ARTICLE

AUTOMATION IS NOT "HACKING": WHY COURTS MUST REJECT ATTEMPTS TO USE THE CFAA AS AN ANTI-COMPETITIVE SWORD

JAMIE L. WILLIAMS†

INTRODUCTION

Open access to information is a hallmark of today's Internet. It is one of the main reasons the Internet has become, in the words of the U.S. Supreme Court, our "modern public square."[1] And it underlies and is essential for the Internet's promise, as articulated by the late Internet pioneer and Grateful Dead lyricist John Perry Barlow, of "a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth[,]" and that facilitates the "global conveyance of thought."[2]

Open access is more important than ever. The Web is the largest, ever-growing data source on the planet, and it is a critical resource for journalists,

† Staff Attorney, the Electronic Frontier Foundation ("EFF"). I am grateful to Marcia Hoffman for her helpful suggestions and commentary, Cindy Cohn for consistently serving as a thoughtful sounding board and for her inspiring dedication to protecting ordinary Internet users, and Andrew Fogg, founder of Import.io, for graciously walking me through countless ways organizations use automated Web browsing to collect data to meet business or research needs and providing insightful feedback on earlier drafts. I would also like to thank Korey Cowan, Brandan Ray, and the other journal editors for all of their hard work and helpful comments, and for organizing a fantastic symposium on an important, and ambitious, topic: private regulation of the public Internet; Boston University School of Law Professor Andrew Sellars and University of Pittsburgh School of Law Professor David Thaw for being excellent co-panelists; and Boston University School of Law Professors Wendy Gordo and Paul Gugliuzza for their help moderating and coordinating a successful panel. Finally, I would like to thank Hanni Fakhoury for leading me to this issue back when I first joined EFF and Matt Ghering for patiently putting up with me working on this Article in the midst of moving.

[1] Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017) (striking down a North Carolina law making it a felony for a registered sex offender to access social media websites like Facebook and Twitter on First Amendment grounds, because, *inter alia*, "[s]ocial media allows users to gain access to information").

[2] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence (originally published via email from Davos, Switzerland) [https://perma.cc/38MV-DQ2J].

academics, businesses, and everyday people alike. Open access is at risk, however, as a result of recent efforts by companies to use the Computer Fraud and Abuse Act ("CFAA")[3]—an imprecise and outdated anti-"hacking"[4] statute that makes it a crime to access another person's computer "without authorization" [5]—to block competitors from using automated scripts to access publicly available information on their websites.

The problem? Merely accessing *publicly available* information on the Web cannot give rise to criminal liability under the CFAA. Congress intended the statute's unauthorized access provisions[6] to criminalize malicious break-ins of private computer systems,[7] and you cannot break into the open Web. Interpreting the CFAA's unauthorized access provisions to apply to publicly available information—*i.e.*, to not require a computer break-in—would push the statute beyond the brink of absurdity and harm the Web. Companies seeking the power to police use of publicly available information want to "participate in the open Web" but at the same time abuse the CFAA to avoid accepting the

[3] 18 U.S.C. § 1030 (2012).

[4] The term "hacking" has been, and continues to be, used incorrectly by legislators, courts, and others to refer to nefarious computer break-ins by "bad" actors. But not all hacking is "bad." While there are "black hat" hackers who "intentionally break[] into systems or networks to illegally procure information or infuse chaos into a network[,]" there are also good, "white hat" hackers who break into systems to identify security flaws, and who intend to do a public service—not to wreak havoc or steal information from private computer systems. *See* Jerri Collins, *Good Hackers, Bad Hackers - What's the Difference?*, LIFEWIRE, https://www.lifewire.com/hackers-good-or-bad-3481592 [https://perma.cc/ZB6W-C8UW] (last updated June 15, 2017). The non-nefarious nature of the word "hack" is reflected by its use in popular culture. "Life hack," for example, a term coined by EFF's International Director Danny O'Brien in 2004 and added to the Oxford Dictionaries Online in 2011, refers to "[a] strategy or technique adopted in order to manage one's time and daily activities in a more efficient way." *Lifehack*, OXFORD U. PRESS, https://en.oxforddictionaries.com/definition/lifehack [https://perma.cc/7PFL-XUCG] (last visited Apr. 2, 2018). Meanwhile, IKEAhackers.net, a website "all about modding, repurposing and customizing IKEA products," boasts of 5,000 "hacks from all over the globe." IKEA HACKERS, https://www.ikeahackers.net/ [https://perma.cc/5PZC-BZ3R] (last visited Mar. 17, 2018). This Article, when referring to the CFAA's intended purpose, uses the word "hacking" only within quotations, and otherwise refers to the actual conduct courts and legislatures are talking about when they talk about "hacking": nefarious computer break-ins.

[5] *See* 18 U.S.C. § 1030(a)(2)(C) (2012).

[6] This Article refers to the CFAA's "access[ing] without authorization" and "exceed[ing] authorized access" provisions collectively as the statute's "unauthorized access provisions." This does not include the portions of the statute that do not require an unauthorized access, such as 18 U.S.C. § 1030(a)(5)(A)'s prohibition on "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer[,]" along with 18 U.S.C. § 1030(a)(6)'s prohibition on password trafficking.

[7] *See infra* Section III.A.

Web's "open trespass norms."[8] This Article argues that to protect and preserve open access to information online, and to remain consistent with the statute's purpose, courts must not allow it.

The use of automated scripts to access publicly available information on the Web does not change the analysis. Indeed, meaningful access sometimes requires the assistance of technology to automate and expedite an otherwise tedious process of accessing, collecting, and analyzing publicly available information. The process of using a computer to automatically load and read the pages of a website for later analysis is often referred to as "Web scraping."[9] As a technical matter, Web scraping is simply machine automated Web browsing. There is nothing that can be done with a Web scraper that cannot be done by a human with a Web browser. As one district court judge recently recognized, Web scraping "is merely a technological advance that makes information collection easier; it is not meaningfully different from using a tape recorder instead of taking written notes, or using the panorama function on a smartphone instead of taking a series of photos from different positions."[10] Web scraping is a widely used method of interacting with content on

[8] Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1163 (2016).

[9] The term "scraping" comes from a time before APIs, when the only way to build interoperability between computer systems was to "read" the information directly from the screen. Engineers used various terms to describe this technique, including "shredding," "scraping," and "reading." Because the technique was largely only discussed in engineering circles, the choice of terminology was never widely debated. As a result, today, many people still use the term "scraping," instead of something more technically descriptive—like "screen reading" or "Web reading." *See Jamie Williams, 'Scraping' Is Just Automated Access, and Everyone Does It,* ELEC. FRONTIER FOUND. https://www.eff.org/deeplinks/2018/04/scraping-just-automated-access-and-everyone-does-it [https://perma.cc/HA9R-CDFP] (last visited June 20, 2018).

[10] Sandvig v. Sessions, No. CV 16-1368 (JDB), 2018 WL 1568881, at *7 (D.D.C. Mar. 30, 2018).

the Web.[11] Everyone does it—including the companies trying to convince courts to punish others for the same behavior.[12]

CFAA cases involving allegations of 'illegal' automated Web scraping by competitors are nothing new.[13] What is new, however, is a renewed effort, fueled by two poorly reasoned Ninth Circuit password sharing decisions from 2016, to pursue CFAA liability for automated access even in the Ninth Circuit, which has declared that the CFAA's "purpose is to punish hacking"—not to create "a sweeping Internet-policing mandate" by punishing those who violate corporate computer use policies.[14] The companies behind the recent cases[15] are seeking to do just that—*i.e.*, transform the CFAA into a massive computer misappropriation statute—so that they can conduct anti-competitive behavior

[11] Gartner VP Doug Laney advises, "Your company's biggest database isn't your . . . internal database. Rather it's the Web itself." Doug Laney, "Gartner Predicts Three Big Data Trends for Business Intelligence" (Feb. 12, 2015), https://www.forbes.com/sites/gartnergroup/2015/02/12/gartner-predicts-three-big-data-trends-for-business-intelligence/. And indeed, companies across various industries use automated Web browsing products to gather data for a wide variety of uses, including: tracking the performance ranking of products in the search results of retailer websites; monitoring a competitors' pricing and inventory, or information posted publicly on social media to keep tabs on issues that require customer support; staying up to date on news stories relevant to their industry across multiple sources; aggregating information to help manage supply chains; detecting fraud; aggregating market data to help plan for the future; and collecting images and data for machine learning model training. *See, e.g.*, Import.io, Solutions Overview, https://www.import.io/solutions.

[12] Microsoft-owned LinkedIn, for example, one company seeking to use the CFAA to block automated Web scraping by a competing service, acknowledges in its privacy policy that it uses automated tools, *i.e.*, Web scraping, to "collect public information about you, such as professional-related news and accomplishments" and makes that information available on its own website—unless a user opts out via adjusting their default privacy settings. *See* LinkedIn, Privacy Policy, §§ 1.1-1.2 (May 30, 2018), https://www.linkedin.com/legal/privacy-policy [https://perma.cc/P9UU-7R4D].

[13] *See, e.g.*, Craigslist Inc. v. 3Taps Inc. (*Craigslist II*), 964 F. Supp. 2d 1178, 1180–81, 1184 (N.D. Cal. 2013) (finding that the defendant acted "without authorization" under the CFAA when it accessed the plaintiff's public website after the plaintiff sent cease-and-desist letters and blocked the defendant's IP addresses); Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 932–33 (E.D. Va. 2010) (finding that scraping publicly available information from a public website is not a crime under the CFAA, which prohibits "hacking or other unauthorized access to files"); Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439–40 (N.D. Tex. 2004) (finding that a plaintiff plausibly alleged a CFAA claim when Southwest "directly informed" the defendant that its scraping activity violated the Use Agreement on Southwest's website, which was "accessible from all pages on the website," as well as via "direct repeated warnings and requests to stop scraping"); *see also* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372 (2018) for a further discussion of CFAA case law as it relates to Web scraping.

[14] United States v. Nosal (*Nosal I*), 676 F.3d 854, 858, 863–64 (9th Cir. 2012) (en banc).

[15] *See infra*, notes 54, 108.

under the color of the law. Specifically, they want to use the CFAA to restrict their competitors' access to information they've published publicly online for the rest of the world to see.[16]

The stakes of these disputes go far beyond skirmishes between competing commercial services. While they are civil cases, brought pursuant to the CFAA's private enforcement provision,[17] the CFAA is first and foremost a criminal statute—and one with serious penalties.[18] Judicial decisions in civil cases brought under the CFAA's private enforcement provision have the same precedential value as decisions reached in criminal cases.[19] While a company may not want its competitors to use automated Web browsing tools to access publicly available information on its website, that does not mean use of those tools should be a *crime*.

What's more, the question of who can grant or revoke permission to access a website is one of increasing importance. Today, nearly all Internet services are built on top of someone else's computer system. Platforms like Amazon

[16] LinkedIn characterizes its reliance on the CFAA as about protecting user privacy, not about stifling competition. *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1106 (N.D. Cal. 2017). But the company's proposed rule—imposing criminal CFAA liability for automated access of publicly available user data by competitors that LinkedIn has told to "go away," *see infra* note 108 and accompanying text—will not truly protect the privacy interests of LinkedIn users who decide to publish their information publicly online. The data will still be freely available on the Web for anyone else to access and use, without consequence. LinkedIn's privacy policy acknowledges the inherent lack of privacy in data users post publicly on its site and makes no promises to users about LinkedIn's ability to protect it: "Please do not post or add personal data to your profile that you would not want to be publicly available." *See* LinkedIn, Privacy Policy, § 1.1 (May 30, 2018), https://www.linkedin.com/legal/privacy-policy [https://perma.cc/P9UU-7R4D]. What is needed to protect privacy is comprehensive, well thought out privacy regulation—which LinkedIn, its parent company Microsoft, and all other websites and Internet service providers would be subject to.

