Digital Gatekeepers

Thomas E. Kadri*

If in William Blackstone's time we might have thought of a person's home as their castle, in Mark Zuckerberg's time we might say that their website is too. Under cyber-trespass laws like the Computer Fraud and Abuse Act, courts have treated online platforms as digital gatekeepers—as property owners that may permit and restrict access to websites much like landowners may do with private land in the real world. If platforms withhold their consent through words or inference, cyber-trespass laws let them enforce their preferences about who may access their services and gather information from the internet. Concerned about reputations and profits, platforms have deployed their gatekeeper rights to scare and sue those seeking to use their websites against their wishes. This legal regime affects all sorts of actors—from academics to journalists to businesses to consumers—who want to engage with the platforms' websites, even when they're open to the public or when people permit complementary services to access their accounts.

This Essay challenges the law's current embrace of gatekeeper rights. Applying cyber-trespass law across the entire internet has empowered private platforms to become public policymakers in unintended and unchecked ways. But it's not too late to adopt a different legal regime—one that defers far less to private companies to establish and enforce the internet's accessibility and informational rules. This Essay offers a three-part legislative framework to restrain the power of digital gatekeepers. To begin, Congress should clarify that cyber-trespass laws don't apply on websites that are accessible to the general public. Congress should then mandate and shield certain forms of interoperability between platforms. Finally, Congress should pass targeted laws to regulate the collection and use of publicly accessible information on websites. Taking these steps will change the locus of governance in key internet policy choices, stripping private platforms of the unbounded and trans-substantive decisionmaking power they currently enjoy. Although this regulatory agenda is ambitious, these are the kinds of fundamental and structural changes needed to protect privacy, speech, and consumer interests in the digital age.

---

* Assistant Professor, University of Georgia School of Law. I'm grateful for generous and insightful feedback from Jack Balkin, Jane Bambauer, Elettra Bietti, Gordon Bottomley, Nathan Chapman, Ignacio Cofone, Harlan Cohen, Cory Doctorow, Evelyn Douek, MJ Durkee, Michal Gal, Ben Gifford, Jack Goldsmith, James Grimmelmann, Nikolas Guggenberger, Sarah Haan, Woody Hartzog, Claudia Haupt, Don Herzog, Margot Kaminski, Daphne Keller, Orin Kerr, Mark Lemley, Michael Lwin, Sandy Mayson, Joe Miller, Przemek Pałka, Caio Mario da Silva Pereira Neto, Nate Persily, Jonathan Peters, Natália Pires de Vasconcelos, Robert Post, Alan Rozenshtein, Laurent

Don't let the fox guard the henhouse.
Don't assign a job to someone who will then
be in a position to exploit it for his own ends.[1]

Introduction

Everyone's agonizing over how to "fix" social media.[2] After a steady stream of scandals that shows no sign of abating, there's anger that online

Sacharoff, Alex Stamos, Nicolas Suzor, Christian Turner, Mariana Valente, and Rory Van Loo, and for helpful discussions after presentations at the University of Georgia School of Law, Insper São Paulo, the University of Minnesota Law School, Stanford University, and Yale Law School.

1. GREGORY TITELMAN, RANDOM HOUSE DICTIONARY OF POPULAR PROVERBS AND SAYINGS 68 (1996).

2. *See, e.g.*, MIKE GODWIN, THE SPLINTERS OF OUR DISCONTENT: HOW TO FIX SOCIAL MEDIA AND DEMOCRACY WITHOUT BREAKING THEM 80 (Charles Duan ed., 2019) (noting a "growing sentiment among commentators that there's something out of control with social media and internet companies that needs to be brought back into control"); Jamie Condliffe, *How to Fix Social Media's Big Problems? Lawmakers Have Ideas*, N.Y. TIMES (July 30, 2018), https://www.nytimes.com/2018/07/30/business/dealbook/big-tech-regulation-ideas.html [https://perma.cc/KQN4-BLAE] (discussing reports from the U.S. Senate and British House of Commons that both advocated for new regulations of large tech companies, such as mandatory audits, liability for failures to take down illegal content, and duties to remove fake accounts); Daniel Kreiss & Matt Perault, *Four Ways to Fix Social Media's Political Ads Problem—Without Banning Them*, N.Y. TIMES (Nov. 16, 2019), https://www.nytimes.com/2019/11/16/opinion/twitter-facebook-political-ads.html [https://perma.cc/ZSC7-7JW4] (recommending "four common-sense changes to political advertising" on social media, including "clear[er] enforcement mechanisms for violations of targeting policies"). *But see* SIVA VAIDHYANATHAN, ANTISOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY 9 (2018) (questioning whether Facebook can be reformed because "the problem with Facebook is Facebook"); JARON LANIER, TEN ARGUMENTS FOR DELETING YOUR SOCIAL MEDIA ACCOUNTS RIGHT NOW 22 (2018) (asserting that quitting social media "entirely is the only option for change").

platforms seem complicit in all sorts of social ills.[3] And following years of laissez-faire attitudes in legislatures, lawmakers are looking for ways to regulate the technology companies that exert so much influence over our lives.

Given that the "techlash" shows little sign of subsiding, reining in giant online platforms might be our best hope for bipartisanship.[4] When Senators Elizabeth Warren and Ted Cruz agree on something, it's worth taking note.[5] Even Facebook founder Mark Zuckerberg has conceded that the internet "needs new rules."[6]

Federal politicians in the United States have so far failed to turn their outrage into action, but federal judges have begun undermining an important source of platform power. On the West Coast in California, a federal appeals court issued a long-awaited ruling in *hiQ v. LinkedIn*,[7] giving a scrappy start-up a win over a Big Tech behemoth.[8] Meanwhile, on the East Coast in Washington, D.C., a federal district court decided *Sandvig v. Barr*,[9] freeing academics and journalists to conduct research that platforms have tried

3. For my purposes, I adopt Tarleton Gillespie's definition of "platforms" as being online sites and services that "host, organize, and circulate users' shared content or social interactions for them," without having produced the bulk of that content themselves, built on an infrastructure for processing data for "customer service, advertising, and profit." TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET 18 (2018). While many of the rules, analyses, and recommendations in this Essay would apply to all online sites and services, I've generally chosen to highlight platforms for three reasons. First, "Big Tech" platforms like Facebook, Twitter, and Amazon have gained significant influence in our society and, as a result, have attracted the interest of the legislators and researchers who are among my primary audiences. Second, these platforms have been particularly aggressive in enforcing their rights as digital gatekeepers under cyber-trespass law. And third, my recommendations regarding interoperability are most relevant to the types of platforms that host third-party content, including in online groups and messaging services.

4. *See* Rana Foroohar, *Year in a Word: Techlash*, FIN. TIMES (Dec. 16, 2018), https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e [https://perma.cc/N9MQ-BVZV] (defining "techlash" as "[t]he growing public animosity towards large Silicon Valley platform technology companies and their Chinese equivalents").

5. Ben Brody, *Ted Cruz Echoes Elizabeth Warren's Criticism of Facebook's Power*, BLOOMBERG (Mar. 12, 2019, 2:25 PM), https://www.bloomberg.com/news/articles/2019-03-12/ted-cruz-retweets-elizabeth-warren-s-criticism-of-facebook-power [https://perma.cc/578X-ZZZA].

6. Mark Zuckerberg, *Mark Zuckerberg: The Internet Needs New Rules. Let's Start in These Four Areas*, WASH. POST (Mar. 30, 2019, 2:00 PM), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html [https://perma.cc/MT6D-MLCH].

7. 938 F.3d 985 (9th Cir. 2019).

8. *Id.* at 1005.

9. 451 F. Supp. 3d 73 (D.D.C.), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020).

to block.[10] Experts agree that these "bombshell"[11] decisions are "groundbreaking" and "a really big deal."[12] The rulings could have influence far beyond Silicon Valley and the Nation's Capital because they concern "the law that threatens to swallow the internet,"[13] better known as the Computer Fraud and Abuse Act (CFAA).[14]

The CFAA is a federal cyber-trespass law that makes it illegal to "access" a website "without authorization" and obtain "information."[15] In both *hiQ* and *Sandvig*, the courts considered whether platforms like LinkedIn and Amazon could use the CFAA to stop people from gathering information from their websites. By clearing the way for large-scale data collection from websites that are "open" to the general public, the decisions contradicted longstanding precedents in other jurisdictions.[16] This twist should interest anyone who uses the internet, but it should especially interest Congress. Why? Because the new *hiQ* rule shows it's high time to pass new laws.

While these recent decisions reveal tensions in the regulatory schemes that govern the internet, the stakes go far beyond the particular cases. Under cyber-trespass laws like the CFAA, some courts have treated platforms as

10. *Id.*; *see also* Sandvig v. Sessions, 315 F. Supp. 3d 1, 10 (D.D.C. 2018) (outlining how platforms prohibit certain research activities through their terms of service); Jeff Horwitz, *Facebook Seeks Shutdown of NYU Research Project into Political Ad Targeting*, WALL ST. J. (Oct. 23, 2020, 8:59 PM), https://www.wsj.com/articles/facebook-seeks-shutdown-of-nyu-research-project-into-political-ad-targeting-11603488533 [https://perma.cc/4BVV-2EQS] (reporting on Facebook's attempts to shut down an academic research project on targeted political advertising by threatening researchers with "enforcement action").

11. Laurent Sacharoff, *Criminal Trespass and Computer Crime*, 62 WM. & MARY L. REV. 571, 574 (2020).

12. Orin S. Kerr, *Scraping a Public Website Doesn't Violate the CFAA, Ninth Circuit (Mostly) Holds*, VOLOKH CONSPIRACY (Sept. 9, 2019, 7:22 PM), https://reason.com/2019/09/09/scraping-a-public-website-doesnt-violate-the-cfaa-ninth-circuit-mostly-holds [https://perma.cc/7R5C-CCZT] (unpacking the "hugely important" decision in *hiQ*).

13. Orin S. Kerr, *Criminal Law in Virtual Worlds*, 2008 U. CHI. LEGAL F. 415, 423.

14. Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology [https://perma.cc/MX4M-PHMY] (dubbing the CFAA "the worst law in technology" and "the most outrageous criminal law you've never heard of," while arguing that its "egregiously overbroad" provisions are "a nightmare for a country that calls itself free").

15. 18 U.S.C. § 1030(a)(2)(C) (2018). Similar laws now exist in all fifty states and over forty foreign countries. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1597 (2003) [hereinafter Kerr, *Cybercrime's Scope*]; *see also* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1017 (2001) (noting that "when Vermont enacted a statute proscribing computer crime in 1999, it became the fiftieth state to devote specific legislation to computer crimes"); Mary W. S. Wong, *Cyber-Trespass and 'Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience*, 15 INT'L J.L. & INFO. TECH. 90, 115–24 (2007) (discussing similarities between cyber-trespass laws in the United States and other countries); CAL. PENAL CODE § 502(c)(2) (West 2011) (outlining criminal prohibitions for anyone who "accesses and without permission takes, copies, or makes use of any data" from a computer network).

16. *See infra* Part I.

digital gatekeepers—as property owners that may permit and restrict access to their websites much like landowners may do with private land in the real world.[17] If platforms withhold their consent through words or inference, cyber-trespass laws let them enforce their preferences about who may access their services and gather information from the internet.

This is but one way that platforms act as "gatekeepers." Other scholars have used this terminology to capture different features of private control in the digital age. Rory Van Loo, for example, has called platforms the "New Gatekeepers" to describe how administrative agencies increasingly conscript them to "perform the duties of public regulator" and police other businesses.[18] Scholars like Danielle Citron, meanwhile, have used the terminology in the context of content moderation, observing that the internet "has many different digital gatekeepers"—from internet service providers to search engines to social media—that "have substantial freedom to decide whether and when to tackle" harms like cyber-harassment by deciding what content appears on their websites.[19] Relatedly, Eli Pariser has invoked the gatekeeper language to describe how platforms exercise editorial control over the news and information we consume, replacing the "old gatekeepers" that ran traditional broadcast and print media.[20] And other scholars have used it

17. *See generally* Thomas E. Kadri, *Platforms as Blackacres*, 68 UCLA L. REV. (forthcoming 2021), https://ssrn.com/abstract=3742086 (exploring the First Amendment implications of gatekeeper rights under cyber-trespass law).

18. Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467, 467–68, 482–84 (2020) [hereinafter Van Loo, *New Gatekeepers*].

19. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 227–36 (2014); *see also* Thomas E. Kadri, *Networks of Empathy*, 2020 UTAH L. REV. 1075, 1081–92 (proposing ways that platforms could alter their design and values to tackle digital abuse); Robert Gorwa, Reuben Binns & Christian Katzenbach, *Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance*, BIG DATA & SOC'Y, Feb. 28, 2020, at 1, 12 (discussing how "companies like Facebook now can boast of proactively removing 99.6% of terrorist propaganda" to legitimize "both their technical expertise and their role as a gatekeeper protecting a 'community'" (citation omitted)); Mark Bunting, *From Editorial Obligation to Procedural Accountability: Policy Approaches to Online Content in the Era of Information Intermediaries*, 3 J. CYBER POL'Y 165, 172 (2018) (observing that online speech policies "are enforced by armies of human moderators, who work as 'digital gatekeepers' for platforms, interpreting standards and guidelines, reviewing vast amounts of deeply unpleasant content, and becoming critical arbiters and adjudicators of which content violates rules, norms or law"). For a foundational take on the history of online gatekeeping and its relationship to legislative and judicial forbearance in regulating information technology, see generally Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253 (2006). *See also* Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53 (1986) (providing an influential framework for when to impose gatekeeper liability on private parties who might be in a position to disrupt misconduct).

20. Eli Pariser, *When the Internet Thinks It Knows You*, N.Y. TIMES (May 22, 2011), https://www.nytimes.com/2011/05/23/opinion/23pariser.html [https://perma.cc/BRV5-L9VR]. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 176–272 (2006) (exploring how information consumption in the networked public sphere functions differently from obtaining information through commercial mass media in the twentieth century).

when discussing antitrust concerns related to the power of digital platforms to control access to particular goods, markets, or people.[21]

The gatekeeper terminology has even made its way to Congress. In July 2020, at the long-awaited congressional hearings about allegedly anti-competitive practices by Amazon, Apple, Google, and Facebook, Representative David Cicilline gave his damning assessment: "As gatekeepers to the digital economy, these platforms enjoy the power to pick winners and losers, shake down small businesses and enrich themselves while choking off competitors. . . . Our founders would not bow before a king. Nor should we bow before the emperors of the online economy."[22]

These scholars and lawmakers call platforms "gatekeepers" principally to describe their design features, private rules, and business practices.[23] In this Essay, I explore a distinct but linked angle of platforms' gatekeeper role—one that focuses on how cyber-trespass law empowers them with *legal* rights of inclusion and exclusion over information on websites. Anxious about reputations and profits, platforms have touted their gatekeeper rights to scare and sue those seeking to use their websites against their wishes.[24] This legal regime affects all sorts of actors—from academics to journalists to businesses to consumers—who want to engage with the platforms' websites, even when they're open to the public or when people permit complementary services to access their accounts.[25] *HiQ* and *Sandvig* represent steps in the other direction, but platforms continue to enjoy power as digital gatekeepers in other jurisdictions across the country.

This Essay challenges the law's current embrace of gatekeeper rights. Applying cyber-trespass law across the entire internet has empowered private platforms to become public policymakers in unintended and unchecked ways, letting them establish and enforce the internet's accessibility and

21. *See*, *e.g.*, Peter Alexiadis & Alexandre de Streel, *Designing an EU Intervention Standard for Digital Platforms* 5–6 (Robert Schuman Ctr. for Advanced Studies, Working Paper No. 2020 /14, 2020), https://ssrn.com/abstract=3544694 (discussing "digital gatekeepers" in the context of antitrust concerns); *see also* Rory Van Loo, *Rise of the Digital Regulator*, 66 DUKE L.J. 1267, 1321 (2017) [hereinafter Van Loo, *Rise of the Digital Regulator*] (describing digital intermediaries as "potentially manipulative and deceptive machines serving as market gatekeepers").

22. Cecilia Kang & David McCabe, *Lawmakers, United in Their Ire, Lash Out at Big Tech's Leaders*, N.Y. TIMES (July 31, 2020), https://www.nytimes.com/2020/07/29/technology/big-tech-hearing-apple-amazon-facebook-google.html [https://perma.cc/2MEH-ARNK].

23. The main exception is Van Loo, whose work has revealed the regulatory gatekeeper function of "Big Tech" platforms under administrative law. *See* Van Loo, *New Gatekeepers*, *supra* note 18, at 467–68, 482–84 (describing how the Federal Trade Commission has pressured Amazon and Facebook to engage in regulation of third parties). My focus, by contrast, is on platforms' legal gatekeeper role under criminal and tort law.

24. *See infra* Parts I & II; *see also* Nathaniel Persily & Joshua A. Tucker, *The Challenges and Opportunities for Social Media Research*, *in* SOCIAL MEDIA AND DEMOCRACY: THE STATE OF THE FIELD AND PROSPECTS FOR REFORM 313, 321 (Nathaniel Persily & Joshua A. Tucker eds., 2020) (discussing how decisions like *hiQ* implicate the ability of academic researchers to study platforms).

25. *See infra* Part II.

informational rules. To borrow from an old proverb, we've let the foxes guard the henhouses.[26] But it's not too late to adopt a different legal regime—one that defers far less to private companies. Safiya Umoja Noble has taught us that "the very concept of community control on the web is increasingly becoming negligible" as we move toward an "increasingly privately controlled, neoliberal communication sphere."[27] While our legal rules don't explain this shift entirely, they're an important factor. But as Anupam Chander urged in this journal's pages nearly twenty years ago, "we should not view any rule as *natural*" and should instead critically assess "the principles governing the distribution of entitlements to property" on the internet.[28] It's time to heed his call.

After exploring the nature of platforms' gatekeeper rights under cyber-trespass law, this Essay offers a three-part legislative framework to curtail their power. To begin, Congress should amend the CFAA to clarify that cyber-trespass laws don't apply on websites that are accessible to the general public. Congress should then mandate and shield certain forms of interoperability between platforms, repealing or preempting laws that platforms use to thwart complementary interconnection with other services. Finally, Congress should pass targeted laws to regulate the collection and use of publicly accessible information on websites, plugging a hole that decisions like *hiQ* have created. Taking these three steps will change the locus of governance in key internet policy choices, stripping private platforms of the unbounded and trans-substantive decisionmaking power they currently enjoy. Although this regulatory agenda is ambitious, these are the kinds of fundamental and structural changes needed to protect privacy, speech, and consumer interests in the digital age.

The Essay proceeds in three Parts. Part I explores the genesis of platforms' gatekeeper rights and then examines the recent judicial skepticism of these rights. Part II demonstrates how gatekeeper rights allow platforms to enforce their preferences on a range of policies at the core of internet governance. Part III then outlines a three-part legislative agenda to regulate and restrain digital gatekeepers.

I. Platforms as Gatekeepers

When John Perry Barlow typed his famed *Declaration of the Independence of Cyberspace* in 1996, he proclaimed that cyberspace was a "global social space" where property laws "do not apply" because they "are

26. *See supra* note 1 and accompanying text.

27. SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 92 (2018).

28. Anupam Chander, *The New, New Property*, 81 TEXAS L. REV. 715, 719–21 (2003) (making this argument in the context of critiquing first-come, first-served property rules governing domain names on the internet).

all based on matter, and there is no matter here."[29] Barlow's utopian rhetoric overlooked the CFAA, a federal law that had already been on the books for a decade.

Barlow might have wished that cyberspace was immune from property law, but the CFAA borrowed from the ancient concept of trespass to prohibit unauthorized "access" to computer networks.[30] The statute imposes criminal and tort liability on anyone who "accesses a computer without authorization" and "obtains . . . information."[31] Through many twists and turns, this language has created powerful gatekeeper rights over websites. This Part recounts how.

A. Legislative Endorsement of Gatekeeper Rights

Our story begins in 1983 at Camp David. Amid Cold War tensions, President Ronald Reagan screened *WarGames*, a sci-fi movie about a teenager who brings the world to the verge of World War III after mistaking the Pentagon's online weapons system for a computer game.[32] President Reagan later interrupted a meeting to quiz his generals about the plot's plausibility.[33] Prompted in part by his concerns, Congress then passed the CFAA to "deter[] the criminal element from abusing computer technology."[34] Though the law initially covered only financial records obtained from a narrow set of computer networks, Congress repealed these limitations over time.[35] The upshot is that the CFAA now governs all of us

29. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/ER9Q-BDGW].

30. Sacharoff, *supra* note 11, at 573, 576 n.26 (detailing how the CFAA "criminalizes the simple act of computer trespass" and noting that "Congress intended courts to analogize the CFAA to state criminal trespass laws"); United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015) (noting that "the legislative history consistently characterizes the evil to be remedied—computer crime—as 'trespass'"); *see also* H.R. REP. NO. 98-894, at 10 (1984) (discussing the problem of hackers who gain "access (trespass into)" computers and debating legislation to address a "flurry of electronic trespass[es]").

31. 18 U.S.C. § 1030(a)(2), (c), (g); *see also* Musacchio v. United States, 136 S. Ct. 709, 713 (2016) (describing the CFAA's prohibition on "improperly accessing a protected computer").

32. Gabe Rottman, *Knight Institute's Facebook 'Safe Harbor' Proposal Showcases Need for Comprehensive CFAA Reform*, REPS. COMMITTEE FOR FREEDOM PRESS (Aug. 6, 2018), https://www.rcfp.org/knight-institutes-facebook-safe-harbor-proposal-showcases-need-compr [https://perma.cc/93VN-2MLT].

33. *Id.*; *see also* STEPHANIE RICKER SCHULTE, CACHED: DECODING THE INTERNET IN GLOBAL POPULAR CULTURE 21–54 (2013) (exploring the influence of the *WarGames* storyline in many cyber-related policy debates in the 1980s).

34. H.R. REP. NO. 98–894, at 4 (1984).

35. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1564–71 (2010) [hereinafter Kerr, *Vagueness Challenges*] (providing the history behind this statutory creep); Sacharoff, *supra* note 11, at 580–81 (same).

whenever we use the internet.[36] A person "need not have a bad motive or an intent to gain, nor cause any harm or damage to the computer or its owner."[37] Rather, the law can kick in as soon as you visit *any* website and view *any* information.[38]

In practice,[39] the only meaningful constraint in the CFAA's legal framework—"the distinguishing line between *legal* and *prison*"—is whether you visit a website "without authorization."[40] These two words have

36. *See* Sacharoff, *supra* note 11, at 578 n.30 (explaining that the definition of "protected computers" under the CFAA "effectively includes any computer connected to the internet, and even perhaps some that are not" (citing 18 U.S.C. § 1030(e)(2))); *see also* Kerr, *Cybercrime's Scope*, *supra* note 15, at 1663 n.284 (observing that "[t]he term 'protected computer' is defined extremely broadly to include essentially every computer connected to the Internet"); Jack Dahm, Note, *No Internet Does Not Mean No Protection Under the CFAA: Why Voting Machines Should Be Covered Under 18 U.S.C. § 1030*, 94 NOTRE DAME L. REV. 1775, 1790–91 (2019) (arguing that the CFAA covers some computers not connected to the internet).

37. Sacharoff, *supra* note 11, at 573.

38. *See* S. REP. NO. 99-432, at 6 (1986) (noting that the statute's "obtaining information" language includes the "mere observation of the data"); Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 648 (E.D. Pa. 2007) (explaining that "[v]iewing material on a computer screen constitutes 'obtaining' information under the CFAA"); Sacharoff, *supra* note 11, at 578 (arguing that the "obtaining information" element "adds almost nothing" because "observing information suffices"). *See generally* Kerr, *Vagueness Challenges*, *supra* note 35, at 1568, 1571, 1577 (observing that the CFAA appears to cover "every computer connected to the Internet" located anywhere in the world).

39. I give this qualifier in part because of an insightful new article by Laurent Sacharoff that explores another possible constraint within the statute itself: the *mens rea* requirement that a defendant *knowingly* access the information without authorization. Sacharoff, *supra* note 11, at 598–607. Sacharoff mounts a persuasive case that courts and scholars have overlooked this limitation and unwisely focused on the meaning of "without authorization." I share his hope that the *mens rea* requirement could constrain troubling cyber-trespass liability, but even he acknowledges that courts have so far shown no signs of limiting the CFAA's reach on this basis. *See id.* at 574, 587–99 (describing how courts "misdiagnose the problem as arising from the element 'without authorization' and propose the wrong solution in the form of a code-based test"); *see also* Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1180 (2016) [hereinafter Kerr, *Norms*] (observing that "[c]ourts have not explored the role of mental state in establishing liability for computer trespass"); William A. Hall, Jr., *The Ninth Circuit's Deficient Examination of the Legislative History of the Computer Fraud and Abuse Act in* United States v. Nosal, 84 GEO. WASH. L. REV. 1523, 1528–31 (2016) (emphasizing how one court failed to grapple with the mental state necessary to sustain CFAA liability); *cf.* David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 945–47 (2013) (proposing a legislative amendment to the required mental state for CFAA liability).

40. *See* Jennifer Granick, *Towards Learning from Losing Aaron Swartz*, STAN. CTR. FOR INTERNET & SOC'Y (Jan. 14, 2013, 4:37 PM), https://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz [https://perma.cc/G8V2-QE74] (emphasis added) (explaining why the CFAA is "one of [her] biggest concerns" as a former criminal defense lawyer). A second form of unauthorized access under the CFAA is when a person "exceeds authorized access." 18 U.S.C. § 1030(a)(2) (2018). This Essay focuses principally on instances when access is "without authorization" because that prong is more commonly invoked when "outsiders" access websites without the platform's permission, but many of the same principles are at play under both theories of liability. *See* United States v. Nosal, 844 F.3d 1024, 1033–34, 1036 & n.9 (9th Cir. 2016)

generated considerable controversy. While the Second Circuit has declared that they are words "of common usage, without any technical or ambiguous meaning,"[41] others have complained that Congress's failure to define them is the law's "original sin."[42] Jennifer Granick, for example, has bemoaned that "authorization" under the CFAA is in the "eye of the beholder."[43]

Granick's complaint has a twofold meaning—one descriptive, one conceptual. In a descriptive sense, she observes that courts have endorsed numerous and conflicting indicators of when access is unauthorized and therefore illegal.[44] This doctrinal mishmash has costs: courts may issue contradictory decisions on what the law prohibits; prosecutors may charge broadly to secure indictments and gain leverage in plea negotiations; and private actors may threaten litigation based on inconsistent theories of liability.[45] In the end, people are puzzled about what will land them in hot water.

In a conceptual sense, Granick's complaint gets to the heart of the CFAA's structure. "Authorization" is in the "eye of the beholder" because the CFAA gives each website owner the autocratic power to decide whether someone's access to its website is allowed. Granick sees this as a *bug* because it gives website owners unchecked power to "unilaterally decide what is right and wrong" and then use "the full force of federal law" to enforce their wishes.[46] But others see this as a *feature*. Just as real-world trespass liability turns on whether property owners want you on their land, so too cyber-trespass liability turns on whether website owners want you on their websites.[47] Laurent Sacharoff, for example, has argued that the term "without authorization" is "perfectly comprehensible"—it means "keep off" or "stay

(distinguishing between the "without authorization" and "exceeds authorization" provisions as applying respectively to "outsiders" and "insiders"); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (recognizing that the distinction between the two theories of liability "is arguably minute"); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (observing that the distinction is often "paper thin").

41. United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991); *accord Nosal*, 844 F.3d at 1028 (concluding that "without 'authorization'" is "an unambiguous, nontechnical term that, given its plain and ordinary meaning, means accessing a protected computer without permission").

42. Rottman, *supra* note 32; *see also* Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, PITT. J. TECH. L. & POL'Y, Fall 2012, at 1, 25–27 (lamenting the lack of statutory definition and proposing language that Congress could adopt).

43. Granick, *supra* note 40.

44. *Id.*

45. *See* CITRON, *supra* note 19, at 187–88 (raising some of these concerns in the context of discussing a famous CFAA case, *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)).

46. Granick, *supra* note 40.

47. James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500, 1502 (2016).

out."[48] In his view, "courts have taken a plain-meaning term, 'without authorization,' and *made it* vague."[49]

James Grimmelmann has made similar observations. Drawing lessons from analogous laws that incorporate notions of permission, he's astutely argued that the term "without authorization" doesn't refer to "what a *computer user does*" but rather "what a *computer owner says* about those uses."[50] To ask if the CFAA prohibits or allows *X* poses a question "at the wrong level of abstraction" because the issue "is not whether *X* is allowed, but whether *X* is allowed *by the computer's owner*."[51] By design, the CFAA "does not of its own force define a class of prohibited conduct, because literally any conduct in relation to a computer could be either authorized or unauthorized."[52] Altering headlines on the *Los Angeles Times* website, for example, could be an unauthorized act of cyber-vandalism when done by a prankster, but it's an authorized act of cyber-maintenance when undone by the newspaper's editors.[53] It's all about consent.[54]

But how do courts determine consent under cyber-trespass laws like the CFAA? To answer this question, it helps to dip into traditional trespass law. A key concept in property law is that landowners enjoy the right to exclude

48. Sacharoff, *supra* note 11, at 575, 610 (citations omitted); *see also* WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 21.2(a) (3d ed. 2018) (asserting that "without authorization" in trespass law means entry is "forbidden"); Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477, 1478–79 (2016) (arguing that "authorization" under the CFAA "has the same meaning as authorization under criminal physical trespass laws"); Martin v. City of Struthers, 319 U.S. 141, 147 (1943) (observing that a person becomes a trespasser once they're warned to "keep off" the owner's property); Bowman v. United States, 212 A.2d 610, 611 (D.C. 1965) (same).

49. Sacharoff, *supra* note 11, at 577.

50. Grimmelmann, *supra* note 47, at 1501.

51. *Id.*

52. *Id.*; *see also* James Grimmelmann, *Computer Crime Law Goes to the Casino*, LABORATORIUM (May 2, 2013, 1:50 PM), http://laboratorium.net/archive/2013/05/02/computer_crime_law_goes_to_the_casino [https://perma.cc/7JRU-YNEM] ("The problem with the CFAA is not some recent mutation of a law that has outgrown its original purpose. The problem was there all along; it was inherent in the very project of the CFAA.").

53. This hypothetical isn't all that hypothetical. *See* United States v. Keys, 703 F. App'x 472, 474 (9th Cir. 2017) (affirming the conviction of a journalist charged with turning over login credentials to a hacker who altered a headline on the *Los Angeles Times* website); Joseph Serna & Stephen Ceasar, *Former Reuters Social Media Editor Convicted of Aiding* L.A. Times *Hack*, L.A. TIMES (Oct. 7, 2015, 4:54 PM), https://www.latimes.com/local/lanow/la-me-ln-matthew-keys-convicted-hacking-la-times-20151007-story.html [https://perma.cc/K8TE-4X9L] (summarizing the events leading up to the CFAA conviction).

54. *See* Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 HARV. J.L. & TECH. 479, 519–26 (2019) (discussing factual and legal consent in the context of the CFAA); Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011) ("Commonly understood, . . . a defendant who accesses a computer 'without authorization' does so without sanction or permission.").

others from their land.[55] This right is better articulated as a "gatekeeper right," for it's as much about inclusion as it is about exclusion.[56] Landowners generally have the right to determine who has access to their property, on what terms, and for what reasons.[57] As a gatekeeper, you can invite me into your home but then tell me to leave; you can set rules and kick me out if I break them; you can summon the police or sue me if I linger too long; and you can arbitrarily deny me access while granting it to others.[58] This gatekeeper right is especially powerful on private property. If you don't consent to my presence in your home, for example, you may exclude me for any reason whatsoever with the backing of trespass law.[59] Your discretion is absolute.

Because trespass liability turns on a landowner's consent, they must give notice of what's forbidden. In the real world, this generally happens in three ways: through actual notice, like the proverbial senior citizen yelling "Get off my lawn!"; through constructive notice, like posting a "No Entry" sign in a conspicuous spot; and through implicit notice, like erecting a fence.[60] Gatekeepers may exercise their legal rights only if they provide proper notice. No notice, no trespass.

---

55. *See* Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979) (holding that the right to exclude is "one of the most essential sticks in the bundle of rights that are commonly characterized as property"); Int'l News Serv. v. Assoc. Press, 248 U.S. 215, 250 (1918) (Brandeis, J., dissenting) ("An essential element of individual property is the legal right to exclude others from enjoying it."); 2 WILLIAM BLACKSTONE, COMMENTARIES *2 (describing the "right of property" as a "sole and despotic dominion").

56. Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 740, 744 (1998).

57. *Id.* at 740.

58. *See* J.E. PENNER, THE IDEA OF PROPERTY IN LAW 74 (1997) (asserting that the right of property is "like a gate, not a wall" because it "permits the owner not only to make solitary use of his property, by excluding all others, but also permits him to make a social use of his property, by selectively excluding others, which is to say by selectively allowing some to enter"); Carol M. Rose, *Canons of Property Talk, or, Blackstone's Anxiety*, 108 YALE L.J. 601, 604 (1998) (explaining how the right to exclude provides property owners with "decisionmaking authority" and "a small domain of complete mastery, complete self-direction, and complete protection from the whims of others").

59. *See* Jacque v. Steenberg Homes, Inc., 563 N.W.2d 154, 159–60 (Wis. 1997) (describing the "long recognized" right of a property owner to exclude others from private property for any purpose that does not infringe on another's rights); Felix S. Cohen, *Dialogue on Private Property*, 9 RUTGERS L. REV. 357, 374 (1954) (setting forth the proposition that property involves the right to exclude others unless the owner consents, with such consent being given or withheld at the owner's discretion).

60. *See, e.g.*, MODEL PENAL CODE § 221.2(2) (AM. LAW INST. 1962) (establishing that notice against trespass can be given by actual communication, posting, or physical enclosure designed to keep out intruders); *Jacque*, 563 N.W.2d at 157, 161, 164 (providing an example of actual notice by a landowner who told trespassers not to come onto his property); C.B.S. v. State, 184 So. 3d 611, 614 (Fla. Dist. Ct. App. 2016) (discussing statutory requirements for constructive notice by posting signs under Florida law). There will be times when these forms of notice overlap. If an intruder sees a "no trespass" sign, for example, it makes sense to talk about them having actual notice. Likewise,

Relying on the cyberspace metaphor,[61] courts have interpreted the CFAA in harmony with traditional trespass laws by granting platforms gatekeeper rights over their websites.[62] Under the law in many jurisdictions, a platform may use the CFAA to prohibit people from accessing its website even if it's otherwise open to the general public and even if the platform's user permits complementary services to access their account.[63] Platforms may selectively enforce their rules, letting some people gather information while forbidding others.[64] And platforms may collect information themselves, selling or trading it for their own benefit. As digital gatekeepers, that is their privilege.[65]

The harmony between realspace and cyberspace goes further because courts have effectively recognized cyber-analogs for each form of real-world notice.[66] In many jurisdictions, platforms may give actual notice by sending

---

the line between constructive and implicit notice is especially fuzzy when states outline types of fencing that will satisfy the notice requirement for trespass claims. *See, e.g.*, V.B. v. State, 959 So. 2d 1252, 1254 (Fla. Dist. Ct. App. 2007) (describing the "constructive notice" that an intruder might have if a landowner erected "a fence of substantial construction" that "stands at least 3 feet in height" (citing FLA. STAT. ANN. § 810.011(7) (2006)). Again, it might make sense to describe notice by fencing as "constructive" when assessing adherence to predetermined statutory requirements for fencing to provide legally sufficient notice, even if it generally makes more sense to think of fencing providing "implicit" notice because it conveys the owner's lack of consent to intruders by implication, as compared to the forms of actual and constructive notice that tend to be explicit.

61. The wisdom and implications of the cyberspace metaphor have been explored and "hotly contested" by scholars for many years. *See generally* Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 210–26 (2007) (describing and critiquing literature in this space). I share concerns about the metaphor raised by Julie Cohen and others, but I leave further discussion for other work. *See* Kadri, *supra* note 17, at 34–35.

62. *See* Orin S. Kerr, *Trespass, Not Fraud: The Need for New Sentencing Guidelines in CFAA Cases*, 84 GEO. WASH. L. REV. 1544, 1545–46 (2016) (discussing how "[m]ost CFAA offenses are trespass offenses" because the "primary harm in most CFAA cases is invasion of privacy and interference with the right to exclude").

63. *See, e.g.*, EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62–64 (1st Cir. 2003) (upholding a preliminary injunction pursuant to the CFAA that precluded defendant from using a "scraper" to collect data from a company's public website); Sw. Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439–40 (N.D. Tex. 2004) (finding the operator of a public website alleged sufficient facts to state a CFAA claim by saying that it had "directly informed" defendant that scraping was prohibited); Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1062–63, 1067–68 (9th Cir. 2016) (ruling that defendant acted "without authorization" under the CFAA when it accessed Facebook user information after receiving Facebook's demand not do to so, even though the Facebook users had consented to defendant's access).

64. *See Facebook*, 844 F.3d at 1067–68 (finding that a cease-and-desist letter explicitly revoked defendant's permission to continue using Facebook's website and that its further use of the website ran afoul of the CFAA); United States v. Nosal, 844 F.3d 1024, 1035–36 (9th Cir. 2016) (acknowledging the "exclusive discretion" of an owner to "issue or revoke access" to a website under the CFAA).

65. Though perhaps it shouldn't be. *See infra* Part II.

66. For a more in-depth discussion of this harmony, see Kadri, *supra* note 17, at 15–18, 20–25.

cease-and-desist letters that explicitly forbid access to their websites,[67] they may give constructive notice by listing rules in their terms of service,[68] and they may give implicit notice by creating technological barriers to accessing their websites.[69] If you fail to heed any of these warnings from a platform, you're in trouble.

