authorize Power.com to collect information from existing social media services by accessing the user's account on each service.[41] One of these existing services, Facebook, demanded that Power.com cease and desist from accessing data this way, and subsequently sued under the CFAA.[42]

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.[43] 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.[44] 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.[45] Scholars often attribute the lack of competition in the social media market to an economic phenomenon called a "network externality" or "network effect," which occurs

---

39. Sellars, *supra* note 10, at 390 (footnote omitted).

40. *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1062 (9th Cir. 2016).

41. *See id.* at 1067.

42. *See id.* at 1063.

43. *See id.* at 1067.

44. *See id.* at 1067 n.3.

45. Within the United States, Facebook is facing antitrust inquiries from the Department of Justice, the Federal Trade Commission, Congress, and state attorneys general. *See* John D. McKinnon, *States to Launch Google, Facebook Antitrust Probes*, WALL ST. J. (Sept. 6, 2019, 5:20 PM), https://www.wsj.com/articles/states-to-launch-google-facebook-antitrust-probes-11567762204 [https://perma.cc/6CAZ-Q6K9]; David McLaughlin, *Attorney General Barr Seeks DOJ Facebook Antitrust Probe*, BLOOMBERG (Sept. 25, 2019, 6:30 PM), https://www.bloomberg.com/news/articles/2019-09-25/attorney-general-barr-sought-doj-facebook-antitrust-probe [https://perma.cc/LZ2S-AEB3]; Cecilia Kang, Jack Nicas, & David McCabe, *Amazon, Apple, Facebook and Google Prepare for Their "Big Tobacco Moment,"* N.Y. TIMES (July 28, 2020), https://www.nytimes.com/2020/07/28/technology/amazon-apple-facebook-google-antitrust-hearing.html [https://perma.cc/WD55-Y42J].

when the value of a product to a consumer depends on the number of other users of that product.[46] The classic example is the telephone network, since the value of owning a telephone increases as more people can be called with it,[47] and modern social media networks plainly display network effects in that their value depends on how many people one can share content or be friends with.[48] Among other consequences of markets exhibiting network effects is that users of the dominant product will tend to be unwilling to switch to a new competitor that lacks an equally sized user base, since that competitor's product will be of less value simply by virtue of being new.[49] In the social media context, users of Facebook's leading service face difficulty switching to new platforms because a new social network without Facebook's expansive user base would be a less effective platform for broadcasting content, messaging friends, and maintaining relationships.[50]

To overcome the impediment to competition that network effects present, policymakers and experts have 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 messaging.[51] There have been calls to encourage or even require data sharing or interoperability to enable new competitor entry.[52] Technology firms have historically leveraged a wide range of legal strategies to hold up interoperability, suggesting that at least in technology markets,

---

46. *See generally* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 174–75, 183–84 (1998).

47. *See* JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 4–5 (2005).

48. *See* Spencer Weber Waller, *Antitrust and Social Networking*, 90 N.C. L. REV. 1771, 1788 (2012).

49. *See* SHAPIRO & VARIAN, *supra* note 46, at 184–85.

50. *See, e.g.*, Waller, *supra* note 48, at 1787–88. About nine years ago, Waller further suggested that Facebook also maintains dominance by making it difficult for users to retrieve their content to bring it over to competitors. *See id.* at 1788–92. But it is generally fairly easy to retrieve content today, and more recent research suggests that the problem with that retrieved data is that the data is not especially useful for enhancing competition. *See* GABRIEL NICHOLAS & MICHAEL WEINBERG, DATA PORTABILITY AND PLATFORM COMPETITION: IS USER DATA EXPORTED FROM FACEBOOK ACTUALLY USEFUL TO COMPETITORS? 14–17 (2019), (available at: https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition) [https://perma.cc/TKQ3-9XBW].

51. *See, e.g.*, Gus Rossi & Charlotte Slaiman, *Interoperability = Privacy + Competition*, PUB. KNOWLEDGE (Apr. 26, 2019), https://www.publicknowledge.org/blog/interoperability-privacy-competition/ [https://perma.cc/LM9A-R7F6]; *see also* Rory Van Loo, *In Defense of Breakups: Administering a "Radical" Remedy*, 105 CORNELL L. REV. 1955, 2006–12 (comparing "access remedies" such as interoperability to antitrust-based firm breakups).

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

interoperability is especially important to competition (and thus especially distasteful to dominant firms).[53]

To be sure, "there is no consensus" as to how antitrust law should account for "technologically dynamic markets characterized by network effects," including matters of interoperability.[54] The problem that the CFAA presents, though, is that it forecloses the competition inquiry as to interoperability entirely. It is difficult for courts and lawmakers to engage in dialogue over which interoperability-restricting terms of service are anticompetitive if the CFAA is understood to legitimize those terms of service by backing them with civil and criminal penalties.[55] Thus, as one commentator argues, the CFAA as interpreted in *Power Ventures* "gives Facebook greater power to reduce its users' ability to control their personal data, leading to further potential issues in the realm of Internet monopolies."[56]

Facebook's invocation of the CFAA against Power.com closely matches a pattern that other commentators have observed of dominant firms using regulatory systems to suppress competition. Robert Bork devoted a full chapter of *The Antitrust Paradox* to describing how the misuse of courts and governmental agencies is a particularly effective means of delaying or stifling competition, which he called "[p]redation by abuse of governmental procedures."[57] He gave business licensing, zoning, health and safety inspections, and sham litigation as examples of uses of public interest legislation to delay or thwart competition.[58] More recently,

---

53. *See, e.g.*, Charles Duan, *Of Monopolies and Monocultures: The Intersection of Patents and National Security*, 36 SANTA CLARA HIGH TECH. L.J. 369, 384 (2020) [hereinafter Duan 2020] (noting invocation of national security concerns to avoid injunction that otherwise would require licensing of patents covering technological interoperability standards); Charles Duan, *Internet of Infringing Things: The Effect of Computer Interface Copyrights on Technology Standards*, 45 RUTGERS COMPUT. & TECH. L.J. 1, 5–10 (2019) (discussing assertion of copyright in computer interfaces to prevent interoperability); MILTON MUELLER, UNIVERSAL SERVICE: COMPETITION, INTERCONNECTION AND MONOPOLY IN THE MAKING OF THE AMERICAN TELEPHONE SYSTEM 129 (2013) (available at: https://surface.syr.edu/books/18/ [https://perma.cc/F6JU-LAYL]) (describing Bell telephone system's use of interoperability restrictions to the disadvantage of competing independent telephone services); *See generally* Cory Doctorow, *Adversarial Interoperability*, ELEC. FRONTIER FOUND. (Oct. 2, 2019), https://www.eff.org/deeplinks/2019/10/adversarial-interoperability [https://perma.cc/Z8TU-YFZE] (noting examples of legal regimes leveraged to prevent such interoperability, including patents, privacy, copyright, and telecommunications).