[17] The CFAA's criminal prohibitions are privately enforceable through a civil suit for damages or injunctive relief. *See* 18 U.S.C. § 1030(g) (2012). The statute provides a civil action only in specified circumstances, requiring a "loss to 1 or more persons during any 1–year period . . . aggregating at least $5,000 in value[,]" except in circumstances involving the impairment or modification of medical treatment, physical injury, or a threat to public safety. *See id.* § 1030(c)(4)(A)(i).

[18] CFAA Penalty Chart, ELEC. FRONTIER FOUND., https://www.eff.org/document/eff-cfaa-penalty-chart [https://perma.cc/P8VU-E2T6] (last visited May 30, 2018).

[19] *See* Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004) (court "must interpret [a] statute consistently, whether [it] encounter[s] its application in a criminal or noncriminal context"); *see also* United States v. Santos, 553 U.S. 507, 522–23 (2008) ("[T]he meaning of words in a statute cannot change with the statute's application.") (citing Clark v. Martinez, 543 U.S. 371, 378 (2005)); United States v. Thompson/Ctr. Arms Co., 504 U.S. 505, 517 (1992) (resolving an ambiguity in a tax statute in favor of the taxpayer in a civil case because the statute had criminal applications that triggered the rule of lenity).

Web Services, which controls 34 percent of the cloud infrastructure market,[20] provide cloud computing services to individuals, organizations, and governments alike.[21] Accessing the Web almost always entails accessing a computer owned by someone else. Allowing computer owners to use the CFAA to police who may access information publicly available on their websites, and the manner in which they can access it, would therefore threaten open access to information across the Web. This would not only impede investigative journalism and research, but in a world of algorithms and artificial intelligence, lack of access to data is a barrier to product innovation, and blocking access to data also means blocking any chance for meaningful competition.

As University of Pittsburgh Professor Michael J. Madison wrote, resolving the debate about the CFAA's scope "is linked closely to what sort of Internet society has and what sort of Internet society will get in the future."[22] The Web of today is open. To preserve this openness, the power to limit access to and use of publicly available information on the Web under color of the law must be dictated by carefully considered rules that balance the various competing policy interests. These rules must not allow the handful of companies that collect massive amounts of user data to reap the benefits of making that information publicly available online—*i.e.*, more Web traffic and thus more users, more data, more business, and more eyes for advertisers[23]—while at the same time limiting use of that public information by anyone they do not like via the force of criminal law. But that is precisely where allowing websites to use the

---

[20] Christine Hall, *Microsoft's Cloud Market Share Grew More than Anyone Else's Last Quarter – Analysts*, DATA CTR. KNOWLEDGE: BUSINESS (Aug. 1, 2017), http://www.datacenterknowledge.com/business/microsofts-cloud-market-share-grew-more-anyone-elses-last-quarter-analysts [https://perma.cc/8G69-CDQX].

[21] *See, e.g.*, Sujatha Perepa, *Why the U.S. Government is Moving to Cloud Computing*, WIRED, https://www.wired.com/insights/2013/09/why-the-u-s-government-is-moving-to-cloud-computing/ [https://perma.cc/MJG8-EAHP] (last visited May 30, 2018).

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

[23] LinkedIn has argued in the pending case against hiQ Labs that Web scraping is what dooms access to public information, because websites will just place their public data behind an authentication gate in order to keep it from competitors. *See* Nicholas Iovino, *LinkedIn Takes Data Scraping Fight to Ninth Circuit*, COURTHOUSE NEWS (Mar. 15, 2018), https://www.courthousenews.com/linkedin-takes-data-scraping-fight-to-ninth-circuit/ [https://perma.cc/3JA2-2HL5] (citing "LinkedIn's argument that [the district court's ruling in hiQ's favor] would disrupt the free flow of information on the internet."). But the default settings on these websites are public for a reason. On LinkedIn, a public profile means that a Web search for a person continues to return their LinkedIn profile among the top results. This helps ensures the people continue to care about maintaining their personal LinkedIn profiles. Users' continued maintenance of their profiles in turn ensures that recruiters will continue to pay for access to LinkedIn recruiter products (*e.g.*, specialized search and messaging), and that companies will continue to pay to post job advertisements on the platform.

CFAA to enforce their contractual computer use restrictions or computer use preferences will lead.

This Article has four Parts. First, it provides background on how courts have interpreted the CFAA's unauthorized access provisions and lays the groundwork for how we got here. Second, it explains how the Ninth Circuit's decisions in *Facebook v. Power Ventures*[24] and *United States v. Nosal* (*"Nosal II"*)[25] blurred clear Ninth Circuit precedent and left room for abuse. Third, it explains why expanding those decisions to cases involving access of publicly available information would be inappropriate as a matter of statutory interpretation and contrary to the Web's open access norms. Fourth, and finally, it argues that allowing companies to use the CFAA to police access to and use of publicly available information would harm open access to information, create an unfair playing field for small companies, and chill the use and creation of Web tools that we all rely on every day.

I. BACKGROUND: SHIFTING TIDES OF 'UNAUTHORIZED ACCESS'

The CFAA makes it a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer"[26]—which includes any computer connected to the Internet.[27] The statute defines "exceeds authorized access,"[28] but

[24] 844 F.3d 1058 (9th Cir. 2016).

[25] 844 F.3d 1024 (9th Cir. 2016).

[26] *See* 18 U.S.C. § 1030(a)(2)(C) (2012). While the same language appears in other subsections of statute with additional elements—such as in § 1030(a)(4), which requires the additional element of an intent to defraud—the interpretation of "accesses a computer without authorization" and "exceeds authorized access" must apply equally to the statute's various subsections, including its broadest section, § 1030(a)(2)(C). *See* Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007) (it is a "standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be given the same meaning").

[27] The first incarnation of the computer crime statute—enacted in 1984—was a narrow statute intended to criminalize unauthorized access to computers to obtain national security secrets or personal financial and consumer credit information, or to "hack" into government computers. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837, 2190-91 (codified as amended at § 1030(a)(1)–(2)). After multiple revisions, the definition of "protected computer" now includes not merely computers "used in interstate or foreign commerce or communication," but computers "used in or *affecting* interstate or foreign commerce or communication." *See* § 1030(e)(2)(B) (emphasis added). The practical effect of this seemingly small change allows the CFAA to reach computers as far as the Commerce Clause can extend. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1570–71 (2010) (arguing that the statute "does not merely cover computers connected to the Internet that are actually 'used' in interstate commerce. Instead, it applies to all computers, period, so long as the federal government has the power to regulate them").

it does not define its most critical terms: unauthorized access and authorized access. In a world where it is difficult to go a single day, or even sometimes a single waking hour, without "accessing" someone else's computer system, the precise meaning of "without authorization . . . has proven to be elusive."[29] In the first two decades following the statute's enactment, "a nearly unbroken string of appellate decisions" adopted increasingly expansive readings of the CFAA's scope.[30] Courts found defendants guilty of computer crimes for a wide range of undesirable conduct that happened to involve a computer, even if it did not rise to the level of a computer break-in, including "objective misconduct, deviating from agency duties, and breach of contract."[31] The CFAA became "the primary tool used by prosecutors to combat . . . assaults on our privacy and our economic well-being."[32] The Department of Justice even infamously tried to convict Lori Drew under the CFAA for violating MySpace's terms of service, which prohibited lying about account information, including age.[33] Drew had posed as a sixteen–year–old boy and used the fake account to bully her daughter's classmate.[34] In another case, in response to a wrongful termination lawsuit, a company retaliated with a counterclaim alleging that the plaintiff had violated the CFAA by making personal use of the Internet at work, in violation of company policy.[35]

Courts eventually began to question the constitutionality of such a "broad" interpretation of the statute's language,[36] and the tide began to shift toward a

---

[28] To exceed authorized access is "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [sic] is not entitled so to obtain or alter . . . ." § 1030(e)(6).

[29] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001).

[30] 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, 1645 (2016).

[31] *Id*. at 1645; *see, e.g*., United States v. Phillips, 477 F.3d 215, 219–21 (5th Cir. 2007); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997); United States v. Morris, 928 F.2d 504, 506, 510 (2d Cir. 1991).

[32] *See* Sheldon Whitehouse, *Hacking into the Computer Fraud and Abuse Act: The CFAA at 30*, 84 GEO. WASH. L. REV. 1437, 1438 (2016).

[33] *See* United States v. Drew, 259 F.R.D. 449, 451, 466–68 (C.D. Cal. 2009).

[34] *Id*. at 452.

[35] Lee v. PMSI, Inc., No. 8:10–CV–2904–T–23TBM, 2011 WL 1742028, at *2 (M.D. Fla. May 6, 2011) (dismissing the company's claims under 18 U.S.C. § 1030(a)(2)(C): "Because PMSI fails to allege that Lee's authorization to use her work computer was terminated prior to her leaving the company, PMSI cannot show that Lee's use of the computer was 'without authorization.'").

[36] *See, e.g*., *Drew*, 259 F.R.D. at 467 (noting the constitutional concerns that would arise "if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization . . . .").

more "narrow" application of criminal and civil CFAA liability.[37] In 2009, the Ninth Circuit issued its decision in *LVRC Holdings LLC v. Brekka*,[38] which rejected the theory that "a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer," such as violating an employer's computer use policies.[39] Instead, the court held, the CFAA's prohibition against accessing a protected computer "without authorization" covers individuals who have no rights to the computer system, while the prohibition against "exceed[ing] authorized access" is aimed at insiders who "ha[ve] permission to access the computer, but access[] information on the computer that the[y] [are] not entitled to access."[40]

This tide gained momentum in 2012, when the narrow interpretation, after "percolat[ing] among lower courts," eventually "won widespread adoption"[41] with the Ninth Circuit's *en banc* decision in *United States v. Nosal* ("*Nosal I*").[42] The case involved disloyal employees of an executive recruiting firm who had used their login credentials to access the company's database for non-business purposes—*i.e.*, to obtain proprietary information to share with an ex-employee, David Nosal, who was starting a competing firm.[43] The court held that the CFAA's "purpose is to punish hacking—the circumvention of technological access barriers"—not to create "a sweeping Internet-policing mandate" by punishing those who violate corporate computer use policies.[44] According to the court, "transform[ing] the CFAA from an anti-hacking statute into an

[37] *See, e.g.*, Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006) ("The gist of [the plaintiff's] complaint is aimed not so much at [the defendants'] improper access of . . . information, but rather at [the defendants'] actions subsequent to their accessing the information."); *see also* Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005) ("[T]he CFAA . . . do[es] not prohibit the unauthorized disclosure or use of information, but rather unauthorized access."); Mayer, *supra* note 30, at 1657 ("[The narrow interpretation] traces its intellectual roots to *International Association of Machinists & Aerospace Workers v. Werner-Masuda* and *Lockheed Martin v. Speed*, a pair of mid-2000s district court opinions that sought to limit liability under the CFAA's exceeding authorization theory.") (citations omitted).

