IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES,	)	
Appellee,	)	BRIEF OF ELECTRONIC
	)	FRONTIER FOUNDATION AND
	)	NATIONAL ASSOCIATION OF
	)	CRIMINAL DEFENSE LAWYERS
v.	)	AS *AMICI CURIAE* IN SUPPORT
	)	OF APPELLANT
Private First Class (E-3)	)	
CHELSEA E. MANNING	)	Crim. App. Dkt. No 20130739
United States Army,	)	USCA Dkt. No. 18-0317/AR
Appellant.	)	

TO THE HONORABLE JUDGES OF THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

The Electronic Frontier Foundation (EFF) and the National Association of Criminal Defense Lawyers (NACDL), pursuant to Rules 26(a)(3) of this Court, respectfully submit this brief as *amici curiae* in support of Appellant Chelsea E. Manning's petition for review of the decision of the Court of Criminal Appeals.

/s/ Jamie Williams
(Motion for Appearance
pro hac vice pending)
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jamie@eff.org

Counsel for *Amici Curiae*

INDEX OF BRIEF

TABLE OF CASES, STATUTES, AND OTHER AUTHORITIES

Cases

Int'l Airport Ctrs. v. Citrin,
440 F.3d 418 (7th Cir. 2006) 15

Kolender v. Lawson,
461 U.S. 352 (1983)...24

Lane v. Brocq,
No. 15 C 6177, 2016 WL 1271051 (N.D. Ill. Mar. 28, 2016)............................12

LVRC Holdings LLC v. Brekka,
581 F.3d 1127 (9th Cir. 2009) 9, 12

Oracle v. Rimini St.,
879 F.3d 948 (9th Cir. 2018) 3, 20

Power Equip. Maint., Inc. v. AIRCO Power Servs., Inc.,
953 F. Supp. 2d 1290 (S.D. Ga. 2013)..12

Sandvig v. Sessions,
No. CV 16-1368 (JDB), 2018 WL 1568881 (D.D.C. Mar. 30, 2018)....................
12, 19, 20, 21

Skilling v. United States,
561 U.S. 358 (2010)...24

United States v. John,
597 F.3d 263 (5th Cir. 2010) 15

United States v. Kozminski,
487 U.S. 931 (1988)...29

United States v. Lanier,
520 U.S. 259 (1997)...24

United States v. Nosal,
676 F.3d 854 (9th Cir. 2012) ....*passim*

United States v. Rodriguez,
628 F.3d 1258 (11th Cir. 2010) 15

United States v. Santos,
553 U.S. 507 (2008)...24

Statutes

Other Authorities

ENES, Script Based Download 8

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 (1990) 11

GNU, Wget Manual 6

Google, Crisis Map Help: About Google Crisis Map (2017) 28

Import.io, Solutions Overview 26

John F. Manning, *Textualism as a Nondelegation Doctrine*, 97 Colum. L. Rev. n.119 (1997) 11

Jonathan P. Tennant, *et al.*, *The academic, economic and societal impacts of Open Access: an evidence-based review,* F1000Research (2016) 28

Julia Angwin and Surya Mattu, “How We Analyzed Amazon’s Shopping Algorithm,” *ProPublica* (Sep. 20, 2016) 27

Leanpub, Scraping for Journalists (2nd edition): About the Book (Sep. 11, 2017) 26

Margaret Rouse, “search-and-replace,” TechTarget 5

Orin Kerr, *The CFAA Meets the “Cannibal Cop” in the Second Circuit—and Maybe Beyond*, Wash. Post: The' Volokh Conspiracy (May 13, 2015) 17

Orin S. Kerr, C*ybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1663 (2003) 15

Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010) 4, 25

Techopedia, “Web Browser” 5

Wikipedia, “My Yahoo!” (last updated Aug. 14, 2018) 7

Wikipedia, “Web portal” (last updated Aug. 23, 2018) 7

Wikipedia, “Wget” 5

Legislative Authorities

STATEMENT OF INTEREST

EFF is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy in the online and digital world for 25 years. With over 40,000 active donors, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age.