---

67. *See, e.g.*, *Facebook*, 844 F.3d at 1067–68 (holding that CFAA liability was triggered by a letter that "revoked explicitly" defendant's permission to access Facebook's website); Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969–70, 970 n.8 (N.D. Cal. 2013) (holding that CFAA liability was triggered by a letter that included "clear statements" that "specifically denied [defendants'] authorization to use the website 'for any purposes'"); *Sw. Airlines Co.*, 318 F. Supp. 2d at 439–40 (holding that CFAA liability was triggered by "repeated warnings and requests" that "directly informed" defendant to stop accessing the website); CouponCabin, Inc. v. PriceTrace, LLC, No. 18-7525, 2019 WL 1572448, at *1–2 (N.D. Ill. Apr. 11, 2019) (holding that CFAA liability was triggered by a letter revoking defendant's permission to access a website); *see also EF Cultural Travel BV*, 318 F.3d at 62–64 (explaining that CFAA liability could be triggered by a clear statement on a website's homepage saying "no scrapers may be used" because such a statement would provide "fair warning" that automatically gathering information from the website was prohibited).

68. *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 461–62, 467 (C.D. Cal. 2009) (holding that CFAA liability was triggered through defendant's violation of a platform's rules prohibiting lies about one's age or identity, before ultimately overturning the conviction on constitutional grounds); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (holding that CFAA liability was triggered through defendant's violation of an internet provider's policies); CollegeSource, Inc. v. AcademyOne, Inc., 597 F. App'x 116, 130 (3d Cir. 2015) (suggesting that CFAA liability could be triggered if defendants "breach[ed] any . . . contractual term of use"); *see also* Wu, *supra* note 14 (discussing CFAA prosecution of Aaron Swartz based "on a terms-of-service violation"); United States v. Lowson, No. 10–114, 2010 WL 9552416, at *5–6 (D.N.J. Oct. 12, 2010) (discussing a CFAA prosecution based in part on defendant's alleged violations of policies outlined in a website's terms of service); United States v. Van Buren, 940 F.3d 1192, 1198, 1208 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667 (2020) (U.S. argued Nov. 30, 2020) (No. 19-783) (affirming a police officer's CFAA conviction after the officer used police database for personal reasons even though officers were "trained on the proper and improper uses of the system" and officer admitted his actions were "wrong"); EarthCam, Inc. v. OxBlue Corp., 703 F. App'x 803, 808 & n.2 (11th Cir. 2017) (stating that "one of the lessons from [circuit precedent] may be that a person exceeds authorized access if he or she uses the access in a way that contravenes any policy or term of use governing the computer in question"). As with real-world trespass, the lines between actual and constructive notice in CFAA cases can blur, especially when an alleged cyber-trespasser is aware that their conduct runs afoul of a website owner's rules. *See* Sandvig v. Sessions, 315 F. Supp. 3d 1, 10, 26–27 (D.D.C. 2018) (discussing potential CFAA liability when researchers are aware that their activities will violate a website's terms of service). The important point, however, is that courts accepting this form of notice will generally do so without requiring proof that the computer user is actually aware of the rules.

69. *See, e.g.*, *EF Cultural Travel BV*, 318 F.3d at 63 ("[L]ack of authorization may be implicit, rather than explicit. After all, password protection itself normally limits authorization by implication (and technology), even without express terms."); Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1038–39 (N.D. Cal. 2012) (accepting Facebook's argument that "circumvent[ing] technical barriers"—specifically, taking steps to evade the blocking of IP addresses—constitutes "access[ing] the site 'without permission'" and triggers liability under the CFAA); *Craigslist*, 942 F. Supp. 2d at 969–70 (accepting Craigslist's argument that "[d]efendants' continued use of Craigslist" despite the "technological measures to block them constitutes unauthorized access under the statute"); *see also CollegeSource*, 597 F. App'x at 130 (suggesting that defendants could be prosecuted under the CFAA if they "breach[] any technological barrier").

Real-world trespass law has generally had more nuance than cyber-trespass law. Landowners may usually exclude people easily and arbitrarily, but not always. Though this oversimplifies current doctrine and glosses over the heroic struggles that led to it,[70] we can loosely say that it becomes harder to exercise your real-world gatekeeper rights if you allow more people on your land.[71] Not only are certain reasons for exclusion impermissible, but the type of notice might need to be more direct and personal.[72] On the internet, however, courts have often applied what I've called the *blackacre principle* of cyber-trespass law: if you provide notice that you forbid access to your website, you may use your gatekeeper rights to exclude anyone from it for any reason whatsoever with the backing of criminal and tort law.[73] At its core, that's the power of a digital gatekeeper.

This jurisprudence has effectively made it "illegal—indeed, criminal—to seek information from a publicly available website" against the website owner's wishes.[74] As one court has remarked, the CFAA's structure makes it "primarily a statute imposing limits on access and enhancing control by information providers" like platforms.[75] Mark Lemley recognized long ago how this consent-based framework could create a "serious problem" in the digital age,[76] and concerns have only deepened as platforms have increasingly used the CFAA to police the internet—and as courts have invited them to do so.[77] More recently, Jane Bambauer has questioned the CFAA's constitutionality under the First Amendment because it applies "serious civil and criminal penalties to anybody who accesses a website for

70. *See generally* Sacharoff, *supra* note 11, at 621–24, 642–43 (discussing the impact of the 1964 Civil Rights Act on contemporary trespass law).

71. *See, e.g.*, *id.* at 616 (detailing how states often add an extra trespass element for places open to the public—like shopping malls, parks, and stores—by requiring "personally communicated" notice to any would-be trespasser (citing N.Y. PENAL LAW 140.00(5) (McKinney 2020))); *cf.* Tim Wu, *It's a Mad, Mad, Mad, Mad Disney World*, NEW YORKER (Jan. 22, 2013), https://www.newyorker.com/culture/culture-desk/its-a-mad-mad-mad-mad-disney-world [https://perma.cc/J6T6-4PEW] (raising the possibility that the makers of indie movie *Escape from Tomorrow* committed trespass if their filming inside Disney World violated Disney's rules).

72. *See* Sacharoff, *supra* note 11, at 622–23 (describing how the presumption that a person has a license to enter a public place like a shopping mall can be superseded if that person has been issued a written ban).

73. Kadri, *supra* note 17, at 15.

74. Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 528 (2003) (criticizing the use of browsewrap licenses to trigger CFAA liability).

75. EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003).

76. Lemley, *supra* note 74, at 528; *see also* Rory Van Loo, *Digital Market Perfection*, 117 MICH. L. REV. 815, 838, 872 (2019) [hereinafter Van Loo, *Digital Market Perfection*] (arguing that courts should refrain from applying the CFAA to block access to publicly accessible information).

77. *See, e.g.*, *EF Cultural Travel BV*, 318 F.3d at 64 (encouraging "public website providers . . . to say just what non-password protected access they purport to forbid"); Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969 n.8 (N.D. Cal. 2013) (stating that the court would assume that the CFAA's broad language allows websites to restrict access to information that is otherwise public information, at least "until the Ninth Circuit holds otherwise").

a purpose that violates the website's terms of service, even when the website is available to the public without password protection."[78] Although some courts have ruled that terms-of-service violations alone can't sustain CFAA liability, platforms may still exaggerate this theory's continued viability and revitalize it through cease-and-desist letters that courts will never see.[79]

Yet despite these concerns, both prosecutors and platforms have repeatedly argued that websites are "merely private property," meaning that "[a] platform can deny access to anyone it wishes, for any reason."[80] This argument flows quite logically if you accept the premise that websites are like private land in the real world: "If the government criminalizes a person who accesses such a website in violation of the website's rules, they have merely criminalized a trespass analogous to a criminal trespass in the real world that would occur if a person refused to leave the premises after being told to leave,"[81] or so the argument goes. But should the law grant platforms these gatekeeper rights? I have my doubts, as do some courts.

B. Judicial Skepticism of Gatekeeper Rights

This brings us back to the two cases mentioned in our introduction. The *hiQ v. LinkedIn* dispute arose because LinkedIn wanted to prevent hiQ from gathering information that people published on their publicly accessible LinkedIn profiles.[82] HiQ relied on this information to conduct statistical analyses and provide business insights. For example, one hiQ service predicted which employees were likely to be recruited by other companies, enabling employers to offer perks like retention bonuses to help keep valuable personnel.[83] Another hiQ service summarized employee skills,

78. Jane R. Bambauer, *The Empirical First Amendment*, 78 OHIO ST. L.J. 947, 957 (2017) (raising the possibility of a First Amendment challenge to the CFAA); *see also* Jacquellena Carrero, Note, *Access Granted: A First Amendment Theory of Reform of the CFAA Access Provision*, 120 COLUM. L. REV. 131, 165–66 (2020) (arguing that Congress should amend the CFAA in order to protect various competing First Amendment interests). I explore these First Amendment questions in Kadri, *supra* note 17, at 5–7, while others have discussed alternative constitutional challenges to cyber-trespass law elsewhere. *See, e.g.*, Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751, 755 (2013) (analyzing court decisions suggesting that broad CFAA interpretations render the statute unconstitutionally vague).

79. *Compare* United States v. Nosal, 676 F.3d 854, 859–62 (9th Cir. 2012) (en banc) (holding that violations of website policies can't trigger CFAA liability because such a rule would create "[s]ignificant notice problems"), *with* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 n.3 (9th Cir. 2016) (distinguishing this doctrinal limitation because the website policies were reiterated in a cease-and-desist letter to provide defendant notice).

80. Laurent Sacharoff, *Russia Gave Bots a Bad Name. Here's Why We Need Them More Than Ever*, POLITICO (Aug. 14, 2018), https://www.politico.com/magazine/story/2018/08/14/russia-gave-bots-a-bad-name-heres-why-we-need-them-more-than-ever-219359 [https://perma.cc/ACL2-BM2G].

81. *Id.*

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

83. *Id.* at 991.

helping employers identify gaps in their workforces and training programs.[84] Both services relied on information that hiQ obtained from LinkedIn profiles that were "visible to the general public."[85] In order to collect this information on a large scale, hiQ used automated bots to "scrape" LinkedIn's website.[86]

LinkedIn wasn't happy with hiQ's behavior. In a move no doubt endorsed by in-house lawyers, the platform mounted a tripartite attack to give notice that hiQ's scraping was forbidden. LinkedIn gave actual notice by sending hiQ a cease-and-desist letter declaring that "[a]ny future access of any kind" to LinkedIn's website would violate the CFAA and be "without permission and without authorization."[87] It gave constructive notice by posting rules on its website that prohibited anyone from collecting information without first getting LinkedIn's "express permission."[88] And it gave implicit notice by implementing technical measures to restrict scraping generally and block hiQ specifically from accessing its website.[89] HiQ then sought an injunction to stop LinkedIn from barring its access. The district court sided with hiQ, issuing an order that left hiQ free to scrape the publicly accessible portions of LinkedIn's website.[90] The Ninth Circuit affirmed on appeal, holding that there was at least a "serious question" as to whether platforms can rely on the CFAA to restrict access to websites that are "open to the general public."[91]

The *hiQ* ruling will be celebrated by academics and journalists who rely on web scraping to do their research.[92] Indeed, our second introductory case, *Sandvig v. Barr*, involved a group of researchers challenging the CFAA's applicability to their use of scraping to study housing and employment discrimination.[93] Two of the plaintiffs, Professors Alan Mislove and Christo Wilson, wished to gather information from job-seeking websites to discover whether potential candidates face discrimination based on their race or gender.[94] They and their *Sandvig* coplaintiffs conceded that the website

84. *Id.*

85. *Id.* at 990.

86. *Id.* at 991. "Scraping involves extracting data from a website and copying it into a structured format, allowing for data manipulation or analysis." *Id.* at 991 n.3. Although scraping can be done manually, it's typically done automatically by a web robot or "bot." *Id.*

87. hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1104 (N.D. Cal. 2017) (alteration in original).

88. *hiQ Labs*, 938 F.3d at 990–91, 991 n.5.

89. *Id.* at 990–92.

90. *Id.* at 992.

91. *Id.* at 1001–02.

92. *See* Persily & Tucker, *supra* note 24, at 321 (noting that "academic researchers often must resort to scraping to get the information under platform control").

93. Sandvig v. Sessions, 315 F. Supp. 3d 1, 8–9 (D.D.C. 2018), *sub nom.* Sandvig v. Barr, 451 F. Supp. 3d 73 (D.D.C.), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020).

94. *Id.* at 9–10.

owners wouldn't consent to their research based on terms of service that prohibit scraping and require permission before using the websites for research purposes.[95] Nonetheless, with the help of the American Civil Liberties Union, the researchers sought a judgment that their research activities would be legally permissible.[96]

In ruling on the government's motion to dismiss, the *Sandvig* court explained that the researchers could challenge the CFAA's constitutionality under the First Amendment because "attempts to record the contents of public websites for research purposes are arguably affected with a First Amendment interest."[97] The court ultimately dodged many of the constitutional claims, however, after concluding that the CFAA didn't prohibit the researchers' attempts to gather information because "[s]craping or otherwise recording data from a site that is accessible to the public is merely a particular use of information that plaintiffs are entitled to see."[98] As a result, the court held, the researchers' "proposed activities fall outside the CFAA's reach" because they involve "obtaining or using information that the general public can access."[99]

The court in *Sandvig* later expanded on this ruling when deciding the parties' cross-motions for summary judgment. In a recent decision, the court asserted that the CFAA's wording "contemplates a view of the internet as divided into at least two realms—*public* websites (or portions of websites) where no authorization is required and *private* websites (or portions of websites) where permission must be granted for access."[100] The court approvingly quoted the Ninth Circuit's *hiQ* decision, explaining that "many websites on the internet are open to public inspection" and that "a website becomes 'private' only if it is 'delineated as private through use of a permission requirement of some sort.'"[101] Ultimately, the court held that the CFAA applies "only when the user bypasses an authenticating permission requirement, or an 'authentication gate,' such as a password restriction," and not on publicly accessible websites.[102] The upshot: the researchers couldn't be liable for cyber-trespass for their planned scraping activities on websites that are "open" to anyone.[103]

95. *Id.* at 10.

96. *Id.* at 7–8.

97. *Id.* at 16.

98. *Id.* at 26–27.

99. *Id.* at 17, 26.

100. Sandvig v. Barr, 451 F. Supp. 3d 73, 85 (D.D.C.), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020).

101. *Id.* (quoting hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1001 (9th Cir. 2019)).

102. *Id.* at 89.

103. *Id.*

Given prior CFAA precedent, *hiQ* and *Sandvig* are quite remarkable decisions.[104] As we've seen, a slew of other courts had endorsed liability for scraping publicly accessible websites, and prior cases had suggested that platforms have broad powers to prevent access to their websites so long as notice is clear. The First Circuit, for example, has declared that an explicit "no scrapers may be used" statement on a website's homepage would trigger CFAA liability by providing "fair warning" that automatically gathering information from the website was prohibited.[105] That court concluded that website owners had unreviewable gatekeeper rights, declaring that "public website providers ought to say just what non-password protected access they purport to forbid" in order to get their way.[106]

Even the Ninth Circuit had previously held that platforms could sustain CFAA claims merely by providing written notice in a cease-and-desist letter.[107] According to earlier decisions by that court, the entity that "own[s] and control[s] access" to a computer network "retain[s] exclusive discretion to issue or revoke access" to it under the CFAA.[108]

Platforms surely felt emboldened by these decisions. LinkedIn's objection to hiQ was crystal clear when it "revoked permission" both "explicitly" and "selectively" for hiQ to access its website.[109] In other words, LinkedIn tried and failed to act as a gatekeeper. The *hiQ* court denied it that power under the CFAA because LinkedIn's website was "open to the general public,"[110] and the *Sandvig* court adopted a similar posture.[111] Now, with the Supreme Court poised to construe the statute's "authorization" element this term, we're at a fascinating juncture in cyber-trespass law.[112]

---

104. *See* Noah Feldman, *This Court Case Is Bad News for Social Media Privacy*, BLOOMBERG (Apr. 5, 2018, 4:00 AM), https://www.bloomberg.com/opinion/articles/2018-04-05/facebook-cambridge-analytica-and-a-new-free-speech-ruling [https://perma.cc/Z3AL-3UC2] (arguing that the *Sandvig* court "made some fascinating and highly controversial new law" and that "[t]he consequences are potentially vast"); Kerr, *supra* note 12 (asserting that *hiQ* is a "really important decision that embraces the open presumption of the Internet far more clearly and directly than prior cases").

105. EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62–64 (1st Cir. 2003).

106. *Id.* at 64.

107. *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1062–63, 1067–68 (9th Cir. 2016) (holding that Facebook could exclude another company from its website by sending a "written notification" that Facebook denied the company permission to access it).

108. United States v. Nosal, 844 F.3d 1024, 1029–30, 1035–36 (9th Cir. 2016).

109. hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1108–09 (N.D. Cal. 2017).

110. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1000 (9th Cir. 2019) (explaining that "[a]t the very least . . . hiQ has raised a serious question" as to whether the CFAA is "inapplicable" to publicly accessible websites).

111. Sandvig v. Barr, 451 F. Supp. 3d 73, 85–89 (D.D.C.), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020).

112. *See* United States v. Van Buren, 940 F.3d 1192, 1198, 1208 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667 (2020) (U.S. argued Nov. 30, 2020) (No. 19-783) (raising the question of what counts as "exceeding authorized access" under the CFAA).

II. Letting Foxes Guard Henhouses

Despite the newfound skepticism that gatekeeper rights apply on publicly accessible websites, platforms still enjoy broad powers to exclude under cyber-trespass precedents in many circuits.[113] Given platforms' trans-jurisdictional operations across the global internet, the legal landscape still tilts in their favor. After all, the threat of liability is often all it takes for platforms to get their way, and they can flex their muscles with cease-and-desist letters that needn't provide citations to contrary precedents like *hiQ* and *Sandvig*. While it's tempting to see recent events as revolutionary, it's premature to assume that the tide has turned, especially because judicial acceptance of scraping tends to come and go in waves.[114] And although the Supreme Court might bring some clarity to cyber-trespass law this term, it's doubtful that this pending case will reach and resolve the many muddles in existing doctrine. I have doubts about the statutory analysis in *hiQ* and *Sandvig*,[115] but my goal here isn't to judge competing CFAA interpretations.[116] Others have done so at length, and the Supreme Court might move the goalposts quite soon.[117] Instead, I hope to lay the foundations for legislative reform by showing that it's normatively desirable to chip away at platforms' gatekeeper rights. Letting platforms serve as gatekeepers for websites is a bit like letting foxes serve as guards for henhouses. Platforms, like foxes, are likely to act in their own interests, and we should be cynical

113. *See* Kerr, *supra* note 12 (emphasizing that circuit splits remain regarding the proper interpretation of the CFAA and "that only the U.S. Supreme Court can resolve" them).

114. Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 378–81 (2018) (arguing that there have been four phases in courts' jurisprudence on the question of whether the CFAA prohibits scraping); *cf.* Kerr, *supra* note 12 (observing that "[t]he Ninth Circuit's approach to the CFAA has zigzagged a bit over time").

115. *See* Sacharoff, *supra* note 11, at 580–81, 644 (arguing that "the only defensible interpretation of the CFAA" doesn't support the public–private distinction in *hiQ*, especially after Congress "wiped away any such division between private and public information" by amending the CFAA over the years). It's worth noting that the *hiQ* and *Sandvig* courts reached similar prescriptive ends through different interpretive means, at least at first. While the Ninth Circuit in *hiQ* focused on textual and historical indications that the CFAA should be limited to *intrusions* into private cyberspaces, the *Sandvig* court initially emphasized a perceived distinction between terms of service that restrict *access* to information and terms of service that restrict *uses* of information. *Compare hiQ Labs*, 938 F.3d at 999–1004, *with* Sandvig v. Sessions, 315 F. Supp. 3d 1, 22–27 (D.D.C. 2018). The *Sandvig* court later adopted much of the Ninth Circuit's reasoning in *hiQ* when ruling on the parties' cross-motions for summary judgment. *See supra* notes 100–103.