[38] 581 F.3d 1127 (9th Cir. 2009).

[39] *Id.* at 1135 (citing Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006)) (declining to adopt the interpretation of 'without authorization' suggested by *Citrin* that an employee's authorization to access a computer ended when the employee violated his duty of loyalty to his employer).

[40] *Id.* at 1133.

[41] *See* Mayer, *supra* note 30.

[42] United States v. Nosal (*Nosal I*), 676 F.3d 854, 858, 863 (9th Cir. 2012) (en banc).

[43] *Id.* at 856.

[44] *Id.* at 858, 863 ("[The] narrower interpretation is . . . a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere.").

expansive misappropriation statute" for enforcing computer use policies would "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime."[45]

The Ninth Circuit ruled that, consistent with both the statute's purpose and the constitutional rule of lenity,[46] "'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*."[47] The Second and Fourth Circuit soon followed suit,[48] along with a wave of district courts across the country,[49] creating a circuit split

[45] *See id*. at 857, 859 ("If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.").

[46] *See id*. at 863 ("The rule of lenity not only ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize. We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals."); *see also* United States v. Lanier, 520 U.S. 259, 266 (1997) ("[The] rule of lenity[] ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered."); United States v. Bass, 404 U.S. 336, 348 (1971) ("[B]ecause of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity."); United States v. Wiltberger, 18 U.S. 76, 95 (1820) ("[P]enal laws are to be construed strictly . . . .").

[47] *Nosal I*, 676 F.3d at 863–64 (emphasis in original).

[48] *See* United States v. Valle, 807 F.3d 508, 526–27 (2d Cir. 2015) (finding that *Nosal I*'s narrow interpretation of the CFAA is "consistent with the statute's principal purpose of addressing the problem of hacking, *i.e*., trespass into computer systems or data" and that "courts that have adopted the broader construction 'looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens'"); United States v. Steele, No. 13-4567, 595 F. App'x 208, 211 (4th Cir. Dec. 24, 2014) ("The narrower construction, adopted by *WEC Carolina*, holds that § 1030(a)(2) applies to employees who unlawfully *access* a protected computer, but not to the improper *use* of information lawfully accessed.") (emphasis in original); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012) ("[W]e are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy.").

[49] *See, e.g*., Lane v. Brocq, No. 15 C 6177, 2016 WL 1271051, at *10 (N.D. Ill. Mar. 28, 2016); Experian Mktg. Sols., Inc. v. Lehman, No. 1:15-CV-476, 2015 WL 5714541, at *5 (W.D. Mich. Sept. 29, 2015); Giles Constr., LLC v. Tooele Inventory Sol., Inc., No. 2:12-cv-37, 2015 WL 3755863, at *3 (D. Utah June 16, 2015); Enhanced Recovery Co. v. Frady, No. 3:13-CV-1262-J-34JBT, 2015 WL 1470852, at *6–7 (M.D. Fla. Mar. 31, 2015); Cranel Inc. v. Pro Image Consultants Grp., LLC, 57 F. Supp. 3d 838, 845-46 (S.D. Ohio 2014); Advanced Fluid Sys., Inc. v. Huber, 28 F. Supp. 3d 306, 329 (M.D. Pa. 2014); Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 619 (E.D. Pa. 2013); Power Equip. Maint., Inc. v. AIRCO Power Servs., Inc., 953 F. Supp. 2d 1290, 1295 (S.D. Ga. 2013).

over whether a violation of a written restriction on computer use constituted criminal unauthorized access under the CFAA.[50]

But even with the shifting tide, and despite criticism of the CFAA as the "worst law in technology,"[51] some judges are having a hard time breaking free from the mindset pressed by prosecutors and civil plaintiffs, that the CFAA should be used as a catchall for any behavior involving a computer that we don't like.[52] In 2016, the Ninth Circuit issued a pair of confusing decisions that contorted *Nosal I's* clear holding to ensure that the defendants did not evade CFAA liability—even though pre-existing statutes or causes of action would have more appropriately targeted the alleged misconduct in both cases.[53] Companies seeking to enforce bans on using automated Web browsing tools to access publicly available information are now seeking to use the two cases—*Facebook v. Power Ventures* and *Nosal II*—to pursue an expansive reading of the CFAA, circumvent *Nosal I,* and win the power to police who can access publicly available information on the open Web, and how.[54]

[50] *See Steele*, 595 F. App'x at 211 ("[T]his split focuses on employees who are authorized to access their employer's computers but use the information they retrieve for an improper purpose.").

[51] 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/U2Z2-76YD].

[52] *See* Whitehouse, *supra* note 32.

[53] *See infra* Section II.

[54] *See, e.g.*, hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1108 (N.D. Cal. 2017); Ryanair DAC v. Expedia Inc., 2:17-CV-01789-RSL (W.D. Wash. filed Nov. 29, 2017) (alleging a CFAA violation for accessing Ryanair's website using automated tools, in violation of Ryanair's terms of service and following receipt of cease and desist letters); Original Complaint at 12–14, Southwest Airlines Co. v. Roundpipe, LLC, No. 3-18-CV-00033-G (N.D. Tex. filed Jan. 5, 2018) (alleging a CFAA violation for accessing fare data on Southwest's website using automated tools, in violation of Southwest's terms of service and following receipt of cease and desist letters); *see also Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, No. 2:17-CV-07232-ODW-JC, 2018 WL 2448115, at *6 (C.D. Cal. May 29, 2018) (alleging a CFAA violation where defendants disregarded an individualized letter "reminding Defendants that 'use of the [Ticketmaster] website is conditioned on an agreement that the user will not . . . use any automated . . . computer system to . . . buy . . . tickets,' and instructing Defendants to 'cease and desist from any further violations of Ticketmaster's rights.'"); Ticketmaster L.L.C. v. Prestige Entm't, No. 2:17-CV-07232-ODW (JCx), 2018 WL 654410, at *6 (C.D. Cal. Jan. 31, 2018) ("Ticketmaster contends that Defendants lacked or exceeded their authorization by violating its [Terms of Use], even after it sent Defendants a cease-and-desist letter outlining the alleged violations[,]" via its continued using automated software to circumvent CAPTCHAs).

II. BLURRED LINES: THE NINTH CIRCUIT'S 2016 PASSWORD SHARING DECISIONS

The Ninth Circuit's *en banc* holding in *Nosal I* was clear: For "a statute whose general purpose is to punish hacking," liability must turn on the "circumvention of technological access barriers"[55]—*i.e.*, code-based restrictions that place limitations on who can and cannot access a system or data. Violations of written computer restrictions, which impose limitations on computer use, do not suffice for CFAA liability.[56] For *Nosal I* to have any meaning, this must be true regardless of whether a written restriction is phrased (properly) in terms of "use" or (improperly) in terms of "access."[57] The two terms are often used interchangeably, because while there is a difference between an "access restriction" (which limits who may enter in the first place) and a "use restriction" (which limits how a commuter may be used), there is no practical difference between generally using a computer and accessing a computer: "[u]se of a computer constitutes an access" and access constitutes a use.[58] But "if you believe that the difference between a *use restriction* and an *access restriction* is just how it is written, then [*Nosal I*] hinges liability on exactly the basis for which it purports to reject hinging liability — the mere words of the written restrictions."[59]

The Ninth Circuit's subsequent decisions in *Facebook v. Power Ventures* and *Nosal II* both purport to be consistent with *Nosal I*, but both panels found

---

[55] *Nosal I*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

[56] The Ninth Circuit "meant 'use restrictions' to refer to any written restrictions, as they technically allowed access but imposed terms of use." Orin Kerr, *The CFAA Meets the "Cannibal Cop" in the Second Circuit—and Maybe Beyond*, WASH. POST: THE VOLOKH CONSPIRACY (May 13, 2015), https://www.washington post.com/news/volokh-conspiracy/wp/2015/05/13/the-cfaa-meets-the-cannibal-cop-in-the-second- circuit-and-maybe-beyond/ [https://perma.cc/BJ99-N75C] (emphasis omitted) [hereinafter Kerr, *CFAA Meets the "Cannibal Cop"*].

[57] Any use restriction can be written in terms of access. *See, e.g.*, United States v. Valle, 807 F.3d 508, 513, 524 (2d Cir. 2015) (a written restriction providing that "databases could only be accessed in the course of an officer's official duties" constituted a computer use restriction, not an access restriction). But "simply denominating limitations as 'access restrictions' does not convert what is otherwise a use policy into an access restriction." Wentworth-Douglass Hosp. v. Young & Novis Prof'l Ass'n, No. 10–CV–120–SM, 2012 WL 2522963, at *4 (D.N.H. June 29, 2012) ("[T]he [plaintiff's] policy prohibiting employees from accessing company data for the purpose of copying it to an external storage device is not an 'access' restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access."); *see also* Craigslist Inc. v. 3Taps Inc. (*Craigslist I*), 942 F. Supp. 2d 962, 969 (N.D. Cal. 2013) (Website's terms of use—which provided rules about how site visitors could use data and prohibited the use of data in ways that violated the site's terms of use—were use restrictions regardless of the fact that they were "framed in terms of 'access").

[58] *See* Kerr, *CFAA Meets the "Cannibal Cop," supra* note 56.

[59] *Id.* (emphasis added).

liability despite no evidence of circumvention of a technological access barrier. In both cases, the defendants accessed data stored behind a code-based authentication barrier via valid, shared login credentials, with the knowledge and consent of the credential holder—not via a computer break-in.[60] Yet, because both cases involved conduct the respective panels did not like,[61] they contorted *Nosal I's* clear holding to ensure that the defendants did not escape CFAA liability—even though David Nosal was also convicted of trade secret theft and even though Facebook could have sued Power Ventures for intentional interference with business relations.

The Ninth Circuit's 2016 decisions blurred previously clear precedent and opened the door for further abuse of an already overused law. To avoid wreaking further havoc on CFAA jurisprudence and on the Web, courts must take care to limit these decisions to their "stark" facts[62] and resist any further urges to apply this blunt and outdated criminal anti-"hacking" statute to every complicated, modern-day, and often commercial dispute involving a computer—even where there is no allegation of an actual computer break-in.

A. Facebook v. Power Ventures

i. The Decision

Facebook v. Power Ventures—a civil case—involved a social media aggregator's consensual use of its users' Facebook passwords to access their Facebook accounts.[63] The social media aggregator, Power Ventures ("Power"), offered users a way to view information regarding various social media accounts in one place.[64] Facebook users seeking to more easily manage multiple social media accounts voluntarily shared their Facebook usernames and passwords with Power so that it could access their accounts and provide its services.[65]

---

[60] People have quibbled over whether *Power Ventures* and *Nosal II* are "about password sharing," but there can be no dispute that consensual password sharing played an integral role in both. *See, e.g.*, *Nosal II*, 844 F.3d 1024, 1029 (9th Cir. 2016) ("This appeal is not about password sharing."); *id.* at 1048 ("This case is about password sharing.") (Reinhardt, J., dissenting).

[61] In *Power Ventures*, for example, in ruling that the defendant had acted without authorization, the panel relied on ill-advised emails sent by company officials, including one from Power Ventures' CEO stating, "[W]e need to be prepared for Facebook to try to block us and . . . turn this into a national battle that gets us huge attention." *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016).

[62] The Ninth Circuit added references to "stark" circumstances in amended decisions issued in both cases, after the court denied the defendants' respective petitions for rehearing and rehearing *en banc*. *See* Power Ventures, 844 F.3d at 1067 n.1; *Nosal II*, 844 F.3d at 1036.