NACDL is a nonprofit, voluntary professional bar association, founded in 1958, that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL has a nationwide membership of approximately 9,000 direct members in 28 countries, in addition to 90 state, provincial, and local affiliate organizations totaling up to 40,000 attorneys. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. In furtherance of NACDL's mission to safeguard fundamental constitutional rights, the Association often appears as *amicus* in cases involving overcriminalization.

Amici's interest in this case is in the principled and fair application of the Computer Fraud and Abuse Act. *Amici* are particularly concerned about the implications of overbroad applications of criminal laws such the CFAA on constitutional rights of criminal defendants and on Internet users, innovators, researchers, and journalists.

INRODUCTION

The military judge and appeals court misunderstood the technology at issue and misapplied the precedent they purport to follow. In so doing, they created a new theory of criminal liability under the Computer Fraud and Abuse Act that would, if upheld, transform ordinary online behavior into a federal criminal offense.

This case addresses the scope of the CFAA and whether the statute criminalizes violating written computer use policies, such as policies dictating the method in which information is accessed.

The four most recent federal circuit courts to address the issue have said no: violating a contractual computer use policy or using a work computer for non-work purposes does not violate the CFAA. A narrow interpretation, these courts have recognized, is necessary to avoid criminalizing common, innocuous conduct that lies beyond the statute's "anti-hacking" purpose and running afoul of the Rule of Lenity. *See WEC Carolina Energy v. Miller*, 687 F.3d 199, 119 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 858–59 (9th Cir. 2012) (en banc) ("*Nosal I*"); *United States v. Valle*, 807 F.3d 508, 527–28 (2nd Cir. 2015); *United States v. Thomas*, 877 F.3d 591, 596 (5th Cir. 2017).

The lower courts' decisions both purport to be consistent with this narrow, prevailing, reading of the statute. Both hold, however, that the CFAA criminalizes violating written computer use restrictions on the method in which data may be accessed. This holding is inconsistent with the very precedent cited and relies on an erroneous premise—which has been rejected by both federal circuit courts to have addressed it—that written restrictions on the method in which information is accessed should be treated differently than other types of written computer use restrictions. *See WEC Carolina,* 687 F.3d at 206; *Oracle v. Rimini St.*, 879 F.3d 948, 962 (9th Cir. 2018).

Despite claiming not to, the courts below transform the CFAA from the "anti-hacking" statute Congress intended into a tool to enforce contractual computer use policies via the force of criminal law. Their decisions, if upheld, would render the statute unconstitutionally vague. This Court should grant review to correct the lower courts' errors.

ARGUMENT

The CFAA makes it a crime to "intentionally access[] a computer without authorization from any protected computer"[1]—which includes any computer connected to the Internet. 18 U.S.C. §§ 1030(a)(2)(C), (e)(2)(B).[2] The question before the lower courts was whether Appellant "exceed[ed] authorized access" when she accessed information she was generally entitled to access in a method not permitted by the applicable written computer use policy, which prohibits using unauthorized software on systems connected via SIPRNet, the Defense Department's classified version of the civilian Internet.

The military judge and the appeals court held that by using a common software utility for downloading information from the Web called Wget to download materials via a State Department portal on SIPRNet —which Appellant

[1] The CFAA section Appellant was charged under requires "obtain[ing] information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations" and "willfully communicat[ing], deliver[ing], transmit[ting]. . . [the information] to any person not entitled to receive it[.]" 18 U.S.C. § 1030(a)(1). This Court's interpretation of "without authorization," however, must apply equally to the statute's other sections—including its broadest subsection, section 1030(a)(2), which is not limited to classified information and requires no culpable intent. *See IBP, Inc. v. Alvarez*, 546 U.S. 21, 22 (2005).

[2] "Protected computer" includes computers "used in or *affecting* interstate or foreign commerce or communication" and thus reaches as far the as Commerce Clause can extend. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1570–71 (2010) (emphasis added).

was authorized to access—she violated the computer use policy and "exceed[ed] [her] authorized access."[3] This holding is based on a flawed understanding of the technology at issue, the fundamental purpose of the CFAA, and the very precedent the courts purport to follow and, if upheld, would render the statute unconstitutionally vague. This Court should grant review.