54. United States v. Microsoft Corp., 253 F.3d 34, 50 (D.C. Cir. 2001).

55. As discussed below, courts have viewed the CFAA as potentially exempting business activities from scrutiny under the antitrust or other laws. *See infra* notes 76–82.

56. Love, *supra* note 24, at 845.

57. ROBERT H. BORK, THE ANTITRUST PARADOX 159–347 (1978).

58. *See id.* at 347–48.

Susan Creighton and colleagues at the Federal Trade Commission have described the phenomenon of "cheap exclusion," namely business strategies that exclude competitors with little cost or risk for firms engaging in them, and have called for "closer enforcement scrutiny" with regard to such practices.[59] Among the cheap exclusion strategies that they describe is the use of litigation or litigation threats that take advantage of "cost/benefit asymmetries" to delay competitor entry.[60]

A perhaps unexpected analogy may be found in pharmaceutical regulations. Generic drug manufacturers must obtain approval to market their products and compete with brand-name pharmaceutical firms;[61] this approval includes showings that their generic drugs are "the same as" and "bioequivalent to" the already-approved brand-name products.[62] To make this showing, the generic manufacturers require samples of the brand-name drug, and brand-name firms have on occasion refused to sell such samples on the grounds that doing so would violate safety regulations on the distribution of the drug.[63] Commentators and competition authorities have described this behavior as "a significant threat to competition" because it prevents the formation of competitive markets for the drug and does not serve the purposes of the safety regulations.[64]

Akin to brand-name drug companies using a pharmaceutical safety regulatory regime to block competition in drug markets by holding up access to an ingredient necessary for regulatory approval, dominant technology firms can use the CFAA's anti-trespass provisions, when broadly construed, to block competition in social media markets by holding up access to interoperability

59. Susan A. Creighton et al., *Cheap Exclusion*, 72 ANTITRUST L.J. 975, 977 (2005).

60. *Id.* at 992–93. To be sure, both Bork and Creighton et al. discuss sham litigation, but the CFAA cases are often meritorious at least in jurisdictions following the broad construction. Nevertheless, their analyses are applicable because they describe situations where litigation is "for the sake of exclusion, rather than on the merits." *Id.* at 992; *see also* BORK, *supra* note 57, at 357–58 (describing "distinction between legitimate and predatory litigation"). A CFAA plaintiff such as Facebook is likewise seeking not to prevent injurious abuse of its computer systems but rather to exclude competitors.

61. *See* 21 U.S.C. § 355(a), (j)(4) (West, Westlaw through Pub. L. 116–259).

62. 21 U.S.C. § 355(j)(2)(A)(ii)(II), (iv); *see* Elizabeth Stotland Weiswasser & Scott D. Danzis, *The Hatch-Waxman Act: History, Structure, and Legacy*, 71 ANTITRUST L.J. 585, 594 (2003).

63. *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).

64. *See* Butler, *supra* note 63, at 991 (quoting FTC assistant director Markus Meier). In particular, the statute authorizing such safety regulations specifically warns against using those regulations "to block or delay approval" of a generic drug. *See* 21 U.S.C. § 355–1(f)(8) (West, Westlaw through P.L. 116–259).

necessary for effective competition in those markets. This anticompetitive potential of the broad construction of the CFAA ought to weigh strongly against that construction.

B. Platform Dominance and Input Foreclosure

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 the well-known website LinkedIn, a platform for professionals to share their resumes and career information.[65] 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.[66]

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.[67] However, 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.[68] Just months later, LinkedIn announced its own new product, Talent Insights, which offered data insights highly similar to hiQ's.[69] In other words, LinkedIn positioned itself to absorb hiQ's business while simultaneously invoking 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.'"[70]

LinkedIn's exclusion of hiQ is an example of "input foreclosure," a competition policy concept generally used in the context of vertical mergers.[71] Input foreclosure occurs when, in a vertical supply chain, an upstream product is concentrated or

---

65. *See* 938 F.3d 985 (9th Cir. 2019).
66. *See id.* at 990.
67. *See id.*
68. *See id.* at 992.
69. *See id.* at 991–92, 992 n.6.
70. *See id.* at 998 (quoting *Inst. of Veterinary Pathology, Inc. v. Cal. Health Labs., Inc.*, 116 Cal. App. 3d 111, 127 (App. Ct. 1981)).
71. *See, e.g.*, U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, VERTICAL MERGER GUIDELINES 4 n.4 (June 30, 2020).

monopolized, but a downstream market is competitive; for example, there may be a single firm supplying oranges but many firms that make and sell orange juice.[72] If the orange supplier decides to go into the orange juice business as well, it could theoretically stop selling oranges to all of the other juicers and thereby monopolize the orange juice market.[73]

Input foreclosure has often been described as "harmful to competition."[74] In *United States v. Microsoft Corp.*, 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.[75] The D.C. Circuit held many of those actions, including the contract-based foreclosure, to violate § 2 of the Sherman Act.[76]

Similarly, LinkedIn foreclosed its data platform to hiQ thereby favoring its own Talent Insights product.[77] To the extent that LinkedIn had market power in its data, its acts would have fallen within the logic of *Microsoft*. Indeed, the Ninth Circuit agreed that, at least for purposes of a preliminary injunction, hiQ was likely to succeed in showing that LinkedIn had tortiously interfered with hiQ's contracts; it appeared to be willing to agree that hiQ would likely succeed on an unfair competition claim as well.[78]

But LinkedIn's potentially anticompetitive actions of blocking hiQ's access to data would have been absolved and permissible if that blocking was permissible under the CFAA.[79] As LinkedIn argued and the court appeared to accept, if hiQ's access to LinkedIn's data was "without authorization" under the CFAA, then "hiQ could have no legal right of access to LinkedIn's data and so could not succeed on any of its state law claims."[80] While the Ninth Circuit ultimately found the CFAA inapplicable, it did so on narrow grounds: because LinkedIn's website and thus data was "accessible

72. *See id.* at 6.