[63] Power Ventures, Inc., 844 F.3d at 1062.

[64] *Id.*

[65] *Id.*

The users had valid Facebook accounts, which allowed them access to Facebook, and they authorized Power to use their valid login credentials to access their accounts on their behalf.[66] Facebook objected to this and sent Power a cease and desist letter citing violations of its terms of use.[67] It also blocked one of Power's IP addresses, which was not effective.[68] Importantly, Facebook never took the one technical measure that would have effectively enforced its terms of use as against Power: it never revoked the login credentials for the accounts of the Facebook users who had voluntarily shared their passwords with Power.[69] Power ignored the cease and desist letter and continued to use the valid, shared user credentials, as authorized by the Facebook users, to provide its services, and Facebook sued.[70]

There was no evidence of any technological computer break-in, but the Ninth Circuit nevertheless found Power liable for violating the CFAA, by continuing to access Facebook (a) after receiving the cease and desist letter *and* (b) despite Facebook's instituting an IP address block.[71] The panel recognized that individual Facebook users (*i.e.*, account holders) can provide third party agents (such as Power) with valid authorization to access their accounts on their behalf: "Power had at least arguable permission to access Facebook's computers" and thus "did not initially access Facebook's computers 'without authorization[.]'"[72] But the panel also held—confusingly—that the valid authorization provided to an agent by an individual account holder could be rescinded or overruled by Facebook, even if the user's authorization to access their account continued.[73] According to the panel, after receipt of the cease and desist letter, Power was no longer accessing Facebook's computers with "authorization" under the CFAA and was thus committing a crime—despite having ongoing authorization from Facebook's users to access their accounts via their still valid login credentials.

---

[66] *Id.* at 1062–63.

[67] *Id.* at 1067 ("Facebook's cease and desist letter informed Power that it had violated Facebook's terms of use and demanded that Power stop soliciting Facebook users' information, using Facebook content, or otherwise interacting with Facebook through automated scripts.").

[68] *Id.*

[69] *Id.* at 1063.

[70] Facebook also alleged that Power Ventures violated the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN–SPAM"). Facebook's CAN-SPAM allegations, which the Ninth Circuit rejected, are beyond the scope of this Article. *See id.* at 1064–65.

[71] *Id.* at 1069.

[72] *Id.* at 1067.

[73] *Id.* at 1068.

ii. The Open Question: How Does Ignoring a Cease and Desist Letter and an IP Address Block Add Up to a Computer Break-In?

The *Power Ventures* panel's conclusion that Power violated the CFAA does not rest on whether the company broke into any computer system by circumventing a code-based access barrier, despite *Nosal I's* clear holding that such circumvention is required. The panel tries to avoid this problem—the apparent lack of any circumvention of a code-based access barrier—by squaring its decision with only one aspect of *Nosal I's* holding: it acknowledged that after *Nosal I*, "a violation of the terms of use of a website—without *more*—cannot establish liability under the CFAA."[74] It failed to acknowledge, however, that the "more" required by *Nosal I* is circumvention of a code-based *access* barrier. In *Power Ventures*, the only "more" at issue adds up to an individualized written notice of a restriction on computer use (phrased in terms of access),[75] plus an IP address block. But an individualized *written* notice of a restriction on computer use does not constitute a code-based access barrier, and neither does an IP address block, as the panel itself recognized: "Simply bypassing [a block placed on] an IP address [sic], without more, would not constitute unauthorized use."[76]

The panel's failure to square its decision with *Nosal I's* requirement of circumvention of a code-based access barrier raises a number of questions. Did the panel consider Facebook's username and password gate to be the code-based access barrier that was circumvented, which would mean that Power Ventures' use of still-valid passwords, with the continuing authorization of Facebook users, constituted criminal circumvention? If so, how should Internet users distinguish this type of unauthorized password sharing "from one in which a bank has clearly told customers that no one but the customer may access the customer's account, but a husband nevertheless shares his password with his wife to allow her to pay a bill"?[77] The panel recognized the tension between *Nosal I* and situations in which "an automatic boilerplate revocation follows a violation of a website's terms of use," but held that it "need not address or resolve such questions on the stark facts before [it]."[78] It failed, however, to tell us which "stark facts" relieved the tension, and why.

---

[74] *Id.* at 1067 (emphasis added).

[75] *Id.* at 1068.

[76] *Id.* at 1068 n.5. The panel reasoned, "[b]ecause a blocked user does not receive notice that he has been blocked, he may never realize that the block was imposed and that authorization was revoked. Or, even if he does discover the block, he could conclude that it was triggered by misconduct by someone else who shares the same IP address, such as the user's roommate or co-worker." *Id.*

[77] *Nosal II*, 844 F.3d 1024, 1055 (9th Cir. 2016) (Reinhardt, J., dissenting).

[78] *Power Ventures*, 844 F.3d at 1067 n.1.

Alternatively, did the panel consider the IP address block, following an individualized written "revocation of permission," to be a code-based access barrier—despite acknowledging that without a cease and desist letter, IP address blocks are not access barriers? If so, did it consider Power's use of a dynamic IP address to be the requisite circumvention? Also, what type of notice is sufficient, under what circumstances, to constitute a clear "revocation of permission" for purposes of the CFAA? *Power Ventures* involved a cease and desist letter that, according to the panel, "unequivocally" revoked authorization.[79] But in a subsequent decision, the Ninth Circuit ruled that an IP address block combined with an individualized cease and desist letter prohibiting the defendant from accessing information via automated scripts—though failing to revoke authorization all together—did *not* constitute revocation of access permission under California's or Nevada's computer crime statutes.[80] The Central District of California later applied this same reasoning to grant a motion to dismiss in another case involving automated software, finding that Ticketmaster failed to show that it had revoked the defendants' permission to access its website.[81] But in the same case, following Ticketmaster's filing of an amended complaint with replead CFAA allegations, the same judge denied the defendants' motion to dismiss on the ground that Ticketmaster's cease and desist letter "was, in effect, an individualized access policy that revoked authorization upon breach of the policy."[82] This suggests that revocation of authorization turns solely on how a cease and desist letter is written. This rule cannot be squared with *Nosal I*'s holding that CFAA liability does not hinge on the mere

[79] *Id*. at 1067.

[80] Oracle USA, Inc. v. Rimini St., Inc., 879 F.3d 948, 961 (9th Cir. 2018) ("As EFF puts it, '[n]either statute . . . applies to bare violations of a website's terms of use—such as when a computer user has permission and authorization to access and use the computer or data at issue, but simply accesses or uses the information in a manner the website owner does not like.'").

[81] *See* Ticketmaster L.L.C. v. Prestige Entm't, No. 2:17-CV-07232-ODW-JC, 2018 WL 654410, at *6 (C.D. Cal. Jan. 31, 2018) (dismissing CFAA allegations where Ticketmaster did not show that its cease-and-desist letter—which outlined the defendants' terms of use violations, including the use of automated software to request more than 1,000 pages in a 24-hour period, make more than 800 ticket reservation requests in a 24-hour period, and circumvent CAPTCHA—rescinded permission from Defendants to use its website.).

[82] *See* Ticketmaster L.L.C. v. Prestige Entm't W., Inc., No. 2:17-CV-07232-ODW-JC, 2018 WL 2448115, at *15 (C.D. Cal. May 29, 2018). Relying on *Power Ventures*—and further contorting *Nosal I*—the court held that Ticketmaster's cease and desist letter "remind[ing]" the defendants of Ticketmaster's terms of service prohibition on using automated systems to purchase tickets "was of far greater practical and legal significance than a generally applicable 'use restriction'" and that violations of the letter's "individualized access policy" constituted access in excess of authorization for purposes of the CFAA. *Id*. at *2, *15. For all practical purposes, this decision is inconsistent with the Ninth Circuit's holding in *Oracle USA, Inc. v. Rimini St*., Inc., 879 F.3d 948 (9th Cir. 2018), and further evidence of how *Power Ventures* has set the stage for artful pleading around the limitations set out in *Nosal I*.

words of the written restrictions.[83] Even the *Power Ventures* opinion itself refers to computer "use" and "access" interchangeably[84]—unintentionally illustrating the inherent problem with hinging liability on how a computer use restriction is drafted.

B. United States v. Nosal

i. The Decision

The Ninth Circuit's other confusing password sharing decision, *Nosal II*, was issued a week before *Power Ventures*, by a separate three-judge panel, on Mr. Nosal's second trip to the Ninth Circuit. On this trip, the court addressed not whether current Korn/Ferry employees violated the CFAA by accessing the company's proprietary database for nonbusiness purposes, but whether ex-employees violated the CFAA by using—with permission—a current employee's legitimate, shared login credentials.[85] The ex-employees' own credentials had been revoked when they left the company.[86]

Similar to *Power Ventures*, there was no evidence of any technological computer break-in, but the Ninth Circuit nevertheless found, 2-to-1, that the ex-employees' access violated the CFAA.[87] Korn/Ferry's corporate policies prohibited password sharing and required that anyone who accessed any Korn/Ferry system or information have "specific authority."[88] Consistent with this policy, the Ninth Circuit panel held that only Korn/Ferry (the computer owner)—and not an employee with company-authorized login credentials (a mere account holder)—could provide the ex-employees with "authorization" to access its computers.[89] According to the court, the authorization granted by the current employee simply did not count for purposes of the CFAA: "Nosal

[83] *See* note 60 and accompanying text.

[84] *See Power Ventures*, 844 F.3d at 1068 n.5 (emphasis added) (stating, in interpreting the CFAA's prohibition on *unauthorized access*, "[s]imply bypassing [a block placed on] an IP address [sic], without more, would not constitute *unauthorized use*.").

[85] *Nosal II*, 844 F.3d at 1028–31. Nosal was also convicted of trade secret theft, for which the distinction between who amongst his associates actually accessed the priority database—a current employee or an ex-employee—made no difference. *Id.* at 1031.

[86] *Id.* at 1029–30. Nosal was charged under the CFAA as an accomplice under 18 U.S.C. § 1030(a)(4) and found liable for the actions of Becky Christian and another former Korn/Ferry employee. *See id.* at 1029 n.1.

[87] *Id.* at 1038.

[88] United States v. Nosal, 930 F. Supp. 2d 1051, 1055 (N.D. Cal. 2013). When an individual logged on to Korn/Ferry's computer system, the following notification was displayed: "This computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and to do so without the relevant authority can lead to disciplinary action or criminal prosecution[.]" *Id.* (internal quotations omitted).

[89] *Nosal II*, 844 F.3d at 1035–36.

had 'no possible source of authorization' since the company revoked his authorization and, while [Korn/Ferry's current employee] might have been wrangled into giving out her password, she and the others knew that she had no authority to control system access."[90] Because Nosal and his associates did not have permission directly from Korn/Ferry, their access to the Korn/Ferry database was without "authorization" under the CFAA and thus criminal. The court compared their access to that of a "thief" who had "stolen an employee's password and then used it to rifle through" the database.[91] The thief's access, "without doubt . . . would have been without authorization" and, according to the panel majority, "the same principle holds true here."[92]

The majority stated that "[i]mplicit in the definition of authorization is the notion that" a single entity, the computer owner, "can grant or revoke that permission."[93] But nothing in the definition of "authorization" leads—even implicitly—to the conclusion that only the computer owner, and not a credentialed user, can grant or revoke someone's permission to access the credentialed user's account. Neither the statute, nor any dictionary definition of "authorization," specifies or limits who exactly has the authority to provide the requisite authorization for accessing a computer or website.[94] As Judge Reinhardt recognized in his dissenting opinion, "[w]hile the majority reads the statute to criminalize access by those without 'permission conferred by' the system owner, it is also proper (and in fact preferable) to read the text to criminalize access only by those without 'permission conferred by' *either* a legitimate account holder *or* the system owner."[95] Judge Reinhardt's definition is more consistent with pervasive societal practices and expectations; despite being contrary to good security hygiene, password sharing is a routine online practice.[96]

---

[90] *Id*. at 1035 n.7.