I. The Lower Courts Misconstrued the Technology at Issue.

Wget is a simple, free, open-source utility that has been used since 1996 to download files from the Web.[4] Search-and-replace is another example of a commonly used utility that allows a computer user to find a given sequence of characters in one or more text files—such as Word document—and replace the sequence with another sequence of characters.[5]

Wget allows users to automatically retrieve content from websites that they would otherwise have to download manually. Unlike commonly used Web browser software—which downloads information when a user manually navigates to (or saves[6]) a Web page or clicks on an individual link—Wget simply does the

[3] 31 May 2018 Order, 12; 18 July 2013 Order, 6.

[4] Wikipedia, "Wget," https://en.wikipedia.org/wiki/Wget.

[5] Margaret Rouse, "search-and-replace," TechTarget, https://whatis.techtarget.com/definition/search-and-replace.

[6] Techopedia, "Web Browser," https://www.techopedia.com/definition/288/web-browser; *see also* Google Chrome Help, Read pages later and offline, https://support.google.com/chrome/answer/7343019?co=GENIE.Platform%3DDes

work for the user, downloading the linked data or Web pages one after another, in an automated fashion.[7] Wget can only be used to access information that the user could otherwise access manually with a Web browser.

Wget is one of many automated Web browsing techniques used routinely across the Web for countless applications, such as aggregating information from multiple sources and identifying and extracting data for analysis.[8] Such tools are used by journalists, businesses, academics, and researchers.[9] They can help competition by lowering startup information barriers,[10] for example, or identify and correct issues of algorithmic bias.[11]

The appeals court erroneously found that Wget "allowed [Appellant] to access" cables "by *circumventing* the [State Department] portal and contacting the server directly, which allowed her to directly download the cables onto her hard

ktop&hl=en; Mozilla Firefox Support, How to save a web page, https://support.mozilla.org/en-US/kb/how-save-web-page.

[7] GNU, Wget Manual, https://www.gnu.org/software/wget/manual/html_node/Overview.html#Overview.

[8] Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, Boston University Journal of Science and Technology Law, Forthcoming, 5 (July 28, 2018), https://ssrn.com/abstract=3221625.

[9] *See infra* Section III.

[10] Sellars, *supra* note 8, at 3.

[11] *See* Amanda Levendowski, *How Copyright Law Can Fix AI's Implicit Bias Problem*, 93 Wash. L. Rev. (forthcoming 2018).

drive[.]" 31 July 2018 Order, 12 (emphasis added). This finding relies on a misunderstanding of both portals and Wget.

First, the court treated the portal as if it were an access barrier that required circumvention. A portal is not an access barrier; it is simply a website that brings information from multiple sources together in a uniform way.[12] The My Yahoo! home page, for example, is one popular Web portal, which aggregates personalized links and content.[13] If you access a news story featured on your My Yahoo! portal via a direct link instead of via the portal, you have not *circumvented* the portal. A portal is not a technical access barrier that must be circumvented in order to obtain information.

Second, while some portals include a user name and password barrier, Wget cannot be used to *circumvent* this or any other technological access barrier that allows only authorized individuals in and keeps unwanted individuals out. When Wget is used to access password-protected information, the portal enforces the same authentication checks that would be required to manually access this data, and the checks are enforced in the same way—the user is asked to provide their

[12] A Web portal is "a specially designed website that brings information from diverse sources, like emails, online forums and search engines, together in a uniform way." Wikipedia, "Web portal" (last updated Aug. 23, 2018), https://en.wikipedia.org/wiki/Web_portal.

[13] Wikipedia, "My Yahoo!" (last updated Aug. 14, 2018) https://en.wikipedia.org/wiki/My_Yahoo!.

password, or Wget relies on the user's valid, locally stored login credentials.[14] Wget cannot be used to gain access to any data that the user could not have accessed manually *without* Wget, because it does not allow a user to circumvent any technological access barriers.