116. I also set aside my skepticism about the constitutionality of many CFAA decisions. Briefly, however, I think the First Amendment likely requires the results reached in *hiQ* and *Sandvig* because otherwise the law would restrict access to information that has already been shared with the general public. *See* Kadri, *supra* note 17, at 29–35 (fleshing out this constitutional argument).

117. *See, e.g.*, Sacharoff, *supra* note 11, at 587–97 (surveying the various interpretations of "without authorization" offered by scholars and courts); Jonathan Mayer, *The "Narrow" Interpretation of the Computer Fraud and Abuse Act: A User Guide for Applying* United States v. Nosal, 84 GEO. WASH. L. REV. 1644, 1656 & n.60 (2016) (collecting scholarship advocating for a "code-based" interpretation of "without authorization").

about trusting them with a gatekeeping role. The CFAA has given them policymaking power to make decisions affecting competition, innovation, research, and privacy. This Part explores how platforms have exploited that deference.

A. Competition Policy: Protecting Data Silos

First off, gatekeeper rights allow platforms to set competition policy by enforcing their preferred data-access rules. By empowering platforms to decide who may gather information from websites, cyber-trespass law grants them a legal right to obstruct data flows arbitrarily, giving them a competitive advantage that they can abuse. Many platforms entice people to share as much information as possible on their websites. Even when that information is posted publicly, platforms can use cyber-trespass law to prevent others from accessing it. This gatekeeper's privilege can create data silos and add value to the information—value that the platforms alone can recoup by using or selling the data.[118]

Recall that gatekeeper rights are as much about inclusion as exclusion. To see how that works in practice, consider a recent exposé about Facebook. Thanks to a cache of leaked documents, Olivia Solon and Cyrus Farivar revealed Mark Zuckerberg's plans to consolidate his platform's market dominance and control its competitors by using some publicly accessible information about its users "as a bargaining chip."[119] The documents showed how the platform used information from its users' profiles as "leverage" over other companies.[120] Facebook rewarded some partners with access to data while denying it to rivals.[121] For example, Facebook gave Amazon "special access" when the shopping platform bought Facebook advertising, but it cut off a rival's access "because it had grown too popular and could compete

118. Gregory Day & Abbey Stemler, *Infracompetitive Privacy*, 105 IOWA L. REV. 61, 67–78 (2019) (detailing the ways that platforms extract value from data).

119. Olivia Solon & Cyrus Farivar, *Leaked Documents Show Facebook Leveraged User Data to Fight Rivals and Help Friends*, NBC (Nov. 6, 2019, 9:14 AM), https://www.nbcnews.com/news/all/leaked-documents-show-facebook-leveraged-user-data-fight-rivals-help-n1076986 [https://perma.cc/2FEQ-S8XL]; *see also* Elizabeth Dwoskin, Craig Timberg & Tony Romm, *Facebook Allegedly Offered Advertisers Special Access to Users' Data and Activities, According to Documents Released by British Lawmakers*, WASH. POST (Dec. 5, 2018, 5:05 PM), https://www.washingtonpost.com/technology/2018/12/05/facebook-allegedly-offered-advertisers-special-access-users-data-activities-according-documents-released-by-british-lawmakers [https://perma.cc/5Y4Y-XWAC] ("A trove of emails and internal documents . . . illustrate how Facebook rose to dominance years ago by using people's data as a bargaining chip, undermining the social media giant's claim that changes to its business practices were motivated by a desire to protect people's privacy."). Not all of the information would have been open to the public, but a lot of valuable data is easily accessible on Facebook's websites.

120. Solon & Farivar, *supra* note 119.

121. *Id.*

with Facebook."[122] Internal communications revealed Facebook's plans to publicly frame this strategy as necessary to protect people's privacy,[123] leading Ashkan Soltani, former Chief Technologist at the Federal Trade Commission (FTC), to comment that the evidence showed both how "disingenuous the company is, and how anti-competitive some of [its] practices are."[124]

Platforms can also use the CFAA to sink other companies' competing services, as appears to have been LinkedIn's goal in blocking hiQ's access to its website. LinkedIn's Chief Executive Officer candidly admitted that his platform hoped to "leverage all this extraordinary data we've been able to collect by virtue of having 500 million people join the site."[125] After hiQ presented details of its data analytics to LinkedIn's employees at a conference, LinkedIn began developing strikingly similar services before ultimately blocking hiQ's access.[126] As the *hiQ* court concluded, there was "ample" evidence that LinkedIn's actions threatened hiQ's survival and left hiQ "no viable way to remain in business."[127] Although the preliminary injunction against LinkedIn has kept hiQ afloat, competitors in other jurisdictions might not be so lucky.

This ability to create legally enforceable data silos affects consumers as well as competitors. Platforms may use and have used their gatekeeper rights to restrict the flow of market data. Most commonly, this occurs when platforms obstruct third parties' access to pricing or product information. "Counterintuitively in the information age," Rory Van Loo notes, "businesses can block access to market information that exists openly on the web, such as Amazon's or airlines' prices."[128]

In *Southwest Airlines Co. v. Farechase, Inc.*,[129] for instance, a travel company was hauled into court for collecting information about flight times and fares from an airline's website.[130] The court endorsed the airline's CFAA claim because the airline had given the travel company "repeated warnings and requests to stop scraping" and "directly informed" the company that it

122. *Id.*

123. *Id.*

124. Dwoskin et al., *supra* note 119.

125. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 991–92 (9th Cir. 2019).

126. *Id.*

127. *Id.* at 993–94.

128. Van Loo, *Digital Market Perfection*, *supra* note 76, at 837; *see also* James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 25 (2007) (noting that courts have held that any use of a server that a business does not condone "is *ipso facto* unauthorized"); Maureen A. O'Rourke, *Shaping Competition on the Internet: Who Owns Product and Pricing Information?*, 53 VAND. L. REV. 1965, 1991–92 (2000) (explaining that businesses may claim a CFAA violation even without taking steps to conceal online product and pricing information).

129. 318 F. Supp. 2d 435 (N.D. Tex. 2004).

130. *Id.* at 437.

didn't consent to this practice.[131] Similarly, in *EF Cultural Travel BV v. Zefer Corp.*,[132] competing student travel companies squared off after one gathered pricing information from the other's publicly accessible website.[133] The court explained that this form of data collection could be prevented based merely on an "explicit statement" on the website that it was forbidden.[134]

These uses of gatekeeper rights effectively establish competition policy through what Van Loo has called "data obstruction," whereby companies use law to "freeze the flow of readily available data" and halt services that could offer consumers lower prices and better product information.[135] There have been moves, for instance, to block price-comparison tools that help patients find cheaper prescription drugs and aggregation services that let travelers view all of their loyalty-program perks in one place.[136] Airlines have even thwarted cunning attempts by companies to get better seats for passengers.[137]

My aim isn't to show that platforms always use their gatekeeper rights to set *bad* competition policy. The point is that cyber-trespass law gives them unchecked discretion to set the rules governing data access by competitors and consumers, even on publicly accessible websites. Still, it's worth noting why we might be wary to trust them with this gatekeeper role. For one thing, legally sanctioned data obstruction conflicts with established consensus in law and economics that "good legal interventions should generally remove market information asymmetries, not create them."[138] As we've seen, cyber-trespass law allows platforms to create a range of information asymmetries, selectively choosing who may gather information from their websites, when and how they may do so, and for what reasons. They may turn the tap on and off whenever they please.

---

131. *Id.* at 439–40.

132. 318 F.3d 58 (1st Cir. 2003).

133. *Id.* at 60.

134. *Id.* at 62.

135. Van Loo, *Digital Market Perfection*, *supra* note 76, at 837–38, 872.

136. Van Loo, *Rise of the Digital Regulator*, *supra* note 21, at 1286; Ron Lieber, *Swatting Down Start-Ups that Help Consumers*, N.Y. TIMES (Apr. 6, 2012), https://www.nytimes.com/2012/04/07/your-money/swatting-down-start-ups-with-consumer-friendly-ideas.html [https://perma.cc/TT7M-CV7F].

137. Ron Lieber & Susan Warren, *Southwest Makes It Harder to Jump the Line*, WALL ST. J. (June 7, 2006, 12:01 AM), https://www.wsj.com/articles/SB114964168631673304 [https://perma.cc/U6ML-N27C] (discussing Southwest Airlines' attempts to prevent companies from checking in passengers as soon as check-in opens to secure better seats); *see also* Lieber, *supra* note 136 (describing potential lawsuits that airlines could bring against a company that accesses passengers' reservations to find better seats that open up after they make their initial booking).

138. Van Loo, *Digital Market Perfection*, *supra* note 76, at 872; *see also* Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630, 631 (1979) (asserting that regulation might be warranted when "imperfect information has produced noncompetitive prices and terms").

For another, although the economics of data flows are beyond the scope of my project, it's worth noting some empirical evidence supporting the notion that greater data legibility benefits consumers. After Israel passed a law requiring brick-and-mortar grocery stores to share digitized pricing information, consumers profited.[139] A recent study of the law's effects showed not only that prices decreased by around 5%, but also that prices declined as more shoppers used price-comparison websites fueled by the new data.[140] Beyond this study, ample anecdotal evidence suggests that consumers can benefit from greater pricing transparency online. Take the example of Autoslash, a start-up that reportedly saved customers around 25% on rental cars by monitoring online prices and alerting people when to rent.[141] The major rental agencies didn't take kindly to this practice, and one by one they sought to block their cars from being shown on Autoslash.[142] Even though all of the relevant information was freely available online, the start-up couldn't risk continuing without the agencies' approval—and consumers paid the price.[143]

B. Innovation Policy: Controlling Complementary Services

Platforms may also use their gatekeeper rights to set innovation policy by deciding which complementary services will sink or swim. This might strike some computer scientists as odd given that the technical meaning of a "platform" suggests an innate openness to complementarity. As Tarleton Gillespie has explained, the "computational meaning" of a platform is "a programmable infrastructure upon which other software can be built and run" or "information services that allow developers to design additional layers of functionality."[144] Despite the term's technical connotation, cyber-trespass law contributes to the legal reality that platforms needn't embrace outside collaboration.

The pick-and-choose approach lets individual platforms dictate innovation policy, empowering them to grant or withhold permission for complementary services unilaterally. This legal regime prevents "adversarial interoperability," a phrase popularized by Cory Doctorow to refer to a new

139. Van Loo, *Digital Market Perfection*, *supra* note 76, at 872–73.

140. Itai Ater & Oren Rigbi, *The Effects of Mandatory Disclosure of Supermarket Prices* 27 (CESifo Working Paper No. 6942, 2018), https://ssrn.com/abstract=3046703.

141. Van Loo, *Digital Market Perfection*, *supra* note 76, at 837; Van Loo, *Rise of the Digital Regulator*, *supra* note 21, at 1286; Ron Lieber, *A Rate Sleuth Making Rental Car Companies Squirm*, N.Y. TIMES (Feb. 17, 2012), https://www.nytimes.com/2012/02/18/your-money/autoslash-a-rate-sleuth-makes-rental-car-companies-squirm-your-money.html [https://perma.cc/QQ9L-RAET].

142. Van Loo, *Digital Market Perfection*, *supra* note 76, at 837.

143. *Id.*

144. GILLESPIE, *supra* note 3, at 19; *see also* Tarleton Gillespie, *The Politics of 'Platforms,'* 12 NEW MEDIA & SOC'Y 347, 349–50 (2010) (presenting divergent meanings of "platform").

service that "plugs into the existing ones *without the permission* of the companies that make them."[145] Doctorow observes that adversarial interoperability "was once the driver of tech's dynamic marketplace, where the biggest firms could go from top of the heap to scrap metal in an eyeblink, where tiny startups could topple dominant companies before they even knew what hit them."[146] It helped keep incumbents on their toes, knowing that they had to innovate in order to maintain their success.

Nowadays, however, adversarial interoperability is rare and risky. A handful of platforms have achieved market dominance and have used laws like the CFAA to quash inventive add-ons to their services.[147] Consider *Facebook, Inc. v. Power Ventures, Inc*.[148] In 2008, when Facebook had around 150 million users,[149] a start-up called Power Ventures created a service to let people use multiple social networks within a single interface.[150] To make this service work, the start-up asked for people's permission to gather information from their various profiles.[151] Even though Facebook's users voluntarily provided access to their accounts, Facebook's lawyers sent a letter demanding that Power Ventures stop accessing Facebook's website.[152] When it persisted, Facebook sued under the CFAA and won

145. Cory Doctorow, *Adversarial Interoperability*, BOING BOING (Oct. 2, 2019, 5:07 PM), https://boingboing.net/2019/10/02/plug-and-play.html [https://perma.cc/QY9Z-5CJC]; *see also* Mike Masnick, *There Are Lots of Ways to Punish Big Tech Companies, but Only a Few Will Actually Help Improve the Internet*, TECHDIRT (June 14, 2019, 9:27 AM), https://www.techdirt.com/articles/20190613/02225942388/there-are-lots-ways-to-punish-big-tech-companies-only-few-will-actually-help-improve-internet.shtml [https://perma.cc/P8VY-YY5A] (discussing Doctorow's argument and concluding that "making platforms more open—forcing 'interoperability'—is certainly one way forward" to help make the internet "more dynamic and competitive"); Chris Riley, *Using Interoperability for Horizontal Competition and Data Portability*, MEDIUM (May 24, 2018), https://medium.com/@mchrisriley/using-interoperability-for-horizontal-competition-and-data-portability-6706906ce699 [https://perma.cc/GM5Z-2NSW] (discussing the competitive benefits of data portability and interoperability); *cf.* Josh Constine, *Friend Portability Is the Must-Have Facebook Regulation*, TECHCRUNCH (May 12, 2019, 12:35 PM), https://techcrunch.com/2019/05/12/friends-wherever [https://perma.cc/FDA3-JFD4] (arguing that the Federal Trade Commission "must require Facebook to offer truly interoperable data portability for the social graph" by passing regulations "forcing Facebook to let you export your friend list to other social networks in a privacy-safe way").

146. Doctorow, *supra* note 145.

147. Mark A. Lemley, *The Splinternet*, 70 DUKE L.J. 1297, 1324–25 (2021) (discussing how the CFAA and copyright law have thwarted interoperability and preserved incumbent platforms' dominance).

148. 844 F.3d 1058 (9th Cir. 2016).

149. Ami Sedghi, *Facebook: 10 Years of Social Networking, in Numbers*, GUARDIAN (Feb. 4, 2014, 9:38 AM), https://www.theguardian.com/news/datablog/2014/feb/04/facebook-in-numbers-statistics [https://perma.cc/7TYE-FU94].

150. *Facebook*, 844 F.3d at 1062.

151. *Id.* at 1067.

152. *Id.* at 1063; *see also* Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969 n.8 (N.D. Cal. 2013) (noting that Power Ventures had gathered the information from Facebook "with the consent

simply because the start-up had received "written notification from Facebook" that its complementary service was forbidden.[153] Eleven years on, Facebook now has over two billion users and Power Ventures has none.[154]

At first blush, Power Ventures' multiplatform interface might not appear particularly innovative. After all, it was merely providing a convenient way for people to access existing platforms without seeking to improve or displace them. But that needn't be the case. Take Gobo, an experiment spearheaded by media scholar Ethan Zuckerman. Gobo also offers a multi-platform interface, but its mantra—"Your social media. Your Rules."—animates its four main features in ways that are not only creative but also political.[155] First, Gobo allows you to connect multiple platforms, gathering your feeds in one place.[156] Second, Gobo lets you set rules to control your feeds, replacing the inscrutable algorithms built by existing platforms to curate what you see.[157] Third, Gobo reveals what gets hidden on your feeds, helping you understand how and why your rules affect your information diet.[158] And fourth, Gobo resists echo chambers, permitting you to solicit unfamiliar perspectives in your feeds.[159] As Zuckerman explains, Gobo puts power back in people's hands:

> Want more posts from women? Adjust a slider to set the gender balance of your feed . . . or just click on the "mute all men" button and listen to the folks who often get shouted down in online dialogs. Want to broaden the perspectives in your feed? Move the politics slider from "my perspective" to "lots of perspectives" and Gobo introduces news stories from sources you might not otherwise find.[160]

---

of users who shared their credentials" (citing Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1027 (N.D. Cal. 2012))).

153. *Facebook*, 844 F.3d at 1068; *see also id.* at 1067 (holding that access to a website becomes unauthorized once "permission has been revoked explicitly").

154. *See* Kurt Wilberding & Georgia Wells, *Facebook's Timeline: 15 Years In*, WALL ST. J. (Feb. 4, 2019, 5:30 AM), https://www.wsj.com/articles/facebooks-timeline-15-years-in-11549276201 [https://perma.cc/J4VA-SANG] (reporting that Facebook, as of December 2019, had over two billion users).

155. GOBO, https://gobo.social/ [https://perma.cc/JD52-9MS6].

156. *Id.*

157. *Id.*

158. *Id.*

159. *Id.*

160. Ethan Zuckerman, *Who Filters Your News? Why We Built Gobo.Social* (Nov. 16, 2017), https://ethanzuckerman.com/2017/11/16/who-filters-your-news-why-we-built-gobo-social/ [https://perma.cc/2BZM-8AS2]; *see also* Rachel Metz, *Social Networks Are Broken. This Man Wants to Fix Them*, MIT TECH. REV. (Feb. 9, 2018), https://www.technologyreview.com/s/610152/social-networks-are-broken-this-man-wants-to-fix-them [https://perma.cc/78GA-HX9R] ("[R]ather than making [Gobo's algorithms] a top-secret black box, we made it an open box where you can reach in and set the sliders and experiment and say, 'Oh, I like how this works. Now let me change it this way and see if it works better for me.'" (quoting Zuckerman)).

Gobo might seem too good to be true. And in today's legal landscape, it might well be. Facebook has limited Gobo's ability to attract users by allowing access to only a limited set of posts from public pages—access it could revoke at any time.[161] Under many prevailing CFAA precedents, platforms can stop initiatives like Gobo in their tracks with a single letter from their lawyers.[162]

It's true that complementary services like those offered by Power Ventures don't rest purely on accessing information that's accessible to the general public. Some features relied on users sharing access credentials, enabling an outsider to gather information from their personal feeds or profiles. In that sense, the *technical* access in *Facebook v. Power Ventures* seems different to that sought by, for example, the start-up in *hiQ v. LinkedIn* that wanted to scrape public websites.[163] But the thread binding these activities together is the role cyber-trespass law plays in creating legally enforceable gatekeeper rights. In both scenarios, outsiders had the technical ability to access information from websites—in *hiQ* because the profiles were open to the general public, in *Facebook* because users provided login details to reveal their feeds. And in both scenarios, platforms took legal action to prevent the outsiders' access by exercising their gatekeeper rights on the basis of cease-and-desist letters. Facebook succeeded where LinkedIn failed because of how the court interpreted the statute, but the underlying logic was the same: platforms were invoking cyber-trespass law to set innovation policy by legal means, not merely technical measures.