[91] *Id*. at 1039.

[92] *Id*.

[93] *Id*. at 1035.

[94] *See* United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) ("[A]uthorization" is a word "of common usage, without any technical or ambiguous meaning.") (internal quotation omitted).

[95] *Nosal II*, 844 F.3d at 1052 (Reinhardt, J., dissenting) (emphasis added).

[96] Matthew Humphries, *Up to 60 Percent of Streaming Account Passwords Are Shared*, PC MAG. (May 26, 2017), https://www.pcmag.com/news/353917/up-to-60-percent-of-streaming-account-passwords-are-being-sh; Will Yakowicz, *Study Finds 95 Percent of People Share Up To 6 Passwords*, INC. (Feb. 18, 2016), https://www.inc.com/will-yakowicz/infographic-95-percent-share-6-passwords-with-friends.html [https://perma.cc/5D2M-TCYB] (reporting on a study by password manager Lastpass finding that "58 percent of [respondents] share their WiFi password, 48 percent share their TV or movie streaming service account, 43 percent share financial passwords, 39 percent share email, 28 percent share social media accounts, and 25 percent share work-related passwords with others" and that "61 percent of people are more likely to share work passwords than personal ones"); *see also* Amber Gott, *Infographic: Keep Your Friends Close & Your Pass-*

The premise that only a computer owner, and not a credentialed user, can grant or revoke someone's permission to access a computer is found only—and only implicitly—in Korn/Ferry's ban on sharing passwords. The majority imported this corporate policy into its own definition of authorization, which Judge Reinhardt aptly described as "somewhat circular."[97] Despite claiming not to, the majority's construction "base[s] criminal liability on system owners' access policies" and "loses sight of the [CFAA's] anti-hacking purpose."[98] As a result, under the Ninth Circuit's two *Nosal* decisions, when an employee uses her own password to access a corporate database for nonbusiness purposes, she may be liable for misappropriating a trade secret, but she is not liable under the CFAA. Yet, if she provides her password to an outsider for the very same nonbusiness purposes, then she may be guilty as an accomplice both for unauthorized access under the CFAA and misappropriation of trade secrets.

ii. The Open Question: What Does This Mean For Other Forms of Consensual Password Sharing?

As Judge Reinhardt noted in his dissent, there is no "workable line" separating "the consensual password sharing in [*Nosal II*] from the consensual password sharing of millions of legitimate account holders, which may also be contrary to the policies of system owners."[99] As a technical matter, granting another person access to your online account will *almost always* mean granting them access to data stored on *someone else's* computer. Accessing a Gmail account requires accessing Google's servers, checking for Facebook messages requires accessing Facebook's servers, and logging into a bank account to pay a bill requires accessing the bank's servers. And not only is password sharing routinely done without the express permission of the computer owner—*i.e.*, Google, Facebook, the bank—but service providers commonly restrict password sharing in their terms of use. The *Nosal II* majority notes that Nosal "received particularized notice of his revoked access following a prolonged negotiation" and then "surreptitiously accessed data owned by [his] former employer."[100] According to the majority, under these facts, Nosal's access was unambiguously unauthorized, while a "less stark revocation" followed by "more sympathetic access through an authorized third party" might not be.[101]

words Closer, LASTPASS BLOG (Feb. 18, 2016), https://blog.lastpass.com/2016/02/infographic-keep-your-friends-close-your-passwords-closer-2.html [https://perma.cc/A582-BCHK] ("[O]nly 19% of respondents say they don't share passwords that would jeopardize their identity or financial information, leaving 81% of people who would share those passwords."). Password sharing is not a wise security practice, but Internet users do it *all the time*.

[97] *Nosal II*, 844 F.3d at 1052 (Reinhardt, J., dissenting).

[98] *Id.* at 1049, 1054.

[99] *Id.* at 1049.

[100] *Id.* at 1036, 1038 (majority opinion).

[101] *Id.* at 1036.

But it fails to explain what would constitute a "less stark" revocation or a "more sympathetic" access via a third party agent. As Judge Reinhardt recognized,

> [i]t is impossible to discern from the majority opinion what principle distinguishes authorization in Nosal's case from one in which a bank has clearly told customers that no one but the customer may access the customer's account, but a husband nevertheless shares his password with his wife to allow her to pay a bill.[102]

Part of this confusion stems from *Nosal II*'s failure, as in *Power Ventures*, to square its decision with *Nosal I*'s holding that a violation of the CFAA requires circumvention of a technological access barrier. The majority first noted—in what is at most dictum, and with somewhat confused reasoning[103]—that the statutory language does not require circumvention of a code-based access barrier.[104] It then stated that, in any event, Korn/Ferry's password system was "unquestionably" a "technological access barrier" designed "to keep out those 'without authorization,'"[105] and equated Nosal's consensual use of a shared password with nonconsensual use of a trafficked password.[106] The opinion glossed over critical distinctions between password sharing and password theft in order to draw an analogy between this case and one involving a clear "circumvention" of a technological access barrier. These efforts are directly contradictory to the majority's purported efforts to minimize the significance of circumvention. And in failing to explain how using a shared password equates to using a trafficked password for purposes of the CFAA, it failed to clarify not only what exactly constituted "circumvention" in this case, but what its holding means for password sharing going forward.

---

[102] *Id*. at 1055 (Reinhardt, J., dissenting).

[103] The court opined that requiring the circumvention of a technological access barrier "would make little sense because some [18 U.S.C.] § 1030 offenses do not require access to a computer at all." *Id*. at 1039 (noting that 18 U.S.C. § 1030(a)(6) imposes penalties for trafficking in passwords "through which a computer can be accessed without authorization"). The majority's rationale here itself makes little sense, as interpreting unauthorized access to require circumvention of a technological access barrier would only impact the sections of the statute that require unauthorized access. The password trafficking section identified by the majority actually supports the conclusion that unauthorized access requires the circumvention of a technological access barrier, such as a password requirement; it implicitly recognizes that password-protected systems are the type of computer systems that can be "accessed without authorization" in the first place. *See* 18 U.S.C. § 1030(a)(6) (2012).

[104] *Nosal II*, 844 F.3d at 1038–39.

[105] *Id*. at 1039 (majority opinion).

[106] *Id*. at 1039.

III. MERELY ACCESSING PUBLICLY AVAILABLE INFORMATION ON THE INTERNET CANNOT GIVE RISE TO CRIMINAL LIABILITY UNDER THE CFAA

The Ninth Circuit's password sharing decisions were issued in July 2016.[107] Within weeks, citations to the two cases—particularly *Power Ventures*—began appearing in cease and desist letters, purporting to revoke authorization to access publicly available data published on the open Internet. A few of these disputes have made their way to court, where companies seeking to restrict their competitors' access to publicly available data are attempting to capitalize on the confusion created by *Power Ventures* and *Nosal II* and expand the decisions to publicly available information. Pursuant to their theory of liability, after a website owner sends a written cease and desist letter explicitly revoking the recipient's permission to access their website, any continued access constitutes accessing a computer "without authorization."[108]

This theory faces one critical problem: *Power Ventures* and *Nosal II* were decided on their "stark" facts—and these facts involved access to non-public

[107] The amended decisions were issued five months later, in December 2016. Facebook, Inc. v. Power Ventures, 844 F.3d 1058, 1062 (9th Cir. 2016); *Nosal II*, 844 F.3d at 1028.

[108] *See, e.g.*, hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1108 (N.D. Cal. 2017) ("LinkedIn argues that under the plain meaning of 'without authorization,' as well as under relevant Ninth Circuit authority," hiQ has violated the CFAA "by continuing to access public LinkedIn profiles after LinkedIn has explicitly revoked permission to do so" in a written cease and desist letter); Complaint at 6–10, Ryanair DAC v. Expedia Inc., 2:17-CV-01789-RSL (W.D. Wash. filed Nov. 29, 2017) (alleging a CFAA violation for accessing Ryanair's website using automated tools, in violation of Ryanair's terms of service and following receipt of cease and desist letters); Original Complaint at 12–14, Southwest Airlines Co. v. Roundpipe, LLC, No. 3-18-CV-00033-G (N.D. Tex. filed Jan. 5, 2018) (alleging a CFAA violation for accessing fare data on Southwest's website using an automated script, in violation of Southwest's terms of service and following receipt of cease and desist letters); *see also* Ticketmaster L.L.C. v. Prestige Entm't, No. 2:17-CV-07232-ODW (JCx), 2018 WL 654410, at *6 (C.D. Cal. Jan. 31, 2018) ("Ticketmaster contends that Defendants lacked or exceeded their authorization by violating its TOU, even after it sent Defendants a cease-and-desist letter outlining the alleged violations[,]" via its continued use of automated software to circumvent CAPTCHAs). Plaintiffs have also tried to stretch the CFAA to cover "click fraud" in the wake of *Power Ventures*, *see, e.g.*, Satmodo, LLC v. Whenever Commc'ns, LLC, No. 17-CV-0192-AJB NLS, 2017 U.S. Dist. LEXIS 57719, at *2-4 (S.D. Cal. Apr. 14, 2017), despite that "falsely inflating the number of clicks on a pay-per-click ad"—either to drive up a competitor's advertising costs or to generate more revenue for the platform—does not constitute breaking into a computer system. Erin Sagin, *4 Powerful Ways to Eliminate Click Fraud in Your Account*, WORDSTREAM BLOG (Apr. 9, 2018), https://www.wordstream.com/blog/ws/2015/08/17/click-fraud [https://perma.cc/4N4N-HY4D].

information stored behind code-based authentication barriers.[109] The problem is critical because the CFAA's unauthorized access provisions were intended to criminalize breaking into private computer systems, and you cannot "break into" the public Internet. Pursuant to the Web's open access norms, everyone is authorized to access information posted publicly online, and that authorization cannot be revoked without constructing a technological access barrier.[110] Thus, merely accessing publicly available information on the Internet cannot give rise to criminal liability under the CFAA's unauthorized access provisions—at least not without pushing the statute beyond the brink of absurdity. *Nosal I's* requirement of a code-based authentication barrier reflects, and is consistent with, both Congress's intent and the Web's open access norms. Allowing companies to use the CFAA to restrict access to publicly available information would turn *Nosal I* on its head, contravene Congress's intent, and "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute" and anti-competitive sword.[111] To avoid this result, courts should reject attempts to extend *Power Ventures* and *Nosal II* to entirely public information.[112]

A. Congress Enacted the CFAA To Target Serious Computer Break-Ins

In 1984, when Congress's passed the CFAA's precursor,[113] today's interconnected, networked world was beyond its imagination. Today, it is difficult to go a single day without connecting to someone else's computer system. People rarely host their email or websites on their own servers, so even merely checking email from the comfort of one's own home in the vast majority of cases necessitates accessing information someone else's computer. It is now easier than ever to check one's email, and thus access information on a distant server (*i.e.*, a computer), from almost anywhere on the planet—including from

[109] *See* hiQ Labs, 273 F. Supp. 3d at 1109 (N.D. Cal. 2017) (distinguishing *Nosal II* and *Power Ventures* because neither involved access of public information, such as public LinkedIn user profiles). As outlined above, *Nosal II* involved access to a proprietary corporate computer network by an ex-employee whose own credentials to access the non-public information within that propriety network had been expressly revoked upon termination of his employment. *Nosal II*, 844 F.3d at 1035–36. *Power Ventures* involved access to non-public Facebook user data stored within a password-protected computer system—a system constructed by Facebook "to limit and control access to its website" and that requires third-party developers or websites that wish to access Facebook data to do so via Facebook's application programming interfaces (APIs). *Power Ventures*, 844 F.3d at 1063.