II. The Lower Courts Misconstrued the CFAA's Purpose and Case Law.

The lower courts' holding—that Appellant violated the CFAA by accessing information she was authorized to access in a method prohibited by a computer use policy—is also based on a flawed understanding of the CFAA's legislative intent and the precedent the courts purport to follow.

A. Congress Intended the CFAA to Target Serious Computer Break-Ins.

The CFAA's statutory context is clear: Congress passed the CFAA to target serious computer break-ins. The CFAA's precursor, passed in 1984, was Congress's response to a "flurry of electronic trespassing incidents." H.R. Rep. No. 98–894, U.S.C.C.A.N. 3689, 3696 (1984). Congress was concerned about nightmare scenarios like that depicted in the film *WarGames*—a teenager breaking into a U.S. military supercomputer and unwittingly almost starting nuclear war—

[14] As one website explains, when Wget is used to access information from within its password-protected portal, the script asks for login credentials or uses locally saved login credentials. ENES, Script Based Download, https://portal.enes.org/data/data-metadata-service/search-and-download/script-based-data-access; https://www.earthsystemcog.org/projects/cog/doc/wget.

which it (incorrectly) viewed as a "realistic representation of the automatic dialing and access capabilities of the personal computer." H.R. Rep. No. 98–894, U.S.C.C.A.N. 3689, 3696 (1984). It crafted the CFAA's precursor to target such serious, malicious computer break-ins.

The law was "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[.]'" *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130–31 (9th Cir. 2009) (citation to legislative history omitted); *see also Valle*, 807 F.3d at 525 (Congress sought "to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data."). The 1984 House Committee Report explained, "the conduct prohibited is analogous to that of 'breaking and entering'"— not "using a computer (similar to the use of a gun) in committing the offense." H.R. Rep. No. 98–894, U.S.C.C.A.N. 3689, 3706 (1984). As an example of the conduct targeted, 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." *Id*. at 3691–92. 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. *Id*. 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 CFAA—cited an adolescent gang that "broke into the computer system at [a cancer center] in New York." The group "gained access to the radiation treatment records of 6,000 past and present cancer patients" and "had at their fingertips the ability to alter the radiation treatment levels that each patient received." S. Rep. No. 99-432, 1986 U.S.C.C.A.N. 2479, 2480.

It was this sort of serious, technical, and exploitative behavior—*breaking into* private computer systems for the purpose of accessing or altering non-public information—that Congress sought to outlaw.

B. Consistent With Congress's Intent, Courts Across the Country Have Held that the CFAA Does Not Criminalize Violations of Computer Use Policies.

This legislative context is critical, because the CFAA's text is irresolvably vague. The statute defines the term "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030 (e)(6). It does not, however, define "without authorization" or "with authorization." Congress crafted this language in the early days of the Internet, when today's interconnected world was beyond imagination. At the start of 1986, the total number of networks connected via the Internet was a mere 2,000, and there were a small number of users.[15] Today, every time we log into a bank account, check Facebook, or use a phone app, we access information on a distant server—someone else's computer. In a world where it is difficult to go a single day, or even a single waking hour, without accessing someone else's computer system, the precise meaning of the CFAA "has proven to be elusive." *EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577, 582 n.10 (1st Cir. 2001).

Courts have thus looked to the CFAA's legislative history to provide the "broader context of enactment" and "explain the text's purpose and meaning." *See* 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) (citation and internal quotations omitted). Legislative history "contains the best available evidence of both the context and the circumstances of enactment."[16] And federal courts across the country—including the four most recent federal circuit courts to address the issue,

[15] Computer History Museum, "Internet History 1962 to 1992," http://www.computerhistory.org/internethistory/1980s/.

[16] *See also* John F. Manning, *Textualism as a Nondelegation Doctrine*, 97 COLUM. L. REV. 673, 701 n.119 (1997) (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'": "'The reason for the law is its soul; when the reason for the law changes, the law changes as well.'").

and numerous district courts[17]—have recognized that consistent with the CFAA's "anti-hacking" purpose, the statute must be interpreted to apply narrowly to violations of technical restrictions on access—not written, contractual restrictions on computer use.