73. *See id.*

74. *See* Michael A. Salinger, *Vertical Mergers and Market Foreclosure*, 105 Q.J. ECON. 345 (1988); Oliver Hart & Jean Tirole, *Vertical Integration and Market Foreclosure*, 1990 BROOKINGS PAPERS ON ECON. ACTIVITY: MICROECONOMICS 205, 205–06 (1990).

75. *See* United States v. Microsoft Corp., 253 F.3d 34, 59–64 (D.C. Cir. 2001).

76. *See id.* at 63–78.

77. *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 992 (9th Cir. 2019).

78. *See id.* at 999. Though the court declined to reach the unfair competition claim in view of its decision on tortious interference, the opinion's various references to conduct "not . . . within the realm of fair competition" are telling. *See id.* at 998 (internal quotations removed).

79. *See id.* at 999.

80. *Id.*

to the general public" with no authentication system at all, the authorization elements of the CFAA were not invoked.[81] Had LinkedIn installed even a perfunctory or nominal authentication system,[82] the *HiQ* decision suggests that the CFAA would have applied to preempt hiQ's unfair competition claims, enabling LinkedIn and other technology platforms to engage in input foreclosure to cut off downstream businesses in favor of their own offerings.[83]

To be sure, commentators have vigorously disputed input foreclosure—particularly the frequency and likelihood of it occurring in various contexts such as vertical mergers.[84] Most notably, Bork and the Chicago School took the view that foreclosure was unlikely to occur as a result of a vertical merger because the merged firm still stood to make profits by selling the intermediate good: the orange supplier, for example, would have to forgo substantial profits to be made from orange juicers were it to foreclose on them.[85] Subsequent scholars disagreed, developing economic models for predicting when vertical integration was likely to occur.[86]

The theoretical disagreement over vertical mergers and foreclosure, however, is not relevant to foreclosure based on the CFAA. That disagreement is over when foreclosure will occur if at all; it is generally agreed that if foreclosure does occur, it will negatively affect competition and consumer welfare.[87] But when

---

81. *Id.* at 1003.

82. For example, it could have users create a costless, anonymous account before viewing LinkedIn data. LinkedIn is now doing so. *See* Peter Molnar, *LinkedIn Is Ignoring User Settings*, PETER'S HOMEPAGE (July 1, 2020), https://petermolnar.net/article/linkedin-public-settings-ignored/ [https://perma.cc/CV5K-T84Q].

83. *See hiQ*, 938 F.3d at 1001–02.

84. *See, e.g.*, Steven C. Salop, *Invigorating Vertical Merger Enforcement*, 127 YALE L.J. 1962, 1966–67 (2018) (discussing differing views); Nikolas Guggenberger, *The Essential Facilities Doctrine in the Digital Economy: Dispelling Persistent Myths*, 23 YALE J.L. & TECH. (forthcoming 2021) (manuscript at 8–17), https://ssrn.com/abstract=3703361 [https://perma.cc/HTT5-MDKR] (reviewing arguments relating to the one-monopoly-rent and complementary-efficiencies theorems, often asserted in the context of vertical antitrust analysis).

85. Herbert J. Hovenkamp, *Robert Bork and Vertical Integration: Leverage, Foreclosure, and Efficiency*, 79 ANTITRUST L.J. 983, 995–96 (2014) (describing BORK, *supra* note 57, at 236–37).

86. *See, e.g.*, Patrick Bolton & Michael D. Whinston, *The "Foreclosure" Effects of Vertical Mergers*, 147 J. INSTITUTIONAL & THEORETICAL ECON. 207, 225 (1991) (describing scholarship that "has formally demonstrated that vertical mergers resulting in market foreclosure can indeed be an equilibrium phenomenon"); Jay Pil Choi & Sang-Seung Yi, *Vertical Foreclosure with the Choice of Input Specifications*, 31 RAND J. ECON. 717, 718 (2000); Hart & Tirole, *supra* note 74, at 205–06; Michael H. Riordan, *Anticompetitive Vertical Integration by a Dominant Firm*, 88 AM. ECON. REV. 1232, 1233 (1998).

87. *See* Richard A. Posner, *The Chicago School of Antitrust Analysis*, 127 U. PA. L. REV. 925, 937 (1979).

the CFAA is invoked to prevent a downstream competitor such as hiQ from accessing an input such as LinkedIn data, input foreclosure occurs by definition, since the effect of the CFAA is to enjoin and even criminalize access to that input.[88] The competition harms of input foreclosure are thus at their apex when the CFAA is used to cut off startups and other users of data platforms.

C. Increasing Transaction Costs

The CFAA, broadly construed, also enables companies to impair competition by introducing unnecessary transaction costs and limiting consumer choice.

The quintessential example of a tool that enhances consumer choice is a price comparison service: one that aggregates prices across multiple vendors to allow consumers to make optimal choices. Transaction costs stymie economic efficiency,[89] and finding the best price is a significant transaction cost known as "search cost," so tools for price comparison facilitate efficient markets.[90]

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.[91] Southwest Airlines objected, claiming that the fares listed on its public website were "proprietary" and that automated collection of fare data was unauthorized under the Use Agreement on Southwest's website.[92] 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 their access was unauthorized," and therefore Southwest had stated a claim under the CFAA.[93] Southwest is far from the only company to have invoked the CFAA to limit price comparison services from accessing data: multiple cases have similarly held that collection of computerized public pricing data can violate the CFAA where contractual terms prohibit such collection.[94]

Blocking of price comparison services damages consumer welfare by increasing consumers' costs of searching for the best

88. *See* 18 U.S.C. §§ 1030(a)–(c), (g) (West, Westlaw through P.L. 116–259).