[110] *See infra* Section III.B.

[111] United States v. Nosal (*Nosal I*), 676 F.3d 854, 857 (9th Cir. 2012).

[112] *Power Ventures*, 844 F.3d at 1067; *Nosal II*, 844 F.3d at 1036.

[113] Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976 (codified as amended in scattered sections of 18 and 28 U.S.C.).

a remote campsite,[114] 30,000 feet above sea level,[115] deep underwater,[116] and even from low Earth orbit.[117] But in 1984, the modern Internet was barely a year old.[118] The word "cyberspace" was only starting to appear in popular culture.[119] Even by the start of 1986, with the total number of networks connected via the Internet up to 2,000,[120] accessing another person's computer was relatively rare.

It was in this context, with the Internet in its infancy, that Congress sought to do something to address the threat presented by "so-called 'hackers'" who trespassed into computer systems.[121] After a "flurry of electronic trespassing incidents," Congress was concerned about nightmare scenarios like that depicted in *WarGames—i.e.*, young Matthew Broderick breaking into a U.S. military supercomputer and unwittingly almost starting nuclear war—which it (incorrectly) viewed as a "realistic representation of the automatic dialing and access capabilities of the personal computer."[122] It crafted the CFAA precursor, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, to target such serious and malicious computer break-ins. The 1984

[114] Gerlinda Grimes, *5 Camping Gadgets for Serious Internet Addicts*, HOWSTUFFWORKS, https://adventure.howstuffworks.com/outdoor-activities/hiking/5-camping-gadgets-for-serious-internet-addicts.htm [https://perma.cc/3PH6-T44J] (last visited May 30, 2018).

[115] Aeyne Schriber, *Gogo Inflight Internet: Is It Worthwhile?*, INTERNET ACCESS GUIDE, http://internet-access-guide.com/gogo-inflight-internet-is-it-worthwhile/ [https://perma.cc/YD4W-E593] ("Gogo Inflight Internet works basically the same way except your mobile device is changing towers 30,000 feet above the earth. The towers are configured by Aircell which is the company behind Gogo Inflight Internet. During your flight, the airline network is continually switching towers as you travel and results in a reasonably fast and reliable Internet connection.") (last visited May 30, 2018).

[116] Jeremy Kingsley, *How do submarines get online?*, WIRED (May 29, 2014), https://www.wired.co.uk/article/undersea-internet [https://perma.cc/XK27-CN6M].

[117] Adrienne LaFrance, *The Internet in Space? Slow as Dial Up*, ATLANTIC, (June 11, 2015), https://www.theatlantic.com/technology/archive/2015/06/the-internet-in-space-slow-dial-up-lasers-satellites/395618/ [https://perma.cc/64N4-X8BU].

[118] *See* BARRY M. LEINER ET AL., INTERNET SOC'Y, BRIEF HISTORY OF THE INTERNET 9–10 (1997), https://cdn.prod.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf [https://perma.cc/7A22-VHZR].

[119] "Cyberspace" made its first appearance in a novel in 1984. *March 17, 1948: William Gibson, Father of Cyberspace*, WIRED (Mar. 16, 2009), https://www.wired.com/2009/03/march-17-1948-william-gibson-father-of-cyberspace-2/ [https://perma.cc/5722-D3P4].

[120] *Internet History of 1980s*, COMPUTER HISTORY MUSEUM, http://www.computerhistory.org/internethistory/1980s/ [https://perma.cc/CW36-53YU] (last visited Apr. 5, 2018).

[121] H.R. REP. NO. 98-894, at 10 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3695.

[122] A House Committee Report (incorrectly) characterized *WarGames*, the 1983 techno-thriller film, as "a realistic representation of the automatic dialing and access capabilities of the personal computer." *Id.*, *reprinted in* 1984 U.S.C.C.A.N. 3689, 3696.

House Committee Report explained, "the conduct prohibited is analogous to that of 'breaking and entering'"—and not "using a computer (similar to the use of a gun) in committing the offense."[123] The Report talks in terms of private computer systems protected by "password codes" and expresses concern over "personal computer[s]" giving users the power "to break into other computer systems by systematically speeding up what would otherwise be a slow, hit or miss process."[124] As an example of what Congress intended to target, the Report identified an incident involving an individual who had "stole[n] confidential software" from a previous employer "by tapping into the computer system of [the] previous employer from [a] remote terminal."[125] Federal chargers were brought, but according to the Report, the individual would have escaped federal prosecution—despite a clear computer break-in—had he not made two of his fifty access calls from across state lines.[126] The Report called for a statutory solution to ensure that such computer intrusions would not evade prosecution.

As another example of the conduct targeted, the Senate Committee Report to the 1986 bill—the Computer Fraud and Abuse Act—cited an adolescent gang that "broke into the computer system at Memorial Sloan-Kettering Cancer Center in New York" and "gained access to the radiation treatment records of 6,000 past and present cancer patients"—which meant that they "had at their fingertips the ability to alter the radiation treatment levels that each patient received."[127] It was this sort of serious, technical, and exploitative behavior—breaking into a private computer system for the purpose of accessing or altering non-public information—that Congress sought to outlaw.[128]

The Senate Committee Report explained that it did not intend the CFAA to be so broad as to cover every crime involving a computer, stating, "[i]t has been suggested that, because some States lack comprehensive computer crime statutes of their own, the Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered. The Committee rejects this approach. . . ."[129] The report noted that it specifically was not targeting the actions of "an employee or other individual who, while author-

[123] *Id*. at 20, *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706.

[124] *Id*. at 10-11, *reprinted in* 1984 U.S.C.C.A.N. 3689, 3696 ("Another way of saying this is that prior to the personal computer, password codes were generally satisfactory due to the security inherent in the tedious trial of combinations necessary to break the passwords manually. This aspect is now gone.").

[125] *Id*. at 6, *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691–92.

[126] *Id*.

[127] S. REP. NO. 99-432, at 2–3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2480.

[128] *See, e.g*., LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130–31 (9th Cir. 2009) ("The act was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives. . . .'") (quoting H.R. REP. NO. 98–894, at 9 (1984) (second alteration in original).

[129] S. REP. NO. 99-432, at 4, *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.

ized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at."[130] The Committee noted that "administrative sanctions" would be "more appropriate than criminal punishment in such a case" and recognized the need for "a clear method of delineating which individuals are authorized to access certain of its data."[131]

Proponents of an expansive interpretation of the CFAA—one not limited to serious computer break-ins—point out that the CFAA's precursor applied to anyone who, knowingly "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby obtains information."[132] They argue that Congress's substitution of this "wordy" phrase with a more concise defined term, "exceeds authorized access," was intended only to simplify the statute's language—not modify its substantive meaning.[133] As Judge John D. Bates of the U.S. District Court of the District of Columbia recently recognized, however, "it is notable that Congress did not simply transpose the existing, purpose-oriented language into the definition section—which still would have simplified the language of § 1030(a), as desired—but instead replaced it with new language that focuses on authorization to access particular information."[134] Judge Bates held, "if Congress did not think it was making a substantive change, the legislative history suggests that this was because Congress thought the initial language also was limited to access . . . ."[135]

---

[130] *Id.* at 7, *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2485. The Second Circuit found that the Committee was likely "explaining its removal of 'exceeds authorized access' as a basis for liability under subsection (a)(3), rather than the substitution of 'exceeds authorized access' in other provisions of the statute, including subsection (a)(2)." *See, e.g.*, United States v. Valle, 807 F.3d 508, 526 (2d Cir. 2015). But at that time, subsection (a)(2) was interpreted narrowly, protecting only highly sensitive information such as personal financial information. *See, e.g.*, *Nosal I*, 676 F.3d 854, 858 (9th Cir. 2012). The Committee's explanation thus demonstrates an acknowledgment that the CFAA was not meant to broadly cover computer misuse. As the Second Circuit explained, "[e]ach of these revisions was directed toward the same problem: an employee with authorization to access certain databases entering other databases to which his authorization did not extend." *Valle*, 807 F.3d. at 526. The Committee "understood authorization in spatial terms, namely, an employee going beyond the parameters of his access rights." *Id.*

[131] S. REP. NO. 99-432, at 7, *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2485.

[132] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98–473, tit. II, ch. 21, § 2102(a)(2), 98 Stat. 1837, 2190–91 (codified as amended at § 1030(a)(1)–(2)).

[133] *See, e.g.*, 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, 1534–35 (2016).

[134] Sandvig v. Sessions, No. CV 16-1368 (JDB), 2018 WL 1568881, at *14 (D.D.C. Mar. 30, 2018).

[135] *Id.*

There are, of course, limits to the degree to which legislative history is dispositive. It cannot tell us what the statute's terms actually mean, because "it is the function of the courts and not the Legislature . . . to say what an enacted statute means."[136] It can, however, provide the "broader context of enactment" and help "to explain the text's purpose and meaning."[137] Indeed, legislative history "contains the best available evidence of both the context and the circumstances of enactment."[138] And as courts across the country have recognized, the CFAA's statutory context establishes that Congress sought to target serious computer break-ins in response to a series of high profile computer trespassing incidents.[139]

B. Breaking-In Requires a Private, Non-Public System

Because the CFAA's unauthorized access provisions were intended to require a computer break-in, they cannot apply to publicly available information on the Web. It is impossible to break into the open Web, because it is inherently public and open to all. Open access is fundamental to how the Internet works. "A person who connects a webserver to the Internet agrees to let all access the computer much like one who sells his wares at a public fair agrees

---

[136] Pierce v. Underwood, 487 U.S. 552, 566 (1988).

[137] George A. Costello, *Average Voting Members and Other "Benign Fictions": The Relative Reliability of Committee Reports, Floor Debates, and Other Sources of Legislative History*, 1990 DUKE L.J. 39, 65 (1990).

[138] *Id.*; *see also* John F. Manning, *Textualism as a Nondelegation Doctrine*, 97 COLUM. L. REV. 673, 701 n.119 (1997) (opining that policy evaluation is a judicial tool "so traditional that it has been enshrined in Latin: 'Ratio est legis anima; mutata legis ratione mutatur et lex'"— *i.e.*, "'The reason for the law is its soul; when the reason for the law changes, the law changes as well.'") (citing Antonin Scalia, *Judicial Deference to Administrative Interpretations of Law*, 1989 DUKE L.J. 511, 517) (internal quotation marks omitted).