The Ninth Circuit, in 2009, first rejected the argument 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. *Brekka*, 581 F.3d at 1135. 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." *Id.* at 1133.

[17] *See Sandvig v. Sessions*, No. CV 16-1368 (JDB), 2018 WL 1568881, at *15 (D.D.C. Mar. 30, 2018); *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1110–12 (N.D. Cal. 2017); *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); *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 932 (E.D. Va. 2010).

Three years later, in 2012, the Ninth Circuit, sitting *en banc*, affirmed a narrow construction of the phrase "exceeds authorized access," rejecting the argument that the bounds of an individual's "authorized access" turned on an employer's written computer use policies. *Nosal I*, 676 F.3d at 857. Congress, the court explained, had a far more narrow purpose: "to punish hacking, the circumvention of technological access barriers[.]" *Id.* at 863. The court held that interpreting the statute to criminalize violations of written computer use policies would "expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer"—like checking the score of a baseball game in contravention of an employment agreement—and "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *Id.* at 859.

The same year, the Fourth Circuit, too, ruled that the statute must be narrowly construed. *WEC Carolina*, 687 F.3d at 206. The court concluded that an individual "accesses a computer 'without authorization' when he gains admission to a computer without approval," and "'exceeds authorized access' when he has approval to access the computer, but uses his access to obtain or alter information that falls *outside the bounds* of his approved access." *Id.* at 204 (emphasis added). The court said it was "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." *Id*. at 207.

In 2015, the Second Circuit adopted the narrow interpretation of "exceeds authorized access." *Valle*, 807 F.3d at 527–28. The case involved a police officer charged under the CFAA for violating the NYPD's computer use policy, which provided that its database "could only be accessed in the course of an officer's official duties." *Id*. at 513. The Second Circuit held that such purpose-based limits are de facto restrictions on use, regardless of the terminology employed. *Id*. at 528. The legislative history, the court said, demonstrated Congress's clear intent to criminalize trespassing into portions of a computer beyond which one's access rights extend—not violations of use policies. *Id.* at 525.

Finally, in 2017, the Fifth Circuit recognized that "a narrow reading" of the statute's access provisions "avoids criminalizing common conduct—like violating contractual terms of service for computer use or using a work computer for personal reasons—that lies beyond the antihacking [sic] purpose of the access statutes." *Thomas*, 877 F.3d at 596. The court quoted Professor Orin Kerr: "If we interpret the phrase 'exceeds authorized access' to include breaches of contract, we create a remarkably broad criminal prohibition that has no connection to the rationales of criminal punishment." Orin S. Kerr, C*ybercrime's Scope:*

Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1663 (2003).[18]

A few circuit courts have gone the other way, broadly interpreting "exceeds authorized access" to include acts of disloyal employees who misuse their access to corporate information. *See Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258, 1263-64 (11th Cir. 2010).[19]

[18] The Fifth Circuit previously held in *United States v. John*, 597 F.3d 263, 271–73 (5th Cir. 2010), that written restrictions are enforceable via the CFAA if they prohibit acts that are criminal (*i.e.*, committing fraud) and if the wrongdoer accesses the computer in furtherance of a crime. In *Thomas*, however, the Fifth Circuit did not cite *John* and instead relied solely on cases narrowly construing the CFAA. It thus appears to have moved away from *John*, toward the prevailing interpretation of the CFAA—at least in cases that do not involve terms of service prohibitions on *express* criminal acts. Unlike in *John*, which involved Citibank's prohibition on accessing customer bank accounts to perpetuate fraud, *id.* at 271, the terms of use restriction at issue here on using unauthorized software—which applies not only to Wget but also unauthorized computer games—is not a prohibition on an *express* criminal act. 18 July 2013 Order, 6.