89. *See* R.H. Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1, 16 (1960).

90. *See* J. Yannis Bakos, *Reducing Buyer Search Costs: Implications for Electronic Marketplaces*, 43 MGMT. SCI. 1676, 1677 (1997).

91. *See* 318 F. Supp. 2d 435, 437 (N.D. Tex. 2004).

92. *See id.* at 437.

93. *Id.* at 440.

94. *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).

deal.[95] Economists use the term "obfuscation" for activities that heighten search costs, and find that obfuscation can "increase average markups and the fraction of consumers buying from relatively high-priced firms."[96] "[L]owering search costs[] will unambiguously increase social welfare," so blocking services that lower search costs will decrease welfare.[97] Regarding airlines like Southwest 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."[98] Across six different markets, the study found that cutting off online price comparison services could raise prices by 10–15%.[99]

Nevertheless, companies face strong incentives to leverage legal tools such as the CFAA to limit price comparison shopping.[100] For example, Southwest Airlines was able to raise its prices over competitors, sometimes by over 20%, by refusing to be listed on price comparison services.[101] Propensity to obfuscate price comparisons is also apparent from another strategy that companies use to thwart price comparison services: "drip" or "partitioned" pricing, in which a vendor (such as a hotel) advertises a low base price but then "drips" on mandatory additional costs (such as resort fees).[102] Drip pricing is effective in part because online price comparison services often report only the base price and not the add-on fees, so consumers shopping for the lowest price are duped

95. *See generally* Sara Fisher Ellison, *Price Search and Obfuscation: An Overview of the Theory and Empirics*, *in* HANDBOOK ON THE ECONOMICS OF RETAILING AND DISTRIBUTION 287, 287–88 (Emek Basker ed., 2016).

96. Glenn Ellison & Sara Fisher Ellison, *Search, Obfuscation, and Price Elasticities on the Internet*, 77 ECONOMETRICA 427, 430 (2009).

97. Dale O. Stahl II, *Oligopolistic Pricing with Sequential Consumer Search*, 79 AM. ECON. REV. 700, 709 (1989).

98. FIONA SCOTT MORTON, BENEFITS OF PRESERVING CONSUMER'S ABILITY TO COMPARE AIRLINE FARES VIA OTAS AND METASEARCH SITES 3, 57 (2015).

99. *See id.* at 53.

100. *See* Glenn Ellison & Alexander Wolitzky, *A Search Cost Model of Obfuscation*, 32 RAND J. ECON. 417, 435 (2012); Rory Van Loo, *Digital Market Perfection*, 117 MICH. L. REV. 815, 837 (2019).

101. *See* Volodymyr Bilotkach, *Reputation, Search Cost, and Airfares*, 16 J. AIR TRANSPORT MGMT. 251, 253 tbl.2 (2010).

102. *See* Gorkan Ahmetoglu, Adrian Furnham & Patrick Fagan, *Pricing Practices: A Critical Review of Their Effects on Consumer Perceptions and Behaviour*, 21 J. RETAILING & CONSUMER SERV. 696, 697 (2014). The two terms differ in that "drip" pricing separates the base price from the fees temporally (e.g., a resort fee announced only when the traveler checks into the hotel); "partitioned" pricing may be known simultaneous to the base price but is not presented to the prospective buyer in a unified sum (e.g., a sales tax not shown on a price tag).

into ultimately paying more.[103] That practice is sufficiently pervasive and harmful that the Federal Trade Commission held a full-day conference to investigate how drip pricing "harms consumers and reduces competition."[104] Competition authorities in multiple other countries have similarly considered whether such strategies constitute unfair or deceptive practices.[105] If interfering with price comparison and increasing search costs through drip pricing is a problem for competition, then it must be equally problematic for competition to invoke the CFAA to block price comparison services entirely.

Price comparison tools are just one of many welfare-enhancing services with which the CFAA could interfere.[106] 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.[107] In response, software developers have built tools to combat this loss of privacy by blocking Internet transactions that facilitate online tracking.[108] Such software has received tremendous praise and

---

103. *See* Christopher Elliott, *Why do travelers still fall for drip pricing?*, WASH. POST (Aug. 12, 2020, 10:00 AM), https://www.washingtonpost.com/lifestyle/travel/why-do-travelers-still-fall-for-drip-pricing/2020/08/12/ebd3d720-ca78-11ea-b0e3-d55bda07d66a_story.html [https://perma.cc/AXW7-EKZL].

104. *See* U.S. FED. TRADE COMM'N, A CONFERENCE ON THE ECONOMICS OF DRIP PRICING 4 (2012) (statement of FTC Chairman Jon Leibowitz).

105. *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).

106. A further example is the "plethora of third-party services have arisen which arguably address the privacy and data concerns of Facebook's end users," which some commentators have worried could be blocked under the *Power Ventures* decision. *See* Venkat Balasubramani, *EFF Weighs in on Facebook v. Power Ventures*, TECH. & MKTG. L. BLOG (May 27, 2010), https://blog.ericgoldman.org/archives/2010/05/eff_weighs_in_o.htm [https://perma.cc/59MV-MDWA].

107. *See, e.g.*, David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSP. 37, 55–58 (2009); *See* Latanya Sweeney, *Discrimination in Online Ad Delivery*, 11 AMC QUEUE No. 3, at 44 (Mar. 2013) (observing patterns of racial discrimination in online advertising).

108. 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 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, e.g.*, Cory Doctorow, *Adblocking: How About Nah?*, ELEC. FRONTIER FOUND. (July 25, 2019), https://www.eff.org/deeplinks/2019/07/adblocking-how-about-nah [https://perma.cc/KW4D-3W6M]. 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, Richard Garnier & Kensuke Fukuda, *A Comparison of Web Privacy Protection Techniques*, 144 COMPUT. COMM. 162 (2019).

widespread usage.[109] Nevertheless, online advertisers unsurprisingly dislike privacy-enhancing software and have used terms of service to prohibit its use—terms of service that could be powerfully enforced under the broad construction of the CFAA.[110]

Examples such as these have led commentators to conclude that the CFAA "limit[s] the valid tools consumers need to protect themselves online."[111] 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.