C. Research Policy: Curating External Oversight

Gatekeeper rights also allow platforms to curate external oversight by setting policies that govern outside researchers. As Facebook's former chief security officer Alex Stamos and others have warned, the CFAA's consent-based regime empowers platforms to block and chill all sorts of research that relies on information gathered from websites.[164] Amy Kapczynski,

161. Zuckerman, *supra* note 160.

162. *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067–68 (holding that disregard of a cease-and-desist letter and continued access of a platform's website supports CFAA liability); *see also* Mitch Stoltz & Andrew Crocker, *Once Again, Facebook Is Using Privacy as a Sword to Kill Independent Innovation*, ELEC. FRONTIER FOUND. (Nov. 20, 2020), https://www.eff.org/deeplinks/2020/11/once-again-facebook-using-privacy-sword-kill-independent-innovation [https://perma.cc/MU7E-JJG6] (reporting on the latest example of Facebook's "legal bullying" by invoking the CFAA "to shut down apps that give users more control over their own social media experience").

163. *See supra* subpart I(B).

164. Letter from Alex Stamos et al. to the Senate and House Judiciary Committees (Aug. 1, 2013), https://www.eff.org/document/letter-def-con-cfaa-reform [https://perma.cc/K63P-58G4] ("[T]he CFAA currently threatens and chills valuable research in the field by reaching mere

meanwhile, has protested that platforms can pair the CFAA with boilerplate contracts and terms of service to "forbid users from undertaking research that might disclose aspects of their platform's functioning."[165] This kind of independent scrutiny is crucial in the digital age.[166]

Consider the report by journalists Julia Angwin and Surya Mattu, who analyzed Amazon search results to show the e-commerce giant prioritizing its own products while concealing cheaper deals offered by competitors.[167] Or the research of data analyst Jonathan Albright, who studied Facebook activity to reveal that the 2016 Russian disinformation campaign was worse

violations of terms of use and other acts, such as security research, which cause no real harm and indeed make the public safer."); *see also* Bambauer, *supra* note 78, at 958 ("The CFAA, therefore, dangles significant risk of punishment over researchers who would like to test online services for evidence of racial bias or who would like to scrape publicly displayed information in order to put it in a more usable form for sociological research."); Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1467, 1502 (2016) ("[C]ybercrime liability is, in fact, backfiring: by chilling vital research, cybercrime law actually *reduces* computer security. . . . Prosecutors rarely charge ordinary consumers, journalists, or security researchers under cybercrime law—yet there is a widely perceived legal risk for those communities."); D. Victoria Baranetsky, *Data Journalism and the Law*, COLUM. JOURNALISM REV. (Sept. 19, 2018), https://www.cjr.org/tow_center_reports/data-journalism-and-the-law.php [https://perma.cc/69FJ-5VA3] (stating that there is evidence of stories having been "hindered or held from publication for the threat of penalty," including several reporters on record "describing stories that have been blocked because of legal concerns associated with the CFAA," such that it is clear that "the CFAA presents real obstacles to reporting a variety of important stories in the public interest"); Columbia Journalism School, *Data Journalism and the Law*, YOUTUBE (Jan. 29, 2019), https://www.youtube.com/watch?v=LWKgh7ODYec&feature=youtu.be [https://perma.cc/HK7A-RUGE] (discussing how the CFAA has discouraged and prevented journalists and academics from researching platforms); Cory Doctorow, *Cory Doctorow: Disruption for Thee, But Not for Me*, LOCUS (Jan. 7, 2019), http://locusmag.com/2019/01/cory-doctorow-disruption-for-thee-but-not-for-me/ [https://perma.cc/6X89-L7N4] ("CFAA is used to threaten, intimidate, sue, and even jail people engaged in otherwise perfectly lawful activity, merely because they have violated some term of service on the way."); JOSEPH LORENZO HALL & STAN ADAMS, TAKING THE PULSE OF HACKING: A RISK BASIS FOR SECURITY RESEARCH 9 (Mar. 2018), https://cdt.org/files/2018/04/2018-03-27-Risk-Basis-for-Security-Research-FNL.pdf [https://perma.cc/ZVQ4-3WND] (presenting empirical evidence of how security researchers avoid certain types of research for fear that they will violate the CFAA).

165. *See* Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1502–03 (2020) (observing that platform-written contracts are "dramatically amplified by overbroad laws" like the CFAA).

166. *See* Sheera Frenkel, *She Warned of 'Peer-to-Peer Misinformation.' Congress Listened*, N.Y. TIMES (Nov. 12, 2017), https://www.nytimes.com/2017/11/12/technology/social-media-disinformation.html [https://perma.cc/5SFK-UJSG] (discussing how the "small group of self-made experts" who had gathered and analyzed information on platforms to advise Congress on disinformation campaigns "is a testament to just how long tech companies have failed to find a solution to the problem").

167. Julia Angwin & Surya Mattu, *Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't*, PROPUBLICA (Sept. 20, 2016, 8:00 AM), https://www.propublica.org/article/amazon-says-it-puts-customers-first-but-its-pricing-algorithm-doesnt [https://perma.cc/4UJC-A55F].

than the platform had admitted.[168] Or the experiments by computer scientists Camila Souza Araújo, Wagner Meira Jr., and Virgilio Almeida, who uncovered Google's algorithmic racism in disproportionately showing white women in searches for "beautiful woman" and black women in searches for "ugly woman."[169] Or the analysis by Harvard Business School academics, who examined Airbnb interactions to find that guests with distinctively African American names were 16% less likely to be accepted relative to identical guests with distinctively white names.[170] Or the study by Abby Whitmarsh, who exposed the gendered dynamics of image-based sexual abuse by finding that 378 out of 396 posts on a self-styled "revenge pornography" website depicted women while only 18 depicted men.[171]

All five of these research projects relied on scraping information from publicly accessible websites. All five uncovered salient online activity. And all five posed reputational threats or prompted unwanted attention, as this kind of adversarial research often does.[172] No surprise, then, that platforms

168. Craig Timberg & Elizabeth Dwoskin, *Facebook Takes Down Data and Thousands of Posts, Obscuring Reach of Russian Disinformation*, WASH. POST (Oct. 12, 2017, 10:42 AM), https://www.washingtonpost.com/news/the-switch/wp/2017/10/12/facebook-takes-down-data-and-thousands-of-posts-obscuring-reach-of-russian-disinformation [https://perma.cc/4QJ6-EB6W]; *see also* Rob Barry, *Russian Trolls Tweeted Disinformation Long Before U.S. Election*, WALL ST. J. (Feb. 20, 2018, 3:30 PM), https://www.wsj.com/graphics/russian-trolls-tweeted-disinformation-long-before-u-s-election [https://perma.cc/9ZV2-CGS8] (presenting a new picture of the Russian disinformation campaign based on analysis of over 200,000 tweets).

169. Camila Souza Araújo, Wagner Meira Jr. & Virgilio Almeida, *Identifying Stereotypes in the Online Perception of Physical Attractiveness*, *in* 1 SOCIAL INFORMATICS 419, 420–21 (Emma Spiro & Yong-Yeol Ahn eds., 2016); *see also* Caitlin Dewey, *Study: Image Results for the Google Search 'Ugly Woman' Are Disproportionately Black*, WASH. POST (Aug. 10, 2016, 12:36 PM), https://www.washingtonpost.com/news/the-intersect/wp/2016/08/10/study-image-results-for-the-google-search-ugly-woman-are-disproportionately-black [https://perma.cc/6MBX-CQQC] (describing Araújo, Meira, and Almeida's study). For foundational work on algorithmic discrimination and oppression, see NOBLE, *supra* note 27; Latanya Sweeney, *Discrimination in Online Ad Delivery*, ACM QUEUE, Mar. 2013, at 1, 1.

170. Benjamin Edelman, Michael Luca & Dan Svirsky, *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, AM. ECON. J., Apr. 2017, at 1, 1, 7.

171. Abby Whitmarsh, *Analysis of 28 Days of Data Scraped from a Revenge Pornography Website*, EVERLASTING STUDENT (Apr. 13, 2015), https://everlastingstudent.wordpress.com/2015/04/13/analysis-of-28-days-of-data-scraped-from-a-revenge-pornography-website [https://perma.cc/8K2Q-S8Q8].

172. This unwanted attention, beyond creating bad PR, can also have legal consequences. For example, a 2016 ProPublica investigation into Facebook's advertising practices appeared to provoke a 2019 housing-discrimination lawsuit against the platform by the Department of Housing and Urban Development. *See* Julia Angwin & Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race*, PROPUBLICA (Oct. 28, 2016, 1:00 PM), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race [https://perma.cc/NSC6-AW2Z] (revealing how "Facebook's system allows advertisers to exclude black, Hispanic, and other 'ethnic affinities' from seeing ads"); Ariana Tobin, *HUD Sues Facebook over Housing Discrimination and Says the Company's Algorithms Have Made the Problem Worse*, PROPUBLICA (Mar. 28, 2019, 1:18 PM), https://www.propublica.org/article/hud-sues-facebook-housing-discrimination-advertising-algorithms [https://

have threatened legal action when researchers have failed to get advance permission before collecting information from their websites.[173] Cyber-trespass law gives weight to these legal threats and allows platforms to curate the kind of external oversight they receive.

This legal landscape has also encouraged platforms to develop radically different approaches to managing their relationships with outside researchers. Despite the major platforms' uniform policies against scraping,[174] they've selectively waived certain restrictions when it suits them. Twitter, for example, sells data access to those willing to pay.[175] Facebook, meanwhile, cherry-picks particular researchers by entering into data-sharing partnerships that permit a handful of lucky outsiders to study information on its website.[176]

---

perma.cc/96HQ-STL4] (reporting on the government's claim that Facebook violated the Fair Housing Act "by allowing advertisers to limit housing ads based on race, gender and other characteristics").

173. *See supra* note 164; *see also* Horwitz, *supra* note 10 (discussing Facebook's legal threats against New York University researchers studying political advertising); Pete Warden, *How to Split Up the US*, PETE WARDEN'S BLOG (Feb. 6, 2010), https://petewarden.com/2010/02/06/how-to-split-up-the-us [https://perma.cc/X6M2-V7KC] (presenting research about social networks based on data gathered from 210 million public Facebook profiles using crawling); Pete Warden, *How I Got Sued by Facebook*, PETE WARDEN'S BLOG (Apr. 5, 2010), https://petewarden.com/2010/04/05/how-i-got-sued-by-facebook [https://perma.cc/4TU3-76P4] (telling researcher's story of Facebook's threat to sue him for failing to "obtain prior written permission" to conduct the study and Facebook's demand that he delete the data set).

174. *See, e.g.*, *Automated Data Collection Terms*, FACEBOOK (Apr. 15, 2010), https://www.facebook.com/apps/site_scraping_tos_terms.php [https://perma.cc/4X5A-9Z5G] ("You will not engage in Automated Data Collection without Facebook's express written permission."); *Twitter Terms of Service*, TWITTER, https://twitter.com/en/tos [https://perma.cc/4BBZ-2UFR] ("[S]craping the Services without the prior consent of Twitter is expressly prohibited."); *API Terms of Use*, LINKEDIN, https://legal.linkedin.com/api-terms-of-use [https://perma.cc/QL6V-2MGH] ("You must not: . . . Scrape Content from the Services" or "[a]ccess, store, display, or facilitate the transfer of any LinkedIn content obtained through the following methods: scraping, crawling, spidering or using any other technology or software to access LinkedIn content outside the APIs."). Facebook recently celebrated the many legal actions it has taken under the CFAA to prevent scraping, highlighting the platform's "coordinated legal strategy across jurisdictions to enforce its Terms and protect its users" in at least five separate cases in the past two years. *See* Jessica Romero, *Taking Legal Action Against Data Scraping*, FACEBOOK NEWSROOM (Oct. 1, 2020), https://about.fb.com/news/2020/10/taking-legal-action-against-data-scraping [https://perma.cc/D4TB-7HV3].

175. *Twitter API*, TWITTER, https://developer.twitter.com/en/pricing.html [https://perma.cc/52XV-6ZA7]; *see also* Mylynn Felt, *Social Media and the Social Sciences: How Researchers Employ Big Data Analytics*, BIG DATA & SOC'Y, Apr. 29, 2016, at 1, 1 (discussing use of Twitter application for "data mining and analysis").

176. Columbia Journalism School, *supra* note 164 (Alex Abdo, at 1:12:06, noting that Facebook wants researchers to go through "approved channels of access" before doing any research); Gary King & Nathaniel Persily, *A New Model for Industry–Academic Partnerships*, 53 POL. SCI. & POL. 703, 703 (2020), https://doi.org/10.1017/S1049096519001021 [https://perma.cc/PHL3-AL38] (proposing a "model for industry–academic partnerships" that the authors adopted to partner with Facebook to get access to data). *But see* Craig Silverman, *Facebook Said It Would Give Detailed Data to Academics. They're Still Waiting*, BUZZFEED (Aug. 22, 2019, 9:30 PM), https://www.buzzfeednews.com/article/craigsilverman/slow-facebook [https://perma.cc/EMU4-5G74] (noting that Facebook's Social Science One initiative to share data with researchers has been plagued with delays).

Although some access might seem better than no access, it's troubling that platforms get to choose their own overseers.[177] Biases within the platforms might impede oversight from diverse groups, and platforms might favor those who conduct complimentary research over those who don't.[178] This situation, in turn, creates risks that researchers will tailor their work to protect their access to these platforms, compromising the integrity of their findings.[179] Perceptions of partiality—justified or not—leave researchers vulnerable to accusations that they're complicit in corporate propaganda.

The point isn't that researchers must be given free rein. Rather, it's that cyber-trespass law has allowed platforms to set the research agenda. The result is an atmosphere of intense distrust. As Mike Ananny and Emily Bell have complained, researchers must now go to the platforms and "stand in line for "dollops of data."[180] It's only natural to worry about the impartiality of non-adversarial research, either because the platforms might selectively disclose information or because the researchers have an incentive to stay in the platforms' good books. Worse still are the platforms' own claims about what's working and what isn't. "At the moment, they're marking their own homework," says Claire Wardle.[181] She warns that the platforms "like to tell us that the interventions they're rolling out are working, but because they write their own transparency reports, there's no way for us to independently verify what's actually happening."[182] Although Wardle acknowledges that "these companies have to play a really important role in this process," she

177. *See* Persily & Tucker, *supra* note 24, at 324 (raising concerns about "for-profit companies playing the role of gatekeeper, where the assumption would be that research making the company look bad would be more likely to be withheld").

178. *See* Yeshimabeit Milner (Yeshi), *An Open Letter to Facebook from the Data for Black Lives Movement*, MEDIUM (Apr. 4, 2018), https://medium.com/@YESHICAN/an-open-letter-to-facebook-from-the-data-for-black-lives-movement-81e693c6b46c [https://perma.cc/KT4Q-HCQ4] (proposing the "Data for Black Lives" and "Public Data Trust" initiatives to encourage Facebook to permit research from diverse researchers).

179. *See* Luigi Zingales, *Uber and the Sherlock Holmes Principle: How Control of Data Can Lead to Biased Academic Research*, PROMARKET (Oct. 9, 2019), https://promarket.org/uber-and-the-sherlock-holmes-principle-how-control-of-data-can-lead-to-biased-academic-research [https://perma.cc/MML7-XA36] ("Companies control their data. They tend to share that data with researchers who use it only in ways that are blessed by the corporations. Thus, important questions aren't answerable, or worse, the apparent answers might be biased or incomplete.").

180. *See* Ethan Zuckerman (@EthanZ), TWITTER (Nov. 14, 2019, 6:48 PM), https://twitter.com/EthanZ/status/1195141501786963971 [https://perma.cc/EU8N-RC7D] (quoting Emily Bell (@emilybell), TWITTER (Nov. 14, 2019, 7:50 PM), https://twitter.com/emilybell/status/1195142075119001601?s=20 [https://perma.cc/J5VC-QY6Z]) (noting her adoption of the "dollops of data" metaphor from Mike Ananny).

181. Claire Wardle, *How You Can Help Transform the Internet into a Place of Trust*, TED (Apr. 2019), https://www.ted.com/talks/claire_wardle_how_you_can_help_transform_the_internet_into_a_place_of_trust [https://perma.cc/4SPB-5Q7S].

182. *Id.*

correctly observes that "they can't control it" if oversight is to be meaningful.[183]

Platforms like Facebook don't seem shy about their selectivity. On the Facebook Research website, the platform proudly asserts its internal research teams "collaborate broadly with the academic community."[184] But there's a telling caveat about which collaborations the platform will pursue. In Facebook's own words, all proposals to conduct external research should "align with our mission of building community and bringing the world closer together."[185] Even if this capacious language could cover all sorts of studies, it's significant that Facebook admits that external projects must "align" with its own interests.

As I've argued elsewhere, Facebook's prior mission statement—"Making the world more open and connected"—was "a normatively questionable maxim" because the "benefits of greater openness and connection are contestable."[186] While it might seem trivial to quibble with Facebook's slogans, it matters if external research gets sidelined for contesting contestable mantras. Yet the platform's gatekeeper rights give it that preclearance power.[187] Armed with the CFAA, platforms can deter researchers from gathering information from their publicly accessible websites, and some have even stopped users from sharing information from their own feeds with researchers.[188] As gatekeepers, it's their legal right to enforce whatever policies they wish.

---

183. *Id.* Even Facebook concedes that "[n]o company should grade its own homework." Vishwanath Sarang, *Independent Audit of Community Standards Enforcement Report Metrics*, FACEBOOK NEWSROOM (Aug. 11, 2020), https://about.fb.com/news/2020/08/independent-audit-of-enforcement-report-metrics [https://perma.cc/W8AF-5Y23]. In the face of sustained criticism and pressure, the platform has pledged to allow some independent oversight over narrow slices of its operations, including an external audit planned for 2021 to assess the metrics it uses to judge enforcement of its content policies. *Id.* Although initiatives like these give researchers a glimpse behind the curtain, the nature and extent of oversight remain at the platform's whim.

184. *Research Areas*, FACEBOOK RES., https://research.fb.com/research-areas [https://perma.cc/GTN2-9XRV].

185. *Research Awards*, FACEBOOK RES., https://research.fb.com/research-awards [https://perma.cc/4WXT-VJ2W].

186. Kadri, *supra* note 19, at 1091–92.

187. Facebook adopts a similar preclearance policy for qualitative empirical work about the platform. Academics conducting interviews with Facebook employees must agree to "ask Facebook first" before using any quotes in their research. While some academics agree to give the platform review, revision, and veto powers over their work before it's published, others simply refuse to do interviews or use any quotes. I've taken the latter approach as a matter of academic integrity. To me, it's important for my readers to know that nobody at Facebook ever has the chance to sanitize or curate their words before they appear in my work.

188. *See* Jeremy B. Merrill & Ariana Tobin, *Facebook Moves to Block Ad Transparency Tools—Including Ours*, PROPUBLICA (Jan. 28, 2019, 4:29 PM), https://www.propublica.org/article/facebook-blocks-ad-transparency-tools [https://perma.cc/66L2-JK4F] (discussing Facebook's decision to block a crowdsourcing tool that allowed users to share information about the political ads on their feeds with journalists at *ProPublica*).