[139] *See, e.g.*, Sandvig, 2018 WL 1568881, at *13 ("The statutory context buttresses this narrower reading of the text."); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 201, 207 (4th Cir. 2012) (noting that although the statute was amended in 1994 to add a civil provision, it "remains primarily a criminal statute designed to combat hacking," and, as such, jurisprudential care should be taken not to "contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to [defendants] who access computers or information in bad faith. . . ."); *Valle*, 807 F.3d at 525 (noting that "Congress enacted the CFAA in 1984 to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data[,]" and the statute's legislative history "consistently characterizes the evil to be remedied—computer crime—as 'trespass' into computer systems or data, and correspondingly describes 'authorization' in terms of the portion of the computer's data to which one's access rights extend.") (citing H.R. REP. NO. 98–894, at 5-6, 9-11 (1984), *as reprinted in* 1984 U.S.C.C.A.N 3689, 3691–92, 3695–97; S. REP. NO. 99–432, at 2-3, *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2480); Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 932 (E.D. Va. 2010) ("The CFAA is a civil and criminal anti-hacking statute designed to prohibit the use of hacking techniques to gain unauthorized access to electronic data.").

to let everyone see what is for sale."[140] As a technical and practical matter, one cannot publish to the entire world at the same time as keeping people out; content published publicly on the Internet is "open to all."[141] With "no authentication requirement, the web server welcomes all, and the norm is openness to the world"—including "any one of the billion or so Internet users around the world" or "a 'bot,' a computer program running automatically."[142] Internet users understand this; openness is the norm on which the Web was built and on which it functions today.

Pursuant to "the open norm of the World Wide Web," access to websites is inherently authorized "unless it bypasses an authentication gate."[143] Because access to publicly available information lacks an authentication requirement by its very definition, everyone on the Internet is "authorized" to access it.[144] In order to render access "unauthorized," a website must be configured to not respond to every request.[145]

This requires not just any type of code-based limitation, but a code-based authentication gate that lets only authorized users in and keeps unwanted individuals out. "When a limit or restriction does not require authentication, access is still open to all."[146] An IP address block, for example—such as the blocks set up by Facebook in *Power Ventures* and by LinkedIn in *hiQ Labs*—is not a barrier to access. As Professor Orin Kerr argues, IP address blocks "should be construed as merely speed bumps" (and not access restrictions) because "bypassing an IP block is no more culpable than bending your neck to see around someone who has temporarily blocked your view."[147] Indeed, IP addresses change frequently, for a variety of reasons, even without any effort on the part of the Internet users.[148] A person's IP address changes as they move from home to work to a café, or if they use privacy-protecting tools, like Tor or virtual private networks (or VPNs). Merely turning on and off a modem can also cause IP addresses to change. As noted above, the Ninth Circuit itself

[140] Kerr, *supra* note 8, at 1163.

[141] *Id*. at 1164.

[142] *Id*. at 1162.

[143] *Id*. at 1147.

[144] *See, e.g.*, Pulte Homes, Inc. v. Laborers' Int'l Union, 648 F.3d 295, 304 (6th Cir. 2011) (the public is presumptively authorized to access an "unprotected website"); *Craigslist II*, 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013) (making a website publicly available gives everyone "authorization" to view it under the CFAA).

[145] *See* Kerr, *supra* note 8, at 1163 ("[Those] that want to keep people from visiting their websites, shouldn't connect a webserver to the Internet and configure it so that it responds to every request.").

[146] *Id*. at 1164 ("The limit should be construed as insufficient to overcome the open nature of the Web. On the other hand, access that bypasses an authentication gate should, under proper circumstances, be deemed an unauthorized trespass.").

[147] *See id*. at 1161, 1168.

[148] *Id*. at 1168.

recognized in *Power Ventures* that IP address blocks are not authentication barriers. The court explained that a user whose IP address has been blocked,

> does not receive notice that he has been blocked, [so] he may never realize that the block was imposed and that authorization was revoked. Or, even if he does discover the block, he could conclude that it was triggered by misconduct by someone else who shares the same IP address, such as the user's roommate or co-worker.[149]

Even if a user receives notice of the block, an IP address block does not become an authentication barrier, because it still does not require authentication. "IP blocking cannot keep anyone out."[150]

Nor can an individualized cease and desist letter purporting to revoke access to publicly available data keep anyone out—whether alone or followed by an IP block. Cease and desist letters and IP blocks do the same (limited) thing: they "indicate[] that the computer owner does not want at least someone at the IP address to visit the website."[151] They are both comparable to "publishing a newspaper but then forbidding someone to read it."[152] But a computer owner's "subjective desire" does not overcome the Internet's open trespass norms, whether communicated in terms of an individualizes letter or an IP address block.[153] Thus, while ignoring a cease and desist letter and/or bypassing an IP address block may be contrary to the desires of the computer owner, it does not equate to criminal circumvention of a code-based access restriction; it does not rise to the level of a computer break-in.

Courts have recognized that websites cannot revoke authorization to access data that is publicly available on the Web, or accessible "without requiring any login, password, or other individualized grant of access . . . ."[154] As the Eastern District of Virginia held in 2010, by making information publicly available on the Internet, "the entire world [is] given unimpeded access . . . ."[155] The Northern District of California, in 2017, compared a prohibition on accessing publicly available data to a prohibition on viewing a publicly visible sign: "[I]f a business displayed a sign in its storefront window visible to all on a public

---

[149] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1068 (9th Cir. 2016).

[150] Kerr, *supra* note 8, at 1168–69 ("Because of these technical realities, bypassing an IP block is no more culpable than bending your neck to see around someone who has temporarily blocked your view.").

[151] *Id*.

[152] *Id*. at 1169.

[153] *Id*.

[154] Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 932 (E.D. Va. 2010); *see also* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1112–14 (N.D. Cal. 2017); *cf.* Ampex Corp. v. Cargle, 128 Cal. App. 4th Supp. 1569, 1576, 27 Cal. Rptr. 3d 863, 869 (2005) ("Web sites that are accessible free of charge to any member of the public where members of the public may read the views and information posted, and post their own opinions, meet the definition of a public forum for purposes of [California's anti–SLAPP statute].").

[155] *Eventbrite*, 739 F. Supp. 2d at 933.

street and sidewalk, it could not ban an individual from looking at the sign and subject such person to trespass for violating such a ban."[156] And the District Court of the District of Colombia, in 2018, held that "only code-based restrictions, which 'carve[ ] out a virtual private space within the website or service that requires proper authentication to gain access,' remove those protected portions of a site from the public forum."[157]

Other courts, however, have held that websites can, for purposes of the CFAA, revoke authorization to access publicly available information on the Web.[158] These courts have relied on flawed and problematic reasoning.[159] They have focused on whether a defendant's "authorization was ever rescinded or limited" and have ignored the more important question: what type of authorization, to what type of data, was granted in the first place?[160] This analysis is backwards. In order to assess whether authorization for purposes of the CFAA can be rescinded, a court must first look to whether the defendant was affirmatively granted authorization to access a private system protected by a code-based authentication barrier, or whether the defendant was granted implicit and irrevocable authorization—along with the rest of the world—to access publicly available information on the open Web. In the latter case, authorization cannot be rescinded or limited, except via construction of some code-based authentication barrier that renders the data no longer public.[161]

Even courts that have applied the CFAA's unauthorized access provisions to publicly available data have acknowledged that "[a]pplying the CFAA to pub-

[156] *hiQ Labs*, 273 F. Supp. 3d at 1103–04, 1112–13 ("[T]he Court is doubtful that the Computer Fraud and Abuse Act may be invoked . . . to punish [access of publicly available data].").

[157] Sandvig v. Sessions, No. CV 16-1368 (JDB), 2018 WL 1568881, at *5 (D.D.C. Mar. 30, 2018) (quoting Kerr, *supra* note 8, at 1171).

[158] *See, e.g.*, QVC, Inc. v. Resultly, LLC, 159 F. Supp. 3d 576, 596–97 (E.D. Pa. 2016).

[159] *See* Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 528 (2003) (describing "the judicial application of the [CFAA], which was designed to punish malicious hackers, to make it illegal—indeed, criminal—to [those who] seek information from a publicly available website if doing so would violate the terms of [use]" as a serious problem).

[160] *See QVC*, 159 F. Supp. 3d at 596 ("The relevant question is not whether [the defendant] was granted permission to access the information on [the website], but whether that authorization was ever rescinded or limited in a way that would put [the defendant] on notice that it was not authorized to access information it was otherwise entitled to access.").

[161] *See* Kerr, *supra* note 8, at 1161 ("The authorization line should be deemed crossed only when access is gained by bypassing an authentication requirement. An authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web."); *see also id.* at 1163 ("A person who connects a web server to the Internet agrees to let everyone access the computer much like one who sells his wares at a public fair agrees to let everyone see what is for sale. Sellers who want to keep people out, backed by the authority of criminal trespass law, shouldn't set up shop at a public fair.").

licly available website information presents uncomfortable possibilities."[162] In *Craigslist Inc. v. 3Taps Inc.*, the court pointed to a need for clarification from the courts of appeal, stating that it would assume the CFAA covered restrictions on the use of otherwise public information "until the Ninth Circuit holds otherwise" but noting the "potential problems with an overly expansive interpretation of the CFAA."[163] The recent scraping cases will give courts—including the Ninth Circuit—the opportunity to clarify, if further clarification were needed, that Congress never intended merely accessing publicly available information on the Web to give rise to liability under the CFAA.

IV. ALLOWING COMPANIES TO USE THE CFAA TO POLICE ACCESS AND USE OF PUBLICLY AVAILABLE INFORMATION ON THE INTERNET WILL HARM THE OPEN WEB

Ensuring that the CFAA remains limited to its original purpose is not merely a matter of principal. First, it is necessary to ensure that the CFAA is not rendered void for vagueness. A criminal statute that fails to provide fair notice of what is criminal—or that threatens arbitrary and discriminatory enforcement by failing to provide "explicit standards for those who apply them" and thereby "impermissibly delegating basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis"—is void for vagueness.[164] While the original 1984 statute was narrow and specific—"tailored to [protecting] . . . national security, financial records, and government property"—after five separate amendments, each of which expanded the statue's scope, the CFAA became "one of the most far-reaching criminal laws in the United States Code."[165] The meaning of "authorization" is the statute's only limiting principle—and thus the only thing saving the statute from being void for vagueness. What Congress originally had in mind is therefore especially important. Granting websites the ability to render criminal someone's, or some organization's, use of commonplace automated Web browsing tools to access publicly available information by merely sending a letter would not only contravene Congress's intent, but it would "impermissibly delegat[e]" to private entities the ability to define the scope of criminal law and threaten arbitrary and discriminatory enforcement—specifically, enforcement only against competitors or anyone else a website does not like—and render the statute constitutionally void.[166]

---

[162] *Craigslist I*, 942 F. Supp. 2d 962, 969–70 n.8 (N.D. Cal. 2013).

[163] *Id.*

[164] *See* Skilling v. United States, 561 U.S. 358, 412 (2010) (citing Kolender v. Lawson, 461 U.S. 352, 357 (1983)); Grayned v. Rockford, 408 U.S. 104, 108–09 (1972).

[165] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561, 1564 (2010) (tracing the history of the CFAA and Congress's repeated expansions of the statute's scope).

[166] *See Grayned*, 408 U.S. at 108–09.