II. INTELLECTUAL PROPERTY, COMPETITION, AND THE CFAA

The tension between the CFAA and competition policy may also be understood from the perspective of intellectual property. Two insights drive the usefulness of this perspective. First, the CFAA has much in common with intellectual property regimes.[112] Second, intellectual property theory has long been concerned with competition policy and antitrust law, and in particular, exclusions from intellectual property protections generally reflect legislative judgments about competition policy.[113] As a result, the analysis below reveals how discrepancies between the CFAA and intellectual property regimes, specifically information that is protected under the CFAA but excluded under intellectual property laws, are revealing as to competition concerns with the CFAA.

---

109. *See* Doc Searls, *Beyond ad blocking—the biggest boycott in human history*, DOC SEARLS WEBLOG (Sept. 29, 2015), https://blogs.harvard.edu/doc/2015/09/28/beyond-ad-blocking-the-biggest-boycott-in-human-history/ [https://perma.cc/P4L2-QDAC].

110. *See, e.g.*, Dami Lee, *Spotify bans ad blockers in updated terms of service*, THE VERGE (Feb. 7, 2019, 3:41 PM), https://www.theverge.com/2019/2/7/18215845/spotify-ad-blockers-terms-of-service [https://perma.cc/DU63-X4ER]; *cf.* Anastasia Shuba, Athina Markopoulou & Zubair Shafiq, *NoMoAds: Effective and Efficient Cross-App Mobile Ad-Blocking*, PROCEEDINGS ON PRIVACY ENHANCING TECHS., 126 (2018) (noting possible relevance of and lack of case law on the CFAA).

111. Ashkan Soltani, *Protecting Your Privacy Could Make You the Bad Guy*, WIRED (July 23, 2013, 9:30 AM), https://www.wired.com/2013/07/the-catch-22-of-internet-commerce-and-privacy-could-mean-youre-the-bad-guy/ [https://perma.cc/KT3R-75WF].

112. *See supra* notes 30–33 and accompanying text.

113. For general overviews of the relationship between intellectual property and competition policy, *see, e.g.*, Shubha Ghosh, *Intellectual Property Rights: The View from Competition Policy*, 103 NW. U. L. REV. COLLOQUY 344, 344–47 (2009); Herbert Hovenkamp, *The Intellectual Property–Antitrust Interface*, *in* 3 ISSUES IN COMPETITION L. & POL'Y 1979 (2008); FED. TRADE COMM'N, TO PROMOTE INNOVATION: THE PROPER BALANCE OF COMPETITION AND PATENT LAW AND POLICY ch. 1 (2003).

Though intellectual property comes in many forms,[114] particular attention is given to two: trade secrets and copyrights. These two systems are chosen because the protection they offer are the most akin to the ways in which the CFAA has been used to date; indeed, many civil cases brought under the CFAA include trade secret and copyright infringement allegations as well.[115] Trade secrets and copyrights are useful for a second reason: the two legal regimes have been tied together in legislation. In particular, certain critical amendments to the CFAA were enacted in tandem with trade secrets legislation and borrowed text from copyright law.[116] Accordingly, the discussion below compares the CFAA to trade secret and copyright law, and then reviews the relevant relationships found in the legislative history.

A. Trade Secrets

Trade secret law illuminates how the broad construction of the CFAA interferes with competition policy. The broad construction effectively allows firms to protect public information as if it were a trade secret, and the limitation of trade secret protection to nonpublic information is intended to promote competition.

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.[117] However, those powerful remedies are carefully balanced against key limitations of trade secret law, in view of competition concerns. Information generally known to the public cannot be a trade secret.[118] 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

---

114. Others include utility patents, design patents, trademarks, and rights of publicity. *See generally* Gary M. Ropski & Michael J. Kline, *A Primer on Intellectual Property Rights: The Basics of Patents, Trademarks, Copyrights, Trade Secrets and Related Rights*, 50 ALB. L. REV. 405, 405 (1986).

115. *See, e.g.*, hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 992 (9th Cir. 2019) (noting assertion of the Digital Millennium Copyright Act along with the CFAA); EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577, 580 (1st Cir. 2001); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1122 (W.D. Wash. 2000); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1326–27 (N.D. Ga. 2007); I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 523 (S.D.N.Y. 2004).

116. *See infra* Section II.C.

117. *See* 18 U.S.C. § 1836(b)(3) (West, Westlaw through P.L. 116–259) (damages and injunctive relief); § 1836(b)(2) (civil seizure); 18 U.S.C § 1832 (West, Westlaw through P.L. 116–259) (criminal penalties).

118. *See* 18 U.S.C. § 1839(3)(B) (West, Westlaw through Pub. L. 116–259); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974).

of trade secrets.[119] Courts have often held that mere contractual provisions, not backed by technical measures or substantial enforcement capacity, fail to be "reasonable measures."[120]

A narrow construction of the CFAA is 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. The firm would thus enjoy trade secret-like remedies without meeting the requirements for trade secret protection.

Consider, for example, the *Southwest Airlines* case described above.[121] Southwest Airlines could prevent its airfares from being listed on price comparison services by treating those airfares as trade secrets.[122] 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.[123] 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.[124] 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.

That the CFAA provides broader protection than trade secret law is not enough to answer the normative question of whether it should; it is possible that trade secret law is inadequate and the broader level of protection under the CFAA is in fact "preferable" as

119. 18 U.S.C. § 1839(3)(A).

120. *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).

121. *See supra* text accompanying notes 91–94.

122. *See, e.g.*, Sw. Stainless, LP v. Sappington, 582 F.3d 1176, 1189 (10th Cir. 2009) (treating price lists as trade secrets).

123. *See, e.g.*, Colo. Supply Co. v. Stewart, 797 P.2d 1303, 1306 (Colo. App. 1990) (affirming that published price lists are not trade secrets).