D. Privacy Policy: Granting Internal Immunity

Lastly, gatekeeper rights allow platforms to set privacy policies that, unsurprisingly, they don't enforce against themselves. Because the United States lacks federal legislation regulating the collection and use of data, platforms are left to make policy decisions about who may gather data and what they may do with it. Although we can't blame platforms entirely for this legislative lethargy,[189] the result is that cyber-trespass law has become a key legal instrument in setting and enforcing data-privacy rules. Even if we assume that platforms use their power to establish good privacy policies for others, one thing is clear: platforms are immune from their own rules.

Take LinkedIn's position in *hiQ*, in which the platform argued that allowing scraping on its website "threatens its members' privacy."[190] LinkedIn was itself offering third-party access to the very same information that hiQ sought from public profiles—but for a price. LinkedIn allowed recruiters to track particular users and receive alerts when those users made changes to their profiles.[191] The platform also permitted certain third parties to export data from its users' profiles, including their names, employers, and locations.[192] The CFAA's structure authorized LinkedIn to take such contradictory positions. The platform could sell its users' information to clients while still seeking to enforce a privacy policy that forbade hiQ's access to that same information.

---

189. Although their lobbying likely hasn't helped. *See* Carole Cadwalladr & Duncan Campbell, *Revealed: Facebook's Global Lobbying Against Data Privacy Laws*, GUARDIAN (Mar. 2, 2019, 9:00 AM), https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment [https://perma.cc/7WDB-HARC] (reporting that a leak of internal Facebook documents revealed that "Facebook has targeted politicians around the world . . . promising investments and incentives while seeking to pressure them into lobbying on Facebook's behalf against data privacy legislation"); Lee Fang, *Silicon Valley-Funded Privacy Think Tanks Fight in D.C. to Unravel State-Level Consumer Privacy Protections*, INTERCEPT (Apr. 16, 2019, 7:39 AM), https://theintercept.com/2019/04/16/consumer-privacy-laws-california [https://perma.cc/H2F2-NDVT] (observing that industry-funded think tanks that have "positioned themselves as expert voices on consumer privacy" were working to "push[] legislation in a direction that would have weak enforcement mechanisms, give consumers limited means for recourse, and . . . roll back state-level privacy standards being enacted by state legislatures"); Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html [https://perma.cc/36GS-AWPS] (discussing lobbying efforts by several Big Tech companies to encourage the enactment of federal data privacy laws that would be beneficial for those companies); Kartikay Mehrotra, Laura Mahoney & Daniel Stoller, *Google and Other Tech Firms Seek to Weaken Landmark California Data-Privacy Law*, L.A. TIMES (Sept. 4, 2019, 2:32 PM), https://www.latimes.com/business/story/2019-09-04/google-and-other-tech-companies-attempt-to-water-down-privacy-law [https://perma.cc/74GD-UXPH] (discussing a Google lobbyist's attempt to amend a proposed California law that would limit platforms' ability to monetize user data).

190. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 994 (9th Cir. 2019).

191. *Id.* at 994–95.

192. *Id.* at 995.

The CFAA is a poor fit for contemporary privacy interests because the law fails to protect people from the platforms they use. People rely on platforms to engage in all sorts of online activities, from socializing to shopping to networking. These activities leave digital breadcrumbs for platforms to follow.[193] Platforms usually use these breadcrumbs to feed their ad-based business models, but they might also use them to decide what speech you'll see, what prices you'll be offered, or what jobs you'll discover.[194] They could even use them to manipulate your voting behavior on election day.[195] Such practices might strike people as fraudulent and abusive, at least in a colloquial sense. But, somewhat ironically, the Computer *Fraud* and *Abuse* Act does nothing to prevent them. Under the CFAA, platforms are free to "consent" to collecting and using information stored on their own servers.

This dynamic could partially explain why no CFAA charges were brought in a recent cyber-espionage case involving Twitter. Federal prosecutors charged two former Twitter employees with acting as agents for Saudi Arabia, accusing the pair of helping the Saudi government identify and target dissidents by accessing their personal details on Twitter's internal

193. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 89 (2015) ("Today, great chunks of human society are being transformed into digital form, and we all leave digital footprints every day as we live our lives."); Olga Tokarczuk, Nobel Laureate in Literature 2018, Nobel Lecture: The Tender Narrator, at 9 (Jennifer Croft & Antonia Lloyd-Jones trans., Dec. 7, 2019), https://www.nobelprize.org/uploads/2019/12/tokarczuk-lecture-english.pdf [https://perma.cc/FZX8-XYZH] ("[T]he Internet, completely and unreflectively subject to market processes and dedicated to monopolists, controls gigantic quantities of data used not at all pansophically, for the broader access to information, but on the contrary, serving above all to program the behavior of users, as we learned after the Cambridge Analytica affair."); Jack M. Balkin, *Fixing Social Media's Grand Bargain*, LAWFARE (Oct. 24, 2018, 12:37 PM), https://www.lawfareblog.com/fixing-social-medias-grand-bargain [https://perma.cc/GHC7-4HET] ("Digital communication leaves collectible traces of interactions, choices, and activities."). Balkin goes on to explain that as a result of that communication, "digital companies can collect, analyze, and develop rich dossiers of data about end users," which "include not only the information end users voluntarily share with others, but their contacts, friends, time spent on various pages, links visited, even keystrokes." *Id.*

194. *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 8–18 (2019) (discussing the threat to human autonomy brought about by the "surveillance capitalism" underlying the platform economy); LAWRENCE LESSIG, THEY DON'T REPRESENT US 109 (2019) ("The Internet watches us. Everything we do on the Internet is captured and monetized. Everything we do is data, and data is gold.").

195. *See* Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 335–37 (2014) (discussing the possibility of "digital gerrymandering"); Zoe Corbyn, *Facebook Experiment Found to Boost U.S. Voter Turnout*, SCI. AM. (Sept. 12, 2012), https://www.scientificamerican.com/article/facebook-experiment-found-to-boost-us-voter-turnout [https://perma.cc/YDP7-PTLY] (reporting on Facebook experiment that increased voter turnout in 2010 U.S. congressional elections).

database, including allies of murdered Saudi journalist Jamal Khashoggi.[196] Even though the platform's employees accessed information from over 6,000 accounts, neither the government nor the platform has alleged any CFAA violation.[197] Why? We can't know for sure, but one reason might be that the CFAA's structure would make this a legally precarious move.[198] Twitter's own employees accessed the dissidents' information, and, as platform insiders, it's possible that they were "authorized" under the statute to do so.[199] Even if a CFAA claim by Twitter was legally viable, the structural point remains: platforms like Twitter needn't enforce their own data-privacy policies against themselves, and their status as gatekeepers would immunize them if their users tried to bring one themselves.

Beyond the lack of relief available to users under these circumstances, this legal regime also allows platforms to talk the talk of protecting privacy without walking the walk. Although there's growing public consciousness about platforms' self-serving data practices, the "illusion of privacy" supported by the CFAA might lull inattentive users into assuming that information they share with platforms won't be collected and used by others.[200] This impression misses the fact that platforms can enforce their data-privacy policies selectively. Under cyber-trespass law, they have the power to make the rules and then pardon themselves and their clients.

* * *

Simmering under the surface of this Part has been a tale about how platforms both create and extract value through their services. There's no doubt that platforms have built technological tools that are beneficial to the public. At the same time, they've relied on their users—especially

196. Ellen Nakashima & Greg Bensinger, *Former Twitter Employees Charged with Spying for Saudi Arabia by Digging into the Accounts of Kingdom Critics*, WASH. POST (Nov. 6, 2019, 3:46 PM), https://www.washingtonpost.com/national-security/former-twitter-employees-charged-with-spying-for-saudi-arabia-by-digging-into-the-accounts-of-kingdom-critics/2019/11/06/2e9593da-00a0-11ea-8bab-0fc209e065a8_story.html [https://perma.cc/47C7-C8BT].

197. *Id.*

198. *See* United States v. Nosal, 676 F.3d 854, 857–63 (9th Cir. 2012) (en banc) (ruling that an employer can't use the CFAA to sue an employee merely for using company computers for "nonbusiness purposes" but noting that other circuits have "interpret[ed] the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty").

199. *See* Jody Westby, *Twitter Employee Surveillance for Saudi Arabia Raises Questions About Company's Cybersecurity and Governance*, FORBES (Nov. 12, 2019, 1:15 PM), https://www.forbes.com/sites/jodywestby/2019/11/12/twitter-employee-surveillance-for-saudi-arabia-raises-questions-about—companys-cybersecurity-and-governance/?sh=37daeb095f1c [https://perma.cc/37Y7-59QV] (positing that the lack of CFAA charges may have been due to a concern that it would be difficult to prove that the employees' access was "actually 'unauthorized' under the CFAA").

200. *See* Jamie Williams, *EFF to Court: Accessing Publicly Available Information on the Internet Is Not a Crime*, ELEC. FRONTIER FOUND. (Dec. 11, 2017), https://www.eff.org/deeplinks/2017/12/eff-court-accessing-publicly-available-information-internet-not-crime [https://perma.cc/X2LF-6WCT] (criticizing LinkedIn's contract-based restrictions as capable of deterring "law-abiding individuals and U.S.-based companies" from accessing user data, "but nothing more").

information provided *by* their users—to make their services lucrative. One way that platforms preserve that value is by restricting access to that information, as is their prerogative under cyber-trespass law.

But as we've seen, it's a fundamentally political decision about how policymaking power should be allocated in this arena. Our laws influence the type of competition that flourishes, the type of innovation that's possible, the type of research that's available, and the type of privacy that's protected. Cyber-trespass law abdicates that political decisionmaking to platforms. These private actors enjoy broad discretion to set the rules governing key features of digital life, swallowing or stalling other regulatory regimes that might be less defined by the platforms' own interests and preferences.[201] That likely wasn't Congress's goal in expanding cyber-trespass law, but it's still the legal regime we have today.

Again, I'll stress that my claim isn't that platforms will always use their gatekeeper rights to make bad policy. Rather, it's that we should cabin the reach of cyber-trespass law to clear the way for thoughtful, targeted, and public-oriented regulation to govern these key policy questions. Whenever the law delegates decisionmaking authority to private actors, we should critically assess that power allocation. Some delegations will be good, others will be, let's say, "problematic."[202] Instead of reflexively shunning all private delegations, "we should focus on how to structure these arrangements effectively and milk their positive potential."[203]

In this case, the very nature of platforms' data-driven business models should make us hesitant to give them unchecked gatekeeper powers to set the internet's accessibility and informational rules. This cynicism is particularly sound in an environment where a few companies have gained vast market power, especially as cyber-trespass law permits them to further entrench their

201. *See* 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, 357–66 (2004) (analyzing how the CFAA's application to publicly accessible websites disrupts copyright law and threatens the free flow of information protected by that legal regime); Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 155, 159 (2013) (exploring how the CFAA has eroded the traditional boundaries between criminal law and contract law); Doctorow, *supra* note 164 (arguing that the CFAA effectively creates the legal offense of "Felony Contempt of Business-Model"); Eric Goldman, *The Computer Fraud and Abuse Act Is a Failed Experiment*, FORBES (Mar. 28, 2013, 4:21 PM), https://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer-fraud-and-abuse-act-is-a-failed-experiment [https://perma.cc/G55C-GBNZ] (discussing how "doctrinal overlaps" created by expansive CFAA liability cause convergence between cyber-trespass and trade-secret law).

202. Jody Freeman, *The Private Role in the Public Governance*, 75 N.Y.U. L. REV. 543, 586 (2000).

203. *Id.*

data-driven comparative advantages.[204] Because of network effects, economies of scale, and the scope of data collection and analysis at major platforms, we aren't operating on a clean slate. The law is facially neutral—all platforms, big and small, enjoy gatekeeper rights—but the reality is that cyber-trespass law generally rewards already-dominant platforms.

III. Restraining Digital Gatekeepers

Let's take stock of where we are. Cyber-trespass law gives platforms of all shapes and sizes a significant power: the right to act as a gatekeeper. This right gives them discretion that they've used to create policies affecting competition, innovation, research, and privacy. And this legal regime supplements the substantial deference that platforms already enjoy in other areas, from content moderation to product design to political advertising to algorithmic transparency.[205] In the United States, at least, we've largely embraced a laissez-faire approach to platforms, and cyber-trespass law is a crucial—yet underappreciated—part of that story.

Although a causal claim is hard to make, the existence of laws like the CFAA might interfere with the development of regulation in this area. Because the statute's structure and effect has given platforms the power to develop and enforce their own policy agendas, there's perhaps a sense that further regulation isn't needed because rules already exist. The time has come to disrupt that impression. At the very least, we should doubt that platforms will be public-spirited policymakers on questions of access and data. It's only natural: their very corporate essence is to maximize their data-driven profits in self-interested ways. But the law needn't leave them entirely free to do so.

Decisions like *hiQ* and *Sandvig* eroded platforms' gatekeeper rights, but judges alone can't solve the complex problems raised by these cases. If the decisions are ignored in other circuits, platforms will still enjoy the legal right to restrict access to publicly accessible websites across jurisdictions. If

---

204. The CFAA isn't the sole legal regime at play here. Dominant platforms have also used Europe's General Data Protection Regulation (GDPR) to limit outsiders' access to data. *See generally* Michal S. Gal & Oshrit Aviv, *The Competitive Effects of the GDPR*, 16 J. COMPETITION L. & ECON. 349 (2020). The combination of various legal regimes strengthens platforms' powers to play a gatekeeper role, as does the popular "exit by acquisition" funding model that pushes innovative tech startups to merge with dominant firms. *See* Mark A. Lemley & Andrew McCreary, *Exit Strategy*, 101 B.U. L. REV. (forthcoming 2021) (manuscript at 8), https://ssrn.com/abstract=3506919 (observing that modern tech companies are "quite literally swallowing up their competition" due to this now-dominant exit strategy).

205. *See, e.g.*, Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1349–50 (2018) (exploring how private ownership of automated technologies has allowed companies to withhold information about their algorithms under trade-secrets law); Thomas Kadri, *How Supreme a Court?*, SLATE (Nov. 19, 2018, 1:59 PM), https://slate.com/technology/2018/11/facebook-zuckerberg-independent-speech-content-appeals-court.html [https://perma.cc/R6CV-HBNT] (discussing the discretion platforms enjoy in governing content).

instead they become the law of the land, the pendulum will swing in the other direction because everyone will be legally free to gather troves of data from the internet. And regardless which way those precedential winds blow, platforms will retain their gatekeeper discretion to block complementary services that the public desires. We can't rely on the courts to alter these dynamics. Congress should intervene.

This Part proposes a tripartite agenda for federal legislators to pursue, drawing on proposals offered by other scholars and lawmakers. Though each piece has some independent merit, they address the concerns animating this Essay only when pursued together. Congress should begin by amending the CFAA to clarify that it doesn't apply on publicly accessible websites. Next, Congress should mandate and shield certain forms of interoperability between platforms. And finally, Congress should pass targeted laws to regulate the collection and use of publicly accessible information on websites, plugging a hole created by the first two legislative moves.

These three steps would change the locus of governance in key internet policy choices, stripping private platforms of the unbounded and trans-substantive decisionmaking power they currently enjoy over questions affecting competition, innovation, research, and privacy. It's an ambitious plan, but we must take bold steps to create a new legal framework fit for the digital age.

A. Tapering Cyber-Trespass Laws

As an initial step, Congress should amend the CFAA to clarify that the statute is inapplicable to publicly accessible websites. Although the Supreme Court might ultimately resolve the doctrinal tensions in this way, a cleaner path to uniformity would be for Congress to act. The statute's consent-based trigger made more sense at the CFAA's adoption over thirty years ago, when only 2,000 computers were connected to the internet and websites didn't even exist.[206] Granting gatekeeper rights to the tight-knit group that operated fledgling computer networks was an appropriate way to structure legal protection for those comparatively closed systems.

Applying cyber-trespass law to publicly accessible websites, by contrast, clashes with the nature of the modern internet. As we've seen, the CFAA creates incentives for platforms to act selfishly when enforcing their policy preferences. It's also difficult to judge the wisdom of their policies because the CFAA makes external research about platforms legally

206. Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969 n.8 (N.D. Cal. 2013) (noting that the CFAA was passed "well before the development of the modern internet"); Kerr, *Norms*, *supra* note 39, at 1161; Corynne McSherry, *Want More Competition in Tech? Get Rid of Outdated Computer, Copyright, and Contract Rules*, ELEC. FRONTIER FOUND. (Dec. 20, 2018), https://www.eff.org/deeplinks/2018/12/want-more-competition-tech-get-rid-outdated-computer-copyright-and-contract-rules [https://perma.cc/BS3J-4UXL].

precarious. Despite the platforms' assertions that they're setting the right rules, academics and journalists struggle to assess them independently. As Alex Abdo has argued, "we cannot trust Facebook to be the gatekeeper to the information the public needs about Facebook."[207] To make matters worse, even if we assume that a platform has adopted sound strategies to police others, the law effectively immunizes that platform within its own domain by letting it be both the rulemaker and the gatekeeper. This dynamic has become untenable. Reining in gatekeeper rights is the first step to changing it.

A statutory amendment should make clear that the CFAA doesn't cover websites that are accessible to the general public—"publicly accessible," for short. What "publicly accessible" should mean in practice is the subject of much debate among both judges and scholars. The dominant distinction embraced by both groups rests on some sort of code-based, technological barrier that effectively renders a website inaccessible to the general public.[208] Most influentially, Orin Kerr has championed a statutory interpretation of the CFAA's "without authorization" element that would effectively see the statute activated only when a website is rendered inaccessible to the general public by an authentication gate—a form of technical barrier, like a password, to ensure that only certain people may access a particular webpage.[209]

---

207. Merrill & Tobin, *supra* note 188; *see also* Alex Abdo, *Free Speech in Black Boxes*, KNIGHT FIRST AMENDMENT INST. AT COLUM. UNIV. (Feb. 6, 2020), https://knightcolumbia.org/content/free-speech-in-black-boxes [https://perma.cc/V5PA-C7JV] (describing the underappreciated control platforms have over public discourse); Jameel Jaffer, *Digital Journalism and the New Public Square*, KNIGHT FIRST AMENDMENT INST. AT COLUM. UNIV. (Oct. 18, 2018), https://knightcolumbia.org/content/digital-journalism-and-the-new-public-square [https://perma.cc/U62Z-HQ6A] ("If our collective understanding of the platforms is limited, it's in large part because the social media companies have guarded so jealously the information that would help us understand them."); *cf.* Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650, 1668 (2009) ("[I]t is important to note that sometimes the state can censor just as effectively through legal forms that are private as it can through ones that are public.").

208. *See* Mayer, *supra* note 117, at 1656 & n.60 (collecting sources and claiming that scholars have "coalesced around a theory that liability should turn on circumvention of technical protections"); Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1444–60 (2016) (exploring various interpretations of the CFAA and recommending a "narrow and 'code-based' understanding of unauthorized access"). *But see* Ric Simmons, *The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime*, 84 GEO. WASH. L. REV. 1703, 1722 (2016) (arguing that Congress should abolish the CFAA's trespass provision entirely and replace it with agency regulations); Sacharoff, *supra* note 11, at 641 (recommending that Congress should "abolish the trespass provision" of the CFAA); Annie Lee, *Algorithmic Auditing and Competition Under the CFAA: The Revocation Paradigm of Interpreting Access and Authorization*, 33 BERKELEY TECH. L.J. 1307, 1317–18 (2018) (arguing that a code-based trigger for CFAA would create its own uncertainty and vagueness).