[19] The First Circuit's decision in *EF Cultural* is routinely cited—including by the courts below—to have adopted the broad interpretation of CFAA. However, while "dicta" in the opinion "can be read to support" the expansive view, its holding is "more narrow[.]" *Wentworth-Douglass Hosp. v. Young & Novis Prof'l Ass'n*, No. 10-CV-120-SM, 2012 WL 2522963, at *3 (D.N.H. June 29, 2012). *EF Cultural* turned on the fact that the defendants provided their agent, the creator of a scraping tool, with "extremely confidential" information—including "proprietary information about the structure of the [plaintiff's] website" and special login codes—which allowed it to access the website using *false credentials*. *EF Cultural,* 274 F.3d at 583 & n. 14. As *Wentworth-Douglass* explained, *EF Cultural* is "better understood as focusing less on whether defendants violated a website's 'use restrictions,' and more on whether, by employing improperly obtained confidential information, defendants gained unauthorized access by circumventing 'access restrictions' to the website's data." 2012 WL 2522963, at *3.

These decisions—which have been explicitly rejected by the more recent opinions[20]—erroneously "wrap the intent of the employees and use of the information into the CFAA despite the fact that the statute narrowly governs access, not use" and fail "to consider the broad consequences of incorporating intent into the definition of 'authorization.'" *Dresser-Rand*, 957 F. Supp. 2d at 619.

C. Courts Adopting the 'Narrow' Interpretation Have Rejected the Lower Courts' Theory that Written Computer Use Restrictions on *How* Someone Accesses Information Are 'Access' Restrictions.

The courts below both purport to issue decisions consistent with the narrow, prevailing, construction of the CFAA.[21] They both conclude, however, that written terms of use dictating the *method* in which someone may access information they are generally authorized to obtain are somehow distinct from other written computer use restrictions and captured under the "narrow" interpretation.[22]

[20] *See Nosal I*, 676 F.3d at 862–63; *WEC Carolina*, 687 F.3d at 206; *Valle*, 807 F.3d at 527–28.

[21] 18 July 2013 Order, 5 (noting that its two earlier decision in this case "found ambiguity in the statute, applied the rule of lenity, and ruled that the Court would instruct in accordance with the narrow interpretation that 'exceeds authorized access' is limited to violations of restrictions on access to information and not restrictions on the use of information"); 31 May 2018 Order, 10–11 ("We need not decide which interpretation, narrow or broad, applies to military courts" because "this was an access violation[.]").

[22] *See, e.g.,* 31 July 2018 Order, 12 ("Had appellant gone through all the individual clicks necessary to access the [State Department] portal, find and download the

First, this holding is inconsistent with the very precedent the lower courts cite. The holding relies on the conclusion that "[r]estrictions on access to classified information are not limited to code based or technical restrictions on access" and "can arise from a variety of sources, to include regulations, user agreements, and command policies." 18 July 2013, 5; *see also* 31 May 2018, 12. But *Nosal I* held that, for "a statute whose general purpose is to punish hacking," liability must turn on "circumvention of technological access barriers"—*i.e.*, code-based restrictions that place limitations on who can and cannot access a system or data. 676 F.3d at 863. As Professor Kerr has explained, the Ninth Circuit "meant 'use restrictions' to refer to *any* written restrictions, as they technically allowed access but imposed terms of use" and "'access restrictions' to mean code-based restrictions, or in [the court's] words, 'technological access barriers.'" Orin Kerr, *The CFAA Meets the "Cannibal Cop" in the Second Circuit—and Maybe Beyond*, Wash. Post: The Volokh Conspiracy (May 13, 2015) (emphasis in original).[23] Reading *Nosal I* to <u>not</u> require circumvention of code-based barriers "reduces [the Ninth Circuit's] opinion to an absurdity" because the key premise of the holding is: "you can't hinge liability" under an anti-hacking statute "on the mere words of

files, and repeat those steps seventy-five times—this would present a different issue.").

[23] *Available at* 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/.

written restrictions." *Id.* Here, the lower courts' interpretation of the CFAA "hinges liability on exactly the basis for which [*Nosal I*] purports to reject hinging liability—the mere words of the written restrictions." *Id.*

Second, the erroneous premise on which the courts below rely—that written restrictions on the *method* in which information may be accessed should be treated differently than other written computer use restrictions—has been flatly rejected by both the Fourth and Ninth Circuits, the only two federal circuit courts to decide the issue.