124. Defiance Button Mach. Co. v. C & C Metal Prods. Corp., 759 F.2d 1053, 1063–64 (2d Cir. 1985).

several commentators have claimed.[125] Answering that normative question requires reference to the rationale behind limiting trade secrets, and that rationale is competition. The limits of trade secret protection are designed "to strike the classic balance between free competition on one hand and the prevention of unfair competition on the other."[126] The Supreme Court recognized the role of those limitations in preserving competition in *Kewanee Oil Co. v. Bicron Corp.*[127] There, the Court considered the argument that federal patent law preempted state trade secret protection.[128] To answer that question, the Court began with the premise that patent law was designed to encourage disclosure of inventions so that all competitors may make use of them freely after expiration of any granted patents.[129] Since trade secret protection arguably dissuaded some inventors from making that disclosure, the argument in favor of preemption was that trade secret protection thwarted the congressional patent scheme favoring disclosure of and subsequent competitive use of inventions.[130] The Supreme Court disagreed in large part because trade secret law, by virtue of its numerous limitations, "provides far weaker protection in many respects than the patent law."[131] That weaker protection meant, according to the Court, that there was a "substantial risk that the secret will be passed on to . . . competitors" either illicitly or through permissible reverse engineering.[132] In other words, the limitations of trade secret protection allowed the Court to conclude that trade secrets would have minimal effect on Congress's design of making technologies open to competition.

Certainly, it may not be the case that every legislature has set precisely the correct level of trade secret protection, but as *Kewanee Oil* recognizes, at least some degree of limitation to the scope of trade secrets is necessary to avoid unduly interfering with competition. The CFAA, broadly construed, contains none of the limitations of trade secret protection and enables an effective trade secret–like remedy for public information; in so doing, that broad construction is improperly contrary to the balancing of competition interests found in trade secrets law.

---

125. Manion, *supra* note 32, at 304; *see also* references cited *supra* note 32.

126. 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).

127. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).

128. *See id.* at 472.

129. *See id.* at 480–81.

130. *See id.* at 482 (quoting Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225, 232 (1964)) (considering whether state trade secret law "might constitute 'too great an encroachment on the federal patent system to be tolerated'").

131. *Id.* at 489–490.

132. *Id.* at 490.

B. Copyright

Like trade secrets, copyrights enable firms to prevent competitors from using proprietary information. 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.[133] However, not all acts of copying are proscribed. Copyright protection applies only to expressive elements of works, not underlying facts.[134] Copyright inures to the author of the information, even if the information is possessed by someone else.[135] 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.[136] Finally, the Constitution mandates that copyrights subsist only "for limited times."[137]

The CFAA, broadly construed, subverts all these elements of copyright law. Cases such as *Southwest Airlines* demonstrate uses of the CFAA to prevent copying of uncopyrightable factual information such as price lists.[138] *Power Ventures* involved assertion of the CFAA to protect data authored by third parties—indeed, third parties who consented to the copying.[139] 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."[140] 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

133. *See* 17 U.S.C. § 102(a) (1976).

134. *See* 17 U.S.C. § 102(b); Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344–45 (1991) (quoting Harper & Row, Publishers, Inc. v. Nat'l Enterprises, 471 U.S. 539, 556 (1985)).

135. *See* 17 U.S.C. § 201(a) (1976).

136. *See* 17 U.S.C. § 107 (1976); Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 576–78 (1994).

137. U.S. CONST. art. I, § 8, cl. 8; *see* 17 U.S.C. § 302 (Westlaw through Pub. L. 116–259).

138. *See supra* note 91.

139. *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1063 (9th Cir. 2016).

140. Wolfe, *supra* note 12, ¶ 5, at 303.

used, and may then assert the CFAA against undesirable uses, whether or not those uses would be copyright infringements.[141]

That the CFAA, construed broadly, can reach beyond the limits Congress explicitly set in the copyright statutes again demonstrates the anticompetitive effect of that construction. The traditional limitations of copyright law have long reflected a "balance of competing claims upon the public interest," including "promoting broad public availability of literature, music, and the other arts."[142] Those appeals to the public interest reflect a competition concern: copyright protection, like other intellectual property, excludes others from making productive uses of copyrighted works and thereby, at least in the short term, introduces static inefficiencies that reduce consumer welfare.[143] The overall aim of copyright protection is to promote the creation of new works that, in the long run, increase consumer welfare through dynamic efficiency, and the various exceptions and limitations to copyright protection "minimize copyrights potential harm to static competition" and "ensure that it is not used to harm dynamic competition."[144] Thus, insofar as broad construction of the CFAA "upset[s] the careful balance that the Copyright Act has struck between authors and society,"[145] that broad construction interferes with the balance of competitive interests that Congress set in enacting copyright law.

Copyright law has long concerned itself with avoiding expansive intellectual property protections that go "beyond the limits of [the] specific grant" of copyright.[146] To allow an unrelated criminal law—a computer trespass statute, no less—to render the copyright statutes practically superfluous would effectively open a

141. In *Explorica*, the district court found that access to a website was unauthorized under the CFAA based on a copyright notice on the website. *See* EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577, 580 n.6 (1st Cir. 2001). The tour pricing information that was accessed, however, was factual and almost certainly not copyrightable. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 347–48 (1991). Perhaps recognizing this discrepancy, the First Circuit on appeal took no position on the district court's reliance on the copyright notice to determine whether access was authorized. *See Explorica*, 274 F.3d at 583 n.16.

142. Fogerty v. Fantasy, Inc., 510 U.S. 517, 526 (1994) (quoting Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975)).

143. Ariel Katz, *Copyright and Competition Policy*, *in* HANDBOOK OF THE DIGITAL CREATIVE ECONOMY 209, 209 (Ruth Towse & Christian Handke eds., 2013); *see* Marcel Boyer, *Efficiency Considerations in Copyright Protection*, 1 REV. ECON. RES. COPYRIGHT ISSUES 11, 19 (2004).

144. Katz, *supra* note 143, at 210.

145. Galbraith, *supra* note 9, at 365.

146. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 441 (1984). Though the Supreme Court made that statement with respect to patent law, it recognized in the immediately following paragraph that the principle applied equally to copyright law. *See id.* at 442.

back door for circumventing longstanding judicial precedents designed to protect competitive markets.