209. Kerr, *Norms*, *supra* note 39, at 1147.

The *hiQ* and *Sandvig* courts largely embraced Kerr's proposed statutory interpretation, but one lingering uncertainty is whether *any* authentication gate is sufficient to bring the CFAA into play. The vision of a "two-realm internet" rests on a distinction between websites that require authentication and those that don't.[210] For Kerr, however, there's a caveat. While he agrees that authentication is salient, he argues that the CFAA shouldn't kick in if a particular webpage can be accessed by anyone who signs up for an account.[211] In his view, cyber-trespass law shouldn't apply when someone obtains information from a password-protected website "that actually grants access for any username and password combination."[212] He bases this argument on a view that the CFAA should account for the "norms" of cyber-trespass and that, in this scenario, courts should fashion an exception to the general "authentication principle" in order to both reflect and encourage norms of openness on the internet.[213]

Setting aside the merits of Kerr's statutory argument,[214] I agree with his caveat as a policy matter. The presence of an authentication gate shouldn't be the be-all and end-all of cyber-trespass liability; it should matter when practically anyone is allowed to create an account.[215] If it didn't, platforms would remain free to arbitrarily and selectively enforce their access rules against some people and not others, despite the fact that the information is already in the public sphere. When I post this Essay on SSRN.com, for example, nobody should have to worry about facing liability for reading it even though SSRN now prompts people to log into their password-protected accounts to view articles. SSRN likely erected this technical step to disrupt automated downloads of the many articles it hosts on its website, but anybody who creates an account can access any article. Like Kerr, I'd argue that nobody should go to jail or face civil liability for obtaining information accessible by anyone with an internet connection simply because the company has an anti-scraping preference enforced partly by requiring users to sign into an account.[216]

---

210. Sandvig v. Barr, 451 F. Supp. 3d 73, 85 (D.D.C.), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020).

211. Kerr, *Cybercrime's Scope*, *supra* note 15, at 1646.

212. *Id.*

213. Kerr, *Norms*, *supra* note 39, at 1147.

214. *See supra* note 115.

215. *See* Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1399 (2007) (proposing that courts draw on the Fourth Amendment's "reasonable expectation of privacy" test to limit the CFAA's reach, declaring access to be unauthorized only when it violates an "objective norm" that "reflect[s] the customs, practices and values of a society").

216. I explore the intricacies of these accessibility questions in greater depth in Kadri, *supra* note 17, at 7 (arguing that courts should construe the First Amendment to protect various activities on "publicly accessible" websites as a constitutional matter). Briefly, I argue that cyber-trespass law

To recap, Kerr's caveat introduces an exception to his proposed general rule that cyber-trespass law should apply only on websites behind authentication gates. As a result, the caveat seems somewhat in tension with the alternative statutory language he proposed years ago, under which CFAA liability could apply to people who "circumvent technological access barriers" to access a website.[217] Concerned about the possibility of a capacious understanding of Kerr's statutory code-based trigger, Jennifer Granick responded with amended language of her own. Her modification would distinguish between different ways of circumventing technological access barriers, pairing Kerr's language with a proviso that the barrier must "effectively control access to a computer, file, or data."[218] In a similar spirit, Christine Galbraith has proposed amendments to provide immunity for anyone accessing a website merely to obtain "information on public display," which she defines as "information available to the public without a fee, including information on publicly accessible Internet websites."[219]

The common theme connecting these proposals is that platforms should be able to do some things through code that they can't do through law. They should generally be free to create technical measures that slow down access to information that's already accessible to the general public, but they shouldn't be able to use the law to punish people once they access it, nor should the government be able to bring criminal charges based on the same

---

should have no effect on publicly accessible websites, including websites requiring people to apply and even pay for an account, so long as accounts are available to anyone who provides basic identifying information or pays a fee. There may be other legal regimes that give website owners greater control over subsequent uses of information that is placed behind paywalls, including contract and copyright law, but those regimes are subject to their own limitations—including limitations designed to harmonize them with the First Amendment. *See* Galbraith, *supra* note 201, at 324 (warning that "the CFAA unconstitutionally overrides the delicate balance of rights between authors and the public" when courts interpret the law to "allow[] website owners to protect information that is not protectable under copyright law"); *cf.* Goldman, *supra* note 201 (proposing that Congress should amend the CFAA to "[s]pecify that any textual attempts to restrict server usage fail unless the terms are presented in a properly formed contract" like a "mandatory click-through agreement").

217. *See* Orin Kerr, *Proposed Amendments to 18 U.S.C. 1030*, VOLOKH CONSPIRACY (Jan. 20, 2013, 1:10 PM), http://volokh.com/2013/01/20/proposed-amendments-to-18-u-s-c-1030 [https://perma.cc/64PB-ZMDN].

218. Jennifer Granick, *Thoughts on Orin Kerr's CFAA Reform Proposals: A Great Second Step*, STAN. CTR. FOR INTERNET & SOC'Y (Jan. 23, 2013, 9:43 PM), http://cyberlaw.stanford.edu/blog/2013/01/thoughts-orin-kerrs-cfaa-reform-proposals-great-second-step [https://perma.cc/E56R-EL8E].

219. Galbraith, *supra* note 201, at 367. *But see supra* note 216 (arguing that the payment of a fee shouldn't be legally relevant to cyber-trespass liability). Andrea Matwyshyn and Stephanie Pell have suggested replacing the CFAA entirely with a statute grounded explicitly in the idea of computer intrusion: "The Computer Intrusion and Abuse Act." *See generally* Matwyshyn & Pell, *supra* note 54, at 508–73. Because Matwyshyn & Pell's proposal explicitly disavows the trespass framework with which this Essay engages, I don't give it the attention it otherwise deserves as a smart and provocative reform proposal.

conduct. Since proposing his statutory amendments, Kerr has argued that websites must feature "virtual barriers"—and not merely "virtual speed bumps"—in order to activate CFAA liability, presumably in part to clarify his view that the technical measure must effectively restrict the general public's access to the information.[220]

The distinction between legal and technical barriers might seem pedantic, but excludability often splits along these lines. Lawrence Solum distinguishes excludability through *self-help* and excludability through *law*.[221] He observes that I can use self-help to exclude you from my land by building a fence.[222] But, he notes, self-help won't work "if I want to exclude you from copying a novel that I've written and I want to make the novel generally available for sale," partly because "[i]t would be ridiculously expensive to hire a guard to monitor each copy or every photocopy machine."[223] The government, however, could "make unauthorized copying a criminal offense or actionable civil wrong, thereby creating exclusion through law."[224] As Solum's fence example shows, sometimes self-help exclusion and legal exclusion are complementary, as the erection of that physical barrier around your land can support a claim of tortious or criminal trespass.[225] But excludability needn't be reciprocal in this way. It's a political choice whether to supplement self-help exclusion with legal exclusion.

In the context of publicly accessible websites, we've seen why it's risky to trust platforms with legal gatekeeping powers. Now is the time to rescind those rights. I favor Granick's and Galbraith's proposals because they give greater clarity that the CFAA wouldn't apply on websites that are accessible to the general public, including password-protected websites that are effectively open to all. Both amendments would taper platforms' gatekeeper rights, removing their ability to enforce their policy preferences on websites that they make accessible to the general public. Congress should use these proposals as models for an amended cyber-trespass law.

Would these amendments cause platforms to conceal their websites behind technical barriers, making more information inaccessible to the general public? For many reasons, I doubt it. For starters, it would probably reduce the platforms' user bases, thereby hurting their data-driven profits. In

220. *See* Kerr, *Norms*, *supra* note 39, at 1161, 1147 (arguing that "limited efforts to regulate access such as terms of use, hidden addresses, cookies, and IP blocks" should not "overcome the basic open nature of the Web").

221. Lawrence Solum, *Public and Private Goods*, LEGAL THEORY LEXICON (Oct. 20, 2019), https://lsolum.typepad.com/legal_theory_lexicon/2004/03/legal_theory_le.html [https://perma.cc/TUX9-SGQP].

222. *Id.*

223. *Id.*

224. *Id.*

225. *See, e.g.*, V.B. v. State, 959 So. 2d 1252, 1254 (Fla. Dist. Ct. App. 2007) (holding that no trespass had occurred because the land in question wasn't adequately enclosed by fencing).

some cases, inaccessibility would also be antithetical to a platform's very function, purpose, or ethos. And in other cases, it would annoy users and open up space for competition. But even if some platforms decided to erect greater barriers, would it be the worst thing for users to have more choices between the types of online services they can use? I think not, and indeed the second step to this legislative agenda furthers that very goal.

B. Stimulating Adversarial Interoperability

Amending the CFAA is a necessary but insufficient step to cure the present defects in cyber-trespass jurisprudence. Under prevailing law, each platform still enjoys the power to stop its users from using a complementary service that harnesses their existing social networks. To undo these decisions, Congress should pass legislation to mandate and shield forms of adversarial interoperability between platforms.

Platforms have relied on the CFAA to frustrate services offering new forms of social interactions that appeal to their users. Due to the network effects underlying many platforms' success, people are loath to experiment with new players unless enough of their friends or colleagues do too. Interoperability is one way to counteract these high switching costs, and protecting adversarial interoperability ensures that the existing platforms don't retain a veto power over innovation that threatens their market dominance.

Returning to Zuckerman's Gobo experiment helps to illuminate the stakes. As things stand, anyone seeking to create a platform that interacts with Facebook content faces a Sophie's Choice fit for the digital age. They must either ask Facebook's permission, knowing that it may be denied or withdrawn for any reason at the drop of a hat; or they must plow ahead, risking major legal exposure and relying on public opinion as protection. As Zuckerman concedes, if his team tries to show a user's Facebook feed on Gobo's platform, "we expect Facebook to sue us."[226] Zuckerman is bullish about this prospect:

> They sue other people who try to do social network aggregators. But we're looking forward to that. . . . I need Facebook to sue the Gobo team, that's the point. I need to create a tool that works across different social network[s] and when Facebook blocks us, we can say look, these other networks allow us to do this, why is Facebook the only network that isn't permitting this? Why is Facebook not committed to this open-source academic project?[227]

226. *Interview: MIT's Ethan Zuckerman Says 'Be Angry and Engage,'* NEWS LENS (Nov. 17, 2018), https://international.thenewslens.com/article/108378 [https://perma.cc/79FJ-V5DT].

227. *Id.*

Zuckerman's bravado must be read contextually. He probably knew that his then-employer—the mighty Massachusetts Institute of Technology—had savvy lawyers and deep pockets, as well as a cache of rhetorical power to go toe-to-toe with Facebook in the court of public opinion before the platform would go to a court of law. But other entities, particularly fledgling start-ups in über-competitive Silicon Valley, won't be willing to risk similar provocations. They'll have to seek Facebook's blessing and fold if it's denied.

The law can change these dynamics. Scholars have long advocated for legal tools to stimulate greater interconnection between networked technologies.[228] At the turn of the century, James Speta presciently proposed a "general interconnection obligation for Internet carriers," including a requirement of "interoperability at the core of instant messaging technology."[229] Calls have grown stronger in recent years as a cadre of platforms has tightened its grip on the market for online communications.[230] Przemek Pałka, for example, has boldly imagined a "world of fifty facebooks," in which "numerous companies would offer interoperable services" of the kind currently offered by Facebook.[231] Pałka urges legislators to pass laws requiring any platform like Facebook "to give potential competitors access to its platform and network," thereby freeing other platforms "to offer similar and complementary services" and promoting competition on "price, quality, and innovation."[232]

In a similar vein, Mike Masnick has pitched a return to an internet of "protocols, not platforms."[233] While the early internet featured many different protocols—"instructions and standards that anyone could then use to build a compatible interface"—we now have an internet dominated by "controlled platforms that are privately owned."[234] In true gatekeeper style, these platforms "have built up walls around them, locking users in."[235] Masnick's

228. *See, e.g.*, Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 604 (1998) (endorsing interoperability as a possible solution to problems posed by network effects).

229. James B. Speta, *A Common Carrier Approach to Internet Interconnection*, 54 FED. COMM. L.J 225, 228–29 (2002).

230. *See* Barrie Sander, *Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation*, 43 FORDHAM INT'L L.J. 939, 986–87 (2020) (discussing various contemporary proposals).

231. Przemysław Pałka, *The World of Fifty (Interoperable) Facebooks*, 51 SETON HALL L. REV. (forthcoming 2021) (manuscript at 1), https://ssrn.com/abstract=3539792.

232. *Id.* (manuscript at 4).

233. Mike Masnick, *Protocols Not Platforms: A Technological Approach to Free Speech*, KNIGHT FIRST AMENDMENT INST. AT COLUM. UNIV. (Aug. 21, 2019), https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech [https://perma.cc/7XR6-ESGG].

234. *Id.*

235. *Id.*

protocols-based internet "would push the power and decision making out to the ends of the network, rather than keeping it centralized among a small group of very powerful companies," giving people choice among different interfaces and rules to suit their preferences.[236] His vision involves a technical change, not a legal one, but the spirit of his proposal could be stimulated by legislation.

Jonathan Zittrain, meanwhile, has raised the idea of "feed recipes," which would give people greater control over what they see on social media.[237] Those disinclined to manage their own diets could rely on feed recipes made by people or organizations that they trust.[238] Much like Zuckerman's Gobo platform, Zittrain's feature would create "slices" of platforms' services to "introduce littleness within the bigness," instead of breaking up or replacing large platforms entirely.[239] Rather than having platforms exclusively set the menu, people could sample complementary services that are more to their taste.

Finally, Michal Gal and Daniel Rubinfeld's work on "data standardization" has explored the technical hurdles that legislated interoperability would have to overcome.[240] They've shown how standardizing certain types of data is an essential step to enable the "cross-firm and cross-industry data exchanges" necessary for data portability and interoperability between platforms.[241] They acknowledge that standardization can raise privacy concerns—"[t]he easier it is to share data, the greater the concern that private data will fall into more hands"[242]—but they offer compelling proposals for how government could facilitate privacy-protective data standardization through legislation.[243] Their work is essential reading for lawmakers considering mandatory interoperability.

New legislation is already gesturing in the right direction. The bipartisan "Augmenting Compatibility and Competition by Enabling Service Switching" (ACCESS) Act would force platforms with 100 million monthly users to let people download their data or transfer it to another service.[244] To

---

236. *Id.*

237. Columbia Journalism School, *Peter Zenger Lecture with Jonathan Zittrain*, YOUTUBE (Nov. 13, 2018), https://youtu.be/asENunfEKYY?t=1881 [https://perma.cc/TN8C-MRKQ] (speaking at ~31:30).

238. *Id.*

239. *Id.*

240. *See* Michal S. Gal & Daniel L. Rubinfeld, *Data Standardization*, 94 N.Y.U. L. REV. 737, 747–49 (2019) (identifying three primary obstacles to data portability and interoperability).

241. *Id.* at 740.

242. *Id.* at 756.

243. *Id.* at 764–69.

244. Augmenting Compatibility and Competition by Enabling Service Switching Act of 2019, S. 2658, 116th Cong. §§ 2(7)(b), 3(a) (2019); *see also* Adi Robertson, *How Would Opening Up*

carry out this mandate, the platforms must maintain interfaces to enable secure data transfers and provide data in a "commonly used," "machine-readable format."[245] Although Europe's General Data Protection Regulation already requires some degree of data portability, the ACCESS Act goes further by forcing platforms to create new interfaces that their competitors can access.[246] In short, the bill "ensures that users will not be stuck in the walled garden of particular private platforms."[247]

But mandating interoperability through these technical interfaces is just the tip of the iceberg. The ACCESS Act would also allow people to enlist a third-party data custodian to serve as an intermediary to manage their relationships with multiple platforms.[248] These custodians would have to register with the FTC and meet ethics and security standards.[249] Under the Act, platforms may block a custodian's access only if it "repeatedly facilitates fraudulent or malicious activity."[250] Platforms may also charge "reasonable" fees if another service exceeds a "reasonable threshold" of access through their interfaces.[251] But crucially, platforms can't shut out their adversaries willy-nilly, as they've done in the past.[252]

The beauty of this approach is that it meshes with the dominant platforms' existing plans to become *internally* interoperable, giving those platforms less rhetorical sway when they complain—as they surely will—that the law goes too far. In a recent blogpost, Mark Zuckerberg teed up plans to connect WhatsApp, Facebook, and Instagram messaging by saying that people "should be able to use any of our apps to reach their friends, and they

Facebook Change the Internet?, VERGE (Oct. 23, 2019, 9:02 AM), https://www.theverge.com/2019/10/23/20926792/facebook-access-act-interoperability-data-portability-warner-hawley-bill-explainer [https://perma.cc/23E8-DRPT] (explaining that the ACCESS Act would cover Facebook, Twitter, Pinterest, and other sizeable platforms).

245. S. 2658, 116th Cong. § 3(a) (2019).

246. *Id.* § 4(a); *see also* Gal & Rubinfeld, *supra* note 240, at 750 (noting how these interfaces, known as Application Programming Interfaces (APIs), rely on data standardization); Chinmayi Sharma, *Concentrated Digital Markets, Restrictive APIs, and the Fight for Internet Interoperability*, 50 U. MEMPHIS L. REV. 441, 450–61 (2019) (exploring the benefits APIs can have on competition in digital markets). *But see* Daphne Keller, *Who Do You Sue? State and Platform Hybrid Power over Online Speech*, LAWFARE (Jan. 29, 2019, 2:37 PM), https://www.lawfareblog.com/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech [https://perma.cc/M83T-F4XB] (presenting a skeptical view of what she calls the "magic APIs" model).

247. John Bergmayer, *The ACCESS Act Would Give Internet Users More Options*, PUB. KNOWLEDGE (Oct. 22, 2019), https://www.publicknowledge.org/blog/the-access-act-would-give-internet-users-more-options [https://perma.cc/JWC8-96RT].

248. S. 2658, 116th Cong. § 5 (2019).

249. *Id.* § 5(c), (f).

250. *Id.* § 5(e).

251. *Id.* § 4(c)(2)(B)(i).

252. *See* Robertson, *supra* note 244 (discussing how platforms have "weaponize[d] API access to cut off competitors" as when Facebook "did serious damage" to new social network Vine by revoking access to Facebook's friend-finding system).

should be able to communicate across networks easily and securely."[253] Zuckerberg loves interoperability, but only when it keeps people within the Facebook empire. The ACCESS Act would lessen his ability to enforce his preferences.