Second, it is necessary to ensure that the CFAA cannot be used to undermine open access to publicly available information online, "a result that Congress could not have intended when it enacted the CFAA over three decades ago."[167] If it were a crime to continue accessing a website after receiving a cease and desist letter asking you to stop visiting the site, for whatever reason, websites would have the power to cut off free and unrestricted access to "the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge."[168] If a website disagreed with an investigative journalist or researcher's purpose or manner of access, for example, it could render that research criminal by merely sending a cease and desist letter or updating its terms of service.[169] This is not a trivial example. Journalists and researchers increasingly rely on automated tools, including automated Web browsing tools, to support their work—much of which is protected First Amendment activity.[170] Automated Web browsing is "one of the most powerful techniques for data-savvy journalists who want to get to the story first, or find exclusives that no one else has spotted."[171] ProPublica journalists have investigated Amazon's algorithm for ranking products by price via a "software program that simulated a non-Prime Amazon member" and "scraped . . . product listing page[s]"; their research uncovered that Amazon's pricing algorithm was hiding the best deals from many of its customers.[172] The San Francisco Chronicle has also used automated Web browsing tools, to gather

[167] hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1103–04 (N.D. Cal. 2017) (noting that a "broad interpretation" of the CFAA, "if adopted, could profoundly impact open access to the Internet").

[168] Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017).

[169] *See, e.g.*, Fidlar Techs. v. LPS Real Estate Data Sols., Inc., 810 F.3d 1075, 1082 (7th Cir. 2016) (noting in a case involving allegations of illegal scraping that "[i]n an internal e-mail, a Fidlar employee stated that Fidlar could make screen-scraping or web-harvesting illegal with a 'simple disclaimer that states the information can't be scraped from the image'").

[170] Indeed, the mere "act of viewing a publicly accessible website is likely protected by the First Amendment." *hiQ Labs*, 273 F. Supp. 3d at 1114 n.12; *see also* Board of Edu., Island Trees Union Free School Dist. No. 26 v. Pico, 457 U.S. 853, 867 (1982) (noting that the right to receive information "is an inherent corollary of the rights of free speech and press that are explicitly guaranteed by the Constitution").

[171] *E.g.*, Paul Bradshaw, *Leanpub, Scraping for Journalists (2nd edition): About the Book,* LEANPUB, https://leanpub.com/scrapingforjournalists [https://perma.cc/443V-S9LS] (last updated Sept. 11, 2017).

[172] Julia Angwin and Surya Mattu, *How We Analyzed Amazon's Shopping Algorithm*, PROPUBLICA (Sept. 20, 2016), https://www.propublica.org/article/how-we-analyzed-amazons-shopping-algorithm [https://perma.cc/J6S6-SJHF].

data on Airbnb properties in order to assess the impact of Airbnb listings on the San Francisco rental market.[173]

In today's increasingly data-driven world, discrimination research—which has historically proven necessary for ensuring compliance with federal and state anti-discrimination laws[174]—also requires the use of a variety of techniques, including automated tools that many websites ban, in order to conduct audit testing and uncover whether and how any particular website is treating users differently. In a recent study of racial discrimination on Airbnb, for example, researchers "sent inquiries to Airbnb hosts using web browser automation tools" and "collected all data using scrapers"—discovering that distinctively African American names were sixteen percent less likely to be accepted relative to identical guests with distinctively white names.[175] In another study, Carnegie Mellon University researchers looked at discrimination in online ad delivery via "an automated tool that explore[d] how user behaviors, Google's ads, and Ad Settings interact" and found that "setting the gender to female resulted in getting fewer instances of an ad related to high paying jobs than setting it to male."[176] A growing body of evidence shows that proprietary algorithms are causing websites to discriminate among users, including on the basis of race, gender, and other characteristics protected under civil rights laws. As algorithms and artificial intelligence are increasingly relied upon to make decisions that impact people's lives, researchers need the ability to use automated tools to effectively uncover discrimination.

The academic research community also relies on open access to information. Open access to research and scholarship—which includes "non-restrictively allowing researchers to use automated tools to mine the scholarly literature"—has "ensur[ed] rapid and widespread access to research findings such that all communities have the opportunity to build upon them and participate in schol-

[173] Carolyn Said, *Window into Abirbnb's hidden impact on S.F.*, S.F. CHRON., (June 2014) https://www.sfgate.com/business/item/Window-into-Airbnb-s-hidden-impact-on-S-F-30110.php [https://perma.cc/JW35-HNTK].

[174] Offline audit testing has long been recognized as a crucial way to uncover racial discrimination in housing and employment and to vindicate civil rights laws, particularly the Fair Housing Act and Title VII's prohibition on employment discrimination. *Cf.* Havens Realty Corp. v. Coleman, 455 U.S. 363, 373 (1982).

[175] Benjamin Edelman, Michael Luca & Dan Svirsky, *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, 9 AM. ECON. J.: APPLIED ECON. 1, at 1, 7 (Apr. 2017), https://www.aeaweb.org/articles?id=10.1257/app.20160213 [https://perma.cc/X2P8-THW7].

[176] Amit Datta, Michael Carl Tschantz & Anupam Datta, *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination*, 2015 PROC. ON PRIVACY ENHANCING TECHS. 92, at 92 (Apr. 2015), https://doi.org/10.1515/popets-2015-0007 [https://perma.cc/XKM5-4X3F].

arly conversations."[177] And because open access to academic scholarship leads to more media coverage, including via social media, open access allows for broader societal impact.[178]

Imposing potential CFAA liability for using automated Web browsing tools to access publicly available information will chill the use of these societally valuable research tools. To avoid the threat of criminal prosecution, journalists, researchers, and academics will refrain from conducting their socially valuable and constitutionally protected research. In an era of infinite data, a ruling that chills such research will handicap research and journalism, while giving the handful of corporations with the world's largest datasets the upper hand. A company's choice to prohibit investigative journalism or socially valuable research using information publicly available on the open Internet should not be enforceable as a federal criminal offense—especially not under a statute meant to target computer break-ins.

In an era of algorithms, machine learning, and artificial intelligence, allowing companies to use the CFAA to restrict access to publicly available information will also inevitably create an uneven playing field in favor of established players. It will chill innovation by effectively allowing corporations with the largest datasets to control the use of publicly available information on the Web. Alterative search engines, like DuckDuckGo, for example, might never have survived under such a rule, as it might have been either blocked from accessing publicly available data across the Web or chilled from even trying thanks to the threat of potential federal criminal prosecution. And if merely sending a cease and desist letter made it a crime to access publicly available information via automated scripts, this would create legal uncertainty for all automated Web browsing. This will undoubtedly chill[179] the creation and use of many useful Web browsing tools, despite the fact that automated Web browsing is a common and critical online practice.[180] Useful automated Web

[177] Jonathan P. Tennant et al., *The Academic, Economic and Societal Impacts of Open Access: An Evidence-Based Review*, F1000RESEARCH, at 4, 6 (2016), https://f1000research.com/articles/5-632/v3 [https://perma.cc/4KWW-SV89].

[178] *Id.* at 8.

[179] The uncertainty created via some courts' overbroad interpretation of the CFAA has already chilled the work of computer security researchers. *See* Letter from Comput. Sec. Experts to Congress and Members of the Senate and House Comm. on the Judiciary (Aug. 1, 2013), https://www.eff.org/document/letter-def-con-cfaa-reform [https://perma.cc/FK8C-C2EZ] ("Many of our colleagues, and many of us, have directly experienced the chilling effects of the CFAA. Actual litigation or prosecution of security researchers is, to be sure, quite rare. But that's because the mere risk of litigation or a federal prosecution is frequently sufficient to induce a researcher (or their educational or other institution) to abandon or change a useful project. Some of us have jettisoned work due to legal threats or fears.").

[180] *See supra* note 11. Automated Web browsing tools include: feed fetcher "bots" that "ferry website content to mobile and web applications, which they then display to users"; Web crawlers that "collect [or scrape] information for search engine algorithms, which is

browsing tools automatically scrape the public Internet to collect, aggregate, and index publicly available information and support various business and operational goals of their owners—from individual Internet users to multinational corporations. These tools include Google's Crisis Map, which during California's October 2017 wildfires aggregated information about the fires, topology, traffic, shelter availability, and resource needs,[181] and the Internet Archive's Web crawler project, which works to archive as much of the public Web as possible.[182] Creating legal uncertainty for automated Web browsing would make it even more difficult for new or smaller companies to create their new tools. Prohibitions on automated access are a standard provision in websites' computer use policies, so all automated Web browsing tools—other than those operated by established companies that have already been granted express and widespread permission to crawl the Web, like Google's search engine crawler—will be at risk.

There are, of course, bots designed to cause harm, such as by overwhelming computers with traffic via a Distributed Denial of Service (DDoS) attack,[183] but existing legal protections target this activity. The CFAA itself, in section 1030(a)(5)(A), prohibits "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer."[184] There is thus no need to stretch the CFAA's unauthorized access provisions to cover such malicious bots; they are already covered. And indeed, the recent scraping cases have nothing at all to do with stopping malicious bots. They involve

---

then used to make ranking decisions[,]" and systematically index pages and data; commercial crawlers that are "[s]piders used for authorized data extractions, usually on behalf of digital marketing tools"; and monitoring bots, which "monitor website availability and the proper functioning of various online features." *See* Igal Zeifman, *Bot Traffic Report 2016*, INCAPSULA (Jan. 24, 2017), https://www.incapsula.com/blog/bot-traffic-report-2016.html [https://perma.cc/744J-T4XQ]. The Incapsula study estimated that in 2016, "good" bots accounted for twenty-three percent of global Web traffic, and that Internet bots on the whole accounted for fifty-two percent of Web traffic, whereas humans accounted for only forty-eight percent. *Id*.

[181] *See Crisis Map Help: About Google Crisis Map*, GOOGLE, https://support.google.com/crisismaps [https://perma.cc/X8AT-XFH5] (last visited Mar. 29, 2018) ("Crisis Map collects information that's normally scattered across the Web and other resources and makes it easily available through a single map. Find authoritative information as well as crowd-sourced data, all in one place.").

[182] *See* HERITRIX, https://webarchive.jira.com/wiki/x/8Ao (last visited Mar. 29, 2018) ("Heritrix is the Internet Archive's open-source, extensible, web-scale, archival-quality web crawler" that "seeks to collect and preserve the digital artifacts of our culture for the benefit of future researchers and generations[.]").

[183] *What is a DDoS Attack?*, DIGITAL ATTACK MAP, https://www.digitalattackmap.com/understanding-ddos/ [https://perma.cc/9WFK-RJ25] (last visited May 30, 2018).

[184] 18 U.S.C. § 1030(a)(5)(A).

commonplace automated Web browsing tools that merely make collection of publicly available information easier, and companies' attempts to use the CFAA block competitors from using those tools.

CONCLUSION

The stakes of the debate about whether private companies can use the CFAA to police access of publicly available information on the open Web go far beyond the commercial skirmishes at issue in the most recent scraping cases. A broad reading of the CFAA could "profoundly impact open access to the Internet" and "stifle the dynamic evolution and incremental development of state and local laws addressing the delicate balance between open access to information and privacy—all in the name of a federal statute enacted in 1984 before the advent of the World Wide Web."[185] Courts should not allow the fate of the Web to turn on corporate interests and computer use preferences. Ensuring that the CFAA remains limited to its original purpose and is not transformed into a tool for policing Internet use is thus not merely a matter of principal; it is necessary for ensuring the open Internet of today is the Internet we will enjoy in the future.

[185] hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1103, 1110–11 (N.D. Cal. 2017).