C. *Intellectual Property in the CFAA's Legislative History*

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.

As enacted in 1984 and amended in 1986, the CFAA applied only to a limited class of "Federal interest" computers and information; any competition concerns with the statute would have been limited to this narrow class.[147] The key provisions rendering the CFAA applicable to computers generally, such that private competition would be a relevant concern under the statute, appear in the National Information Infrastructure Protection Act of 1996.[148] 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.[149] The provisions of Title I included all of the careful balancing elements discussed above.[150] 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.[151]

The drafters of the 1996 CFAA amendments were also keenly aware of copyright law, indeed borrowing the latter's text.[152]

147. As initially enacted, the CFAA covered only national security–sensitive information, financial records, and government computers. *See Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 §1030(a)(1)–(3), 18 U.S.C §1030* (West, Westlaw through P.L. 116–259). It was subsequently expanded to include offenses related to "Federal interest computer[s]" and password trafficking. Computer Fraud and Abuse Act of 1986 §2(d), 18 U.S.C. § 1030 (1986). Federal interest computers included non-governmental networks of computers connected across different states, *see id.* § 2(g)(4), but "[a]t a time when use of the Internet remained in its infancy, few crimes would have been included in [the statute's] reach." Kerr 2010, *supra* note 17, at 1565. A 1994 amendment to the CFAA did not affect the statute's scope substantially. *See id.* at 1566.

148. *See* 18 U.S.C. § 1030; Kerr 2010, *supra* note 17, at 1568 (discussing how, under the 1996 amendment, "every computer connected to the Internet is a 'protected computer' covered by 18 U.S.C. § 1030").

149. *See* Economic Espionage Act of 1996, 18 U.S.C. § 1831 (1996).

150. *See, e.g.*, 18 U.S.C § 1893(3)(A)–(B) (1996).

151. 142 CONG. REC. 27,116–20 (1996) (statement of Sen. Kohl).

152. *See* 18 U.S.C. § 1030(c)(2)(B)(i) (using test from 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."[153] 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."[154]

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).[155] 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," suggesting that they recognized the importance of balancing competition interests at the time the CFAA was being debated.[156] To be sure, the report acknowledges correctly that the CFAA provides additional causes of action for "theft of intangible information."[157] 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.[158] Because the CFAA contains no limitations parallel to those found in trade secrets or copyright law, it does not merely strike the wrong balance with respect to competition; it ignores the necessary balance entirely.

---

153. S. REP. NO. 104-357, at 7.

154. *Id.* at 7–8.

155. *Id.* at 4; *see* United States v. Nosal, 676 F.3d 854, 857 & n.3 (9th Cir. 2012) (en banc).

156. 142 CONG. REC. 27,116 (1996) (statement of Sen. Kohl). While that statement was made with respect to the Title I trade secret provisions of the EEA rather than the Title II amendments to the CFAA, it seems unlikely that the bill's sponsors would have intended Title II to have a policy consequence directly contrary to the aims of Title I.

157. S. REP. NO. 104-357 at 7.

158. *See* 17 U.S.C. §§ 902(a)(1), 1301(a)(1) (Westlaw through Pub. L. 116–259).

III. NARROWER CONSTRUCTIONS OF THE CFAA

The conflict between the CFAA and competition policy is not inherent to the statute itself, but largely a product of the broad construction taken by several federal courts of appeals, under which violations of conditions on how information is to be used constitute access "without authorization" under the CFAA.[159] Because the broad construction allows a computer operator to set unilateral terms that render access to computer information "unauthorized," that construction 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.[160]

Competition in technology markets is better protected by narrower constructions of the CFAA. At least two such narrower constructions have been proposed, one of which uses an entitlement-based test and the other of which uses a code-based test.

Under the entitlement-based 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.[161] The advantage of this test with respect to competition policy is that 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 entitles the former class of users to access information cannot leverage the CFAA to nevertheless close itself off to the latter competitive uses.[162]

---

159. *See* cases cited *supra* note 7.

160. *See supra* Section I.

161. *See* Brief for Petitioner at 17, Van Buren v. United States, No. 19-783 (U.S. July 1, 2020); United States v. Valle, 807 F.3d 5087, 511–12 (2d Cir. 2015).

162. Theoretically, the computer operator could grant authorization on an individual basis, evaluating each prospective user for likelihood of being a competitor and denying access to them. Indeed, in many cases, computer operators have blocked specific computers by their numeric Internet Protocol addresses, to keep competitors or unwanted users out. *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1068 (9th Cir. 2016); Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969 (N.D. Cal. 2013); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1062 (N.D. Cal. 2000). This approach is likely to be of limited utility, for two reasons. First, users are not readily and permanently identifiable, especially online; a competitor could easily change IP addresses or hire third-party users to query data on its behalf. *See, e.g.*, *Power Ventures*, 844 F.3d at 1068, 1068 n.5; *Craigslist*, 942 F. Supp. 2d at 970. Second, as a general matter, computer operators must establish prospective rules of access well in advance of

The code-based test assesses authorization under the CFAA by whether a computer user circumvented an access restriction implemented in computer software code.[163] This test more strongly guards against anticompetitive behavior. As seen in the examples of cases 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.[164] This post hoc revocation of access by mere legal notification would not be possible under a code-based test which would require the computer operator to reconfigure the computer to block the undesired competitor from access.

A computer operator could perhaps implement a technological restriction on access by a competitor or undesirable user, for example by blocking a specific IP address. Circumventing such a restriction may be a CFAA violation.[165] These sorts of technical restrictions will be of limited utility because identifying specific computer users is often difficult.[166] Nevertheless, it is worth recognizing that even a narrow construction of the CFAA cannot fully prevent the statute from being asserted to anticompetitive ends.

But forcing firms to employ technological restrictions rather than terms of use to suppress competition has several advantages with respect to competition policy. Technological blocking is more difficult to implement than writing a cease-and-desist letter, and increasing the costs of competition-suppressing behavior reduces the likelihood that firms will engage in it.[167] Technological restrictions, unlike cease-and-desist letters, have the potential to be erroneously overbroad such that they block access by legitimate users, meaning that they may attract greater public scrutiny.[168]

---

users accessing a computer, so real-time assessment of whether a user is a competitor will be virtually impossible. *See* Grimmelmann, *supra* note 13, at 1503–04. Of course, a computer operator could retrospectively deny access to a small handful of especially undesirable competitors; this possibility is discussed *infra* notes 165–168.