The ACCESS Act is a promising start. But without additional safeguards, it won't adequately shield *adversarial* interoperability, especially if platforms can still wield laws like the CFAA and the Digital Millennium Copyright Act to discourage innovation that imperils their business interests.[254] Interoperability legislation should clearly supplant other legal regimes that might scupper adversarial interoperability, including state-law torts like trespass to chattels that some courts have flagged as a plausible alternative to a narrowed CFAA.[255] The ACCESS Act's directives also rest on the existing repository of online information, but Congress should consider requiring platforms to make additional digital disclosures that would benefit consumers.[256] Lastly, the Act should ensure that services offered by the nascent data-custodian industry are affordable. A privacy law recently proposed by Senator Ron Wyden allows lower-income Americans to apply for funds from the Federal Communications Commission to subsidize certain "privacy-friendly services."[257] The ACCESS Act should include similar

253. Mark Zuckerberg, *A Privacy-Focused Vision for Social Networking*, FACEBOOK (Mar. 6, 2019), https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634 [https://perma.cc/KKH7-8CU7].

254. *See* Cory Doctorow, *Regulating Big Tech Makes Them Stronger, So They Need Competition Instead*, ECONOMIST (June 6, 2019), https://www.economist.com/open-future/2019/06/06/regulating-big-tech-makes-them-stronger-so-they-need-competition-instead [https://perma.cc/B8FR-FLRT] [hereinafter Doctorow, *Regulating Big Tech*] (proposing an "absolute" legal defense for adversarial interoperability that would block claims for "tortious interference, bypassing copyright locks, patent infringement and, of course, violating terms of service"); Cory Doctorow, *The Company Behind* Fortnite *Is Waging a Righteous War Against Apple*, SLATE (Aug. 17, 2020, 3:30 PM), https://slate.com/technology/2020/08/epic-fortnite-apple-app-store-lawsuit-dmca.html [https://perma.cc/3QWM-QMCV] [hereinafter Doctorow, *Righteous War*] (criticizing how copyright law gives technology companies "the power to control 'interoperability'—that is, which products work with theirs, and how").

255. *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1004 (9th Cir. 2019) (noting that "state law trespass to chattels claims may still be available" even if the CFAA doesn't apply on publicly accessible websites); *see also* Goldman, *supra* note 201 (arguing that "reforming the CFAA is an incomplete solution" unless Congress also preempts analogous state laws).

256. *See* Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. PA. L. REV. 1311, 1387–88 (2015) (proposing that retailers be required to make prices and product information available in machine-readable form to allow third-party services to help consumers find the best deals); Van Loo, *Digital Market Perfection*, *supra* note 76, at 838, 872–73 (arguing that legislatures should pass laws to promote access to information about products and prices).

257. Press Release, Ron Wyden, U.S. Sen. for Or., Wyden Announcement Regarding Proposed New Data Privacy Legislation (Oct. 17, 2019), https://www.wyden.senate.gov/news/press-releases/wyden-introduces-comprehensive-bill-to-secure-americans-personal-information-and-hold-corporations-accountable [https://perma.cc/DL6S-FRTW].

provisions. As Wyden said in announcing his bill, it's essential that "privacy does not become a luxury good."[258]

Even if Congress fails to facilitate interoperability through legislation, antitrust enforcement could command it for certain platforms instead of breaking them up.[259] There appears to be some appetite for this move on Capitol Hill. Representative David Cicilline, chair of the House Judiciary Committee's Antitrust Subcommittee, has complained that platforms—and not people—currently have the "final say" over whether "key information" can be used by competing or complementary services.[260] Cicilline has championed pro-competitive policies to open up the incumbent "walled gardens" that have deterred competitors from entering the market and benefiting consumers.[261] Similar initiatives have support across the pond as well, with European regulators and academics already advocating analogous proposals as part of the antitrust toolkit.[262] The United States should follow suit.

---

258. *Id.*

259. Fiona Scott Morton, *Why 'Breaking Up' Big Tech Probably Won't Work*, WASH. POST (July 16, 2019, 1:41 PM), https://www.washingtonpost.com/opinions/2019/07/16/break-up-facebook-there-are-smarter-ways-rein-big-tech [https://perma.cc/WFR9-9ZJM] (arguing that "requiring that Facebook enable open interconnection between itself and any new market entrant" would be better for consumers and innovation than simply breaking up Facebook); Doctorow, *Regulating Big Tech*, *supra* note 254 (advocating the use of antitrust law to promote interoperability); *see also* Sharma, *supra* note 246, at 477–506 (urging the Federal Trade Commission to regulate anticompetitive APIs). *But see* Rory Van Loo, *In Defense of Breakups: Administering a "Radical" Remedy*, 105 CORNELL L. REV. 1995, 2006–12 (2020) (comparing corporate breakups to access remedies to show why breakups might sometimes be preferable); Rory Van Loo, *Stop with the Egg Metaphor in Discussing Big Tech Break-Ups*, HILL (July 29, 2020, 9:00 AM), https://thehill.com/opinion/technology/509511-stop-with-the-egg-metaphor-in-discussing-big-tech-break-ups [https://perma.cc/N4VG-YGFF] (arguing that access mandates, unlike breakups, "leave the monopoly in place" and are "unlikely to deter anticompetitive behavior," but stressing that "access mandates have a place in the antitrust arsenal").

260. David N. Cicilline & Terrell McSweeny, *Competition Is at the Heart of Facebook's Privacy Problem*, WIRED (Apr. 24, 2018, 8:00 AM), https://www.wired.com/story/competition-is-at-the-heart-of-facebooks-privacy-problem [https://perma.cc/Q2FK-A5N7].

261. Kevin Bankston, *How We Can 'Free' Our Facebook Friends*, NEW AM. (June 28, 2018), https://www.newamerica.org/weekly/edition-211/how-we-can-free-our-facebook-friends [https://perma.cc/F978-YAPA]; *see also* Cicilline & McSweeny, *supra* note 260 ("This friction effectively blocks new competitors—including platforms that might be more protective of consumers' privacy and give consumers more control over their data—from entering the market.").

262. *See* Margrethe Vestager, OECD/G7 Conference, Paris: Competition and the Digital Economy (June 3, 2019), https://wayback.archive-it.org/12090/20191129200956/https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-and-digital-economy_en [https://perma.cc/XZX9-W6A3] (arguing that "interoperability—making sure that products made by one company will work properly with those made by others—can be vital to keep markets open for competition"); Foo Yun Chee, *Force Tech Giants to Share Data Rather Than Break Them Up: Academics*, REUTERS (Apr. 4, 2019, 7:43 AM), https://www.reuters.com/article/us-eu-antitrust-technology/force-tech-giants-to-share-data-rather-than-break-them-up-academics-idUSKCN1RG1IF [https://perma.cc/E37D-6GXD] (reporting that three academics appointed by

C. Regulating Data Gathering

If Congress facilitates data collection and interoperability in the ways I propose, it will become essential for legislators to pass a comprehensive data-privacy law as well.[263] The United States still lacks legislation to regulate privacy in many aspects of our daily lives. Now that both California and the European Union have passed sweeping data-privacy laws, Congress faces significant pressure to act if it wants any say regarding the nature of digital privacy.[264]

As Congress addresses data-privacy protections, a few points are important. First, lawmakers must pay close attention to the particular harms caused by data collection and aggregation.[265] Careless assumptions that all uses of data are harmful allow platforms to hum the tune of privacy when there is little privacy interest at stake. Second, Congress should aim for a "holistic architectural solution" to problems posed by data collection instead of the "piecemeal" solution offered by laws like the CFAA.[266] And third, any legislation must be careful not to impose onerous compliance burdens that only the giant platforms can realistically meet, for doing so will only cement their dominance and squelch any chance of competition.[267]

Margrethe Vestager, the European Competition Commissioner, recommended that the Commission consider forcing the tech giants to share data rather than breaking up the companies).

263. *See* Elettra Bietti, *Competition, Data and Interoperability in Digital Markets*, PRIVACY INT'L (Aug. 20, 2020), https://www.privacyinternational.org/explainer/4130/explainer-competition-data-and-interoperability-digital-markets [https://perma.cc/8757-LYUP] (arguing that "[i]nteroperability measures, even in their most effective and radical forms, must be combined with other regulation including data protection").

264. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1690–92 (2020) (explaining the pressure on the United States to pass data-privacy regulations following laws in California and Europe).

265. *See* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 115 (2014) (arguing that concerns raised by data collection are better addressed through legislation that regulates harmful uses of aggregated information); *see also* Day & Stemler, *supra* note 118, at 80–86 (cataloguing the harms that can flow from platforms' data practices).

266. *Cf.* RICHARDS, *supra* note 193, at 162 (making an analogous argument about the limits of certain privacy torts to protect privacy interests in the digital age); *see also* Hartzog & Richards, *supra* note 264, at 1688–89 (arguing for legislation that takes a "comprehensive approach" to privacy focused on "power asymmetries, corporate structures, and a broader vision of human well-being").

267. In this regard, the recently proposed Online Privacy Act of 2019 seems like a promising effort. Introduced by two Silicon Valley lawmakers, Anna Eshoo and Zoe Lofgren, the Act creates privacy rights for internet users and establishes a new federal agency to enforce its protections and investigate abuses. Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019). The bill enjoys the support of Shoshana Zuboff, whose influential work on "surveillance capitalism" has explored the platform economy's worrying effects on privacy and autonomy. ZUBOFF, *supra* note 194, at 8–18. Zuboff has called the Online Privacy Act a "significant milestone" that would serve "the rights of individuals and the aspirations of a democratic society." Press Release, Anna G. Eshoo, Congresswoman for Cal.'s 18th Cong. Dist., Eshoo and Lofgren Announcement of the Introduction of the Online Privacy Act (Nov. 5, 2019), https://eshoo.house.gov/media/press-releases/eshoo-

Most crucially, legislation should ensure that the law applies to the platforms' own treatment of their users' data. Laws like the CFAA effectively exempt platforms from responsibility for privacy harms that occur in their own backyards. Between the CFAA's consent-based trigger and the flawed "notice and choice" framework of privacy protection that has reigned in the United States,[268] platforms are essentially inoculated against legal liability when they implement harmful data practices. But as we've seen, platforms can engage in suspect practices when they harvest their own users' data. To name but one example, it has emerged that Facebook gathered information from around 1.5 million users' email contact books after asking for their email passwords to "verify" their Facebook accounts.[269] The platform then used the information to improve its ad-targeting algorithms.[270] So far, Facebook appears to have faced no legal consequences for this serious breach of trust.[271]

A pressing situation provides insights into the data-privacy reforms that Congress should pursue: the rise of facial-recognition technologies. When once-obscure company Clearview AI suddenly found itself on the front page of the *New York Times* thanks to Kashmir Hill's investigative reporting, the legal implications of scraping were thrust into public discourse.[272] Clearview AI had spent the last few years collecting over 3 billion photos from platforms like Facebook, YouTube, and Twitter to develop facial-recognition algorithms, selling its services to hundreds of companies and police departments around the country.[273]

---

lofgren-introduce-online-privacy-act [https://perma.cc/XB65-MD8E]. High praise from a preeminent critic of the status quo.

268. For critiques of the "notice and choice" framework, which relies on lengthy and opaque privacy policies as a form of data protection, see generally ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016); Neil Richards & Woodrow Hartzog, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579, 586–88 (2017); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

269. Rob Price, *Facebook May Have Broken the Law by Harvesting 1.5 Million Users' Email Contacts, Experts Say*, BUS. INSIDER (Apr. 18, 2019, 6:14 PM), https://www.businessinsider.com/experts-facebook-law-harvesting-1-5-users-email-contacts-2019-4 [https://perma.cc/5GNX-ZT43].

270. Mike Isaac, *New York Attorney General to Investigate Facebook Email Collection*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/technology/facebook-new-york-attorney-general-investigation.html [https://perma.cc/2GPN-KP5S].

271. The only fallout appears to be an investigation by New York's attorney general, though that appears to have gained little traction to date. *See id.*

272. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/W26F-MVQR].

273. Sacharoff, *supra* note 11, at 585–86.

Armed with Clearview AI's technology, police can, for example, upload a photo of a person captured by a surveillance camera and discover their name and other information, including their accounts on social media.[274] Beyond this use by law enforcement, the technology enables a frightening level of invasive surveillance.[275] The concern with facial-recognition technology doesn't boil down to a simple question of effectiveness. As Philip Agre warned years ago, facial recognition "will work well enough to be dangerous, and poorly enough to be dangerous as well."[276] When it works well, it robs us of our privacy interests in obscurity in public.[277] And when it works poorly, it subjects people to suspicion based on actions they never took.

Clearview AI's technology provides an illustrative example that Congress should consider when crafting data-privacy laws. The company's practices reveal that privacy harms can flow even when data is obtained from publicly accessible websites. Scholars like danah boyd have long made this point:

> Collecting data about people isn't in and of itself a violation of privacy, but piecing it all together and using it to stare is a serious violation of privacy norms. Which is why people scream privacy foul. It's the difference between recognizing that there are others in the locker room and staring at them as they get dressed.[278]

If Congress (or the courts) remove cyber-trespass liability for scraping publicly accessible websites, Clearview AI serves as a cautionary tale. Congress should plug the regulatory hole with targeted laws identifying and regulating specific harms that flow from the collection and use of data, including data that's openly available on the internet.

Lastly, in mulling over potential privacy laws, legislators should pay attention to technological changes that might soon affect how we communicate online. As part of an effort to stave off regulation, prominent platforms are fiddling with their architectures and refocusing their services

---

274. *Id.* at 586.

275. For superb work on the harms enabled by facial-recognition technology, see Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 101, 104 (2019); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1485 (2019); Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/5CKG-SEZ4].

276. Philip E. Agre, *Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places*, UCLA GSEIS (Sept. 10, 2003), https://pages.gseis.ucla.edu/faculty/agre/bar-code.html [https://perma.cc/K3MK-A2RE].

277. *See* Woodrow Hartzog & Evan Selinger, *Why You Can No Longer Get Lost in the Crowd*, N.Y. TIMES (Apr. 17, 2019), https://www.nytimes.com/2019/04/17/opinion/data-privacy.html [https://perma.cc/JMB6-8W7C] (discussing the importance of obscurity and noting that "[t]hreats to our obscurity are growing" due to advances in technology).

278. danah boyd, Address at Personal Democracy Forum: Networked Privacy (June 6, 2011), https://www.danah.org/papers/talks/2011/PDF2011.html [https://perma.cc/NFV6-F523].

in ways that purportedly serve privacy interests. Facebook, for instance, is reorienting its services—including its popular messaging and photo-sharing applications, WhatsApp and Instagram—to prioritize encrypted and secluded communicative forums.[279] In launching a new "privacy-focused vision" for his company, Mark Zuckerberg claimed that Facebook and Instagram had historically "helped people connect with friends, communities, and interests in the digital equivalent of a town square," but that "people increasingly also want to connect privately in the digital equivalent of the living room."[280] He expressed his belief that "we should be working towards a world where people can speak privately and live freely knowing that their information will only be seen by who they want to see it."[281] Zuckerberg predicts that, over the next five years, "we're going to see all of social networking reconstituted around this base of private communication"—and his "predictions" have the ability to reshape online discourse in fundamental ways.[282]

These shifts in the social-media ecosystem should dovetail with changes in the regulatory frameworks that shape that ecosystem. As platforms increasingly differentiate between public and private cyberspaces, so too should the law. The two moves can be mutually reinforcing: the distinctions that platforms create between public and private forums can guide actors within the legal system who draft and implement legislation, and laws can encourage platforms to adopt robust technological barriers by hinging legal protections on the ability to effectively seclude private cyberspaces. Under current CFAA doctrine, platforms can claim to be serving privacy interests by merely forbidding certain activities through their terms of service or sending cease-and-desist letters. This is inadequate. The law can and must create better incentives for platforms to build privacy-protective architecture.

Conclusion

We don't let foxes guard henhouses because we can't trust them to do the job well. Likewise, we should stop giving platforms so much legal power to police their websites.

---

279. Zuckerberg, *supra* note 253.

280. *Id.*

281. *Zuckerberg Outlines Plan for 'Privacy-Focused' Facebook*, BBC (Mar. 7, 2019), https://www.bbc.com/news/world-us-canada-47477677 [https://perma.cc/63UC-V737].

282. *At Harvard Law, Zittrain and Zuckerberg Discuss Encryption, 'Information Fiduciaries' and Targeted Advertisements*, HARV. L. TODAY (Feb. 20, 2019), https://today.law.harvard.edu/at-harvard-law-zittrain-and-zuckerberg-discuss-encryption-information-fiduciaries-and-targeted-advertisements [https://perma.cc/3J2M-TVH4]; *see also* Nick Statt, *Facebook Is Redesigning Its Core App Around the Two Parts People Actually Like to Use*, VERGE (Apr. 30, 2019, 1:30 PM), https://www.theverge.com/2019/4/30/18523265/facebook-events-groups-redesign-news-feed-features-f8-2019 [https://perma.cc/HBE8-27D8] (detailing Facebook's plans to redesign its mobile application to highlight private forums like closed events and groups instead of its more public-oriented newsfeed).

The CFAA is part of a broader trend that pervades internet regulation: legislatures and courts have delegated rulemaking and enforcement authority to platforms by dint of intent or inertia.[283] Private delegation isn't always bad, but regulators should rely on it only when it's likely that platforms will use that leeway responsibly.[284] Platforms, however, have failed to use their gatekeeper rights in ways worthy of our trust. How could we expect otherwise? The incentives are fundamentally misaligned.

The CFAA's scope is closely tied to the type of internet we have now and the type we'll get in the future.[285] If companies continue to use the law to act as gatekeepers, "it will threaten open access to information for everyone."[286] It doesn't need to be this way. Although legislative paralysis appears endemic in our politics, there's reason to be optimistic that Congress might actually step up in this arena.[287] We're in the midst of what Woodrow Hartzog and Neil Richards have called a "constitutional moment" for online privacy, "on the cusp of a set of legal changes that will structure our emergent digital society for decades to come."[288] This constitutional moment extends beyond privacy to cybersecurity, competition, and transparency. Lawmakers must seize this moment to pass laws fit for our times—laws that will "fix the internet, not the tech companies."[289] Let's stop trusting platforms to act in our best interests as digital gatekeepers. Let's stop letting these foxes guard henhouses.

283. *See* Keller, *supra* note 246 (discussing ways that governments have "laundered" state action through private platforms).

284. Freeman, *supra* note 202, at 586.

285. Michael J. Madison, *Authority and Authors and Codes*, 84 GEO. WASH. L. REV. 1616, 1620 (2016).

286. Jamie Williams, *'Scraping' Is Just Automated Access, and Everyone Does It*, ELEC. FRONTIER FOUND. (Apr. 17, 2018), https://www.eff.org/deeplinks/2018/04/scraping-just-automated-access-and-everyone-does-it [https://perma.cc/LPJ3-5TDC].

287. Indeed, bipartisan amendments to the CFAA were proposed in April 2015. *See* Data Breach Notification & Punishing Cyber Criminals Act of 2015, S. 1027, 114th Cong. § 5 (2015) (proposing to double the potential sentences under the CFAA).

288. *See* Hartzog & Richards, *supra* note 264, at 1687, 1693.

289. Cory Doctorow, *Interoperability: Fix the Internet, Not the Tech Companies*, ELEC. FRONTIER FOUND. (July 11, 2019), https://www.eff.org/deeplinks/2019/07/interoperability-fix-internet-not-tech-companies [https://perma.cc/6RY8-63WJ]; *cf.* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019) (arguing that structural reforms to rein in Big Tech's power should be prioritized over regulation focusing on platforms' relationships with their users).