163. *See, e.g.*, Kerr 2003, *supra* note 5, at 1649; Bellia 2016, *supra* note 6, at 1444.

164. *See, e.g.*, *Power Ventures*, 844 F.3d at 1067; hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 992 (9th Cir. 2019); Sw. Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 440 (N.D. Tex. 2004).

165. *See Craigslist*, 942 F. Supp. 2d at 969–70. *But see* Kerr 2016, *supra* note 9, at 1168–69 ("Merely circumventing an IP block does not violate trespass norms.").

166. *See supra* text accompanying note 162.

167. *See* Creighton et al., *supra* note 59, at 981 ("[I]t seems logical to expect that rational firms would prefer, all else equal, exclusionary strategies that are both low-cost and that provide a strong upside, including the opportunity to acquire relatively durable market power.").

168. *Cf.* Benjamin Edelman, *Web Sites Sharing IP Addresses: Prevalence and Significance*, BERKMAN CTR. FOR INTERNET & SOC'Y (Sept. 12, 2003), https://cyber.harvard.edu/archived_content/people/edelman/ip-sharing/ [https://perma.cc/5SQW-QLJE] (noting prevalence of IP addresses shared across multiple websites).

And enforcement of antitrust law is more feasible against technological measures than against CFAA-backed terms of use because the latter may raise *Noerr–Pennington* issues.[169] By requiring firms seeking to undermine competition to use technological approaches rather than terms of use, the code-based construction of the CFAA helps to ensure that anticompetitive conduct is more costly, more visible, and easier to prosecute.

CONCLUSION

Competition policy is a worthwhile frame for studying a wide variety of matters in technology law and policy[170] and the CFAA should be no different. This article considered the CFAA's effects on competition by juxtaposing cases brought under that statute against contemporary problems in antitrust policy, such as interoperability, input foreclosure, and price obfuscation. It further used the perspective of intellectual property and antitrust to highlight ways in which the CFAA goes past accepted norms and legislative decisions on the proper balance of laws to preserve competitive markets.

Based on these observations, the article concludes that narrower constructions of the CFAA are preferable, at least with respect to competition policy. Certainly, the proper construction of the statute must turn on further considerations as well.[171] But insofar as the competitive effects of the CFAA have not been considered in detail so far, it is hoped that the present analysis can help to enrich future consideration of the CFAA. More broadly, the CFAA appears to be one example in a larger trend of using public interest statutes to inhibit competition and protect dominant firms' incumbency.[172] The exercise of considering how seemingly unrelated laws like the CFAA can be used to limit competition

169. More specifically, the *Noerr–Pennington* doctrine generally provides that the bringing of a colorable legal action in court cannot be deemed illegal activity under the antitrust laws. *See* Prof'l Real Est. Inv'rs, Inc. v. Columbia Pictures Indus., 508 U.S. 49, 56 (1993) (discussing E.R.R. Presidents Conference v. Noerr Motor Freight, 365 U.S. 127, 136–38 (1961)); United Mine Workers of Am. v. Pennington, 381 U.S. 657, 669 (1965). Several courts have held that threat letters in preparation for litigation are similarly immunized under that doctrine. *See, e.g.*, Sosa v. DirecTV, Inc., 437 F.3d 923, 942 (9th Cir. 2006); Primetime 24 Joint Venture v. Nat'l Broad. Co., 219 F.3d 92, 100 (2d Cir. 2000). While those cases did not involve the CFAA, they suggest that cease-and-desist letters prior to bringing a CFAA action may be immune to antitrust scrutiny under the *Noerr–Pennington* doctrine.

170. For another example by this article's author, *see* Duan 2020, *supra* note 53, at 394–99.

171. *See supra* notes 9–21 and accompanying text.

172. This is Bork's observation about "[p]redation by abuse of governmental procedures." *See* BORK, *supra* note 57, at 347.

would seem a fruitful exercise for those who hope to preserve competitive markets.

Just before this article went to press, the Supreme Court issued its decision in *Van Buren v. United States*.[173] Essentially adopting the narrow construction of the Computer Fraud and Abuse Act, the Court held that a then–police sergeant's search of the department's license plate database for unauthorized personal gain did not constitute "exceed[ing] authorized access" under the law.[174] Primarily relying on construction of the CFAA's text, the Court concluded that a violation of the statute occurs only when one accesses "information that a person is not entitled to obtain by using a computer that he is authorized to access,"[175] rejecting the government's contention that access for an unauthorized purpose constitutes a violation.[176] Bolstering that narrow construction of the law was the Court's policy concern that "the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity," such that "millions of otherwise law-abiding citizens [would be] criminals."[177]

The Court's adoption of the narrow construction of the CFAA goes a long way toward avoiding anticompetitive misuse of the statute, but it does not prevent such misuse completely. Under the decision, computer services cannot leverage the CFAA to enforce terms of use that disallow accessing data for purposes of building competitive services.[178] However, the Court specifically declined to adopt a code-based test, suggesting that terms of use that wholly exclude certain competitors from accessing data are still enforceable under the CFAA.[179] Such wholesale exclusion of competitors is not uncommon, as seen from the cases reviewed in this article.[180] As a result, the CFAA will continue to be an area ripe for discussion with respect to competition and antitrust policy in the foreseeable future.

173. *See* No. 19-783 (U.S. June 3, 2021).
174. *See Van Buren*, No. 19-783, slip op. at 3–4, 20.
175. *Van Buren*, No. 19-783, slip op. at 8.
176. *See Van Buren*, No. 19-783, slip op. at 7.
177. *Van Buren*, No. 19-783, slip op. at 17–18.
178. *See supra* text accompanying notes 159–160.
179. *See Van Buren*, No. 19-783, slip op. at 13 n.8; *supra* text accompanying notes 161–168.
180. *See supra* Section I.