The Fourth Circuit, in *WEC Carolina*, explicitly held that "Congress has not clearly criminalized obtaining or altering information 'in a manner' that is not authorized. Rather, it has simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter." 687 F.3d at 206. The government raised—and the Fourth Circuit rejected—the very argument the appeals court relied upon below: that Congress intended the word "so" in the definition of "exceeds authorized access"[24] to reach "users whose initial access to information is authorized, but who later use their access to obtain information in an unauthorized manner." *See* 18 July 2013, 11–12. According to the court, "defining 'so' as 'in that manner' only elucidates our earlier conclusion that

[24] *See* 18 U.S.C. § 1030 (e)(6) ("exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter").

'exceeds authorized access' refers to obtaining or altering information beyond the limits of the employee's authorized access." *WEC Carolina*, 687 F.3d at 205. Other courts, too, have explicitly rejected the appeals court's reasoning. *See Sandvig*, 2018 WL 1568881, at *17 ("'so' most naturally refers back to the earlier phrase 'such access,' emphasizing that the accesser must not have been entitled to obtain or alter that particular information through the particular authorization used—even if, theoretically, there were another way in which the accesser might legally obtain or alter the information.").[25]

The Ninth Circuit, in a case involving California and Nevada's state-law CFAA equivalents, held that "taking data using a method prohibited by the

[25] *Nosal I* also addressed the significance of the word "so" in the definition of "exceeds authorized access," in response to the government's argument that the word was intended to mean "in that manner" and capture violations of use restrictions generally. 676 F.3d at 857. The *en banc* Ninth Circuit rejected the government's argument, which it said "places a great deal of weight on a two-letter word that is essentially a conjunction." *Id.* The court stated that Congress could have included the word "as a connector or for emphasis." *Id.* at 858. It also stated that, "assum[ing] [the phrase] must have a substantive meaning to make sense of the statute," Congress could have meant it to cover situations in which someone is authorized to access the information in question, but "circumvents security measures" such as by hacking technical measures blocking information from being downloaded, or bypassing a username and password requirement via someone else's technical credentials rather than the technical credentials they were authorized to use to gain access. *Id.* at 857. The court held that, in any event, the government's interpretation of the word "so" as applying to violations of written computer use restrictions must be rejected: "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." *Id.*

applicable terms of use, when the taking itself generally is permitted," does not render the taking or use "unauthorized." *Oracle*, 879 F.3d at 962. "Oracle obviously disapproved of the method—automated downloading—by which Rimini took Oracle's proprietary information." *Id.* But the key, the court said, "is whether Rimini was authorized in the first instance to take and use the information that it downloaded." *Id.* The fact that Rimini accessed information via automated software that Oracle disallowed was irrelevant to whether it was authorized to access the information in the first place. *Cf. Valle*, 807 F.3d at 523–24 (officer's violation of NYPD's computer use policy, by accessing a database for non-law enforcement purposes, "is irrelevant" to whether he was authorized, via the grant of technical credentials, to access the database).

Other courts, too, have rejected the lower courts' novel theory that violations of terms of use dictating *how* information may be accessed should be treated differently than other written computer use restrictions. In *Sandvig*, for example, the court narrowly interpreted the CFAA to apply only to restrictions "on what information plaintiffs plan to access, not on why they wish to access it, the manner in which they use their authorization to access it, or what they hope to do with it." 2018 WL 1568881, at *15. The court made no distinction between restrictions on the use of automated Web browsing tools, or "scrapers"—a manner/method computer use restriction—and other types of computer use restrictions. "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." *Id.* at *7. The court also noted that interpreting the CFAA to limit the ability of researchers and journalists to make use of technology to access information on the Internet they were otherwise authorized to access would run afoul to the First Amendment, and it narrowly construed the statute to avoid these concerns. *Id.* at *5.

Courts have also rejected attempts to characterize other types of computer use restrictions, such as restrictions on the purpose for which information may be accessed or used, as "access" restrictions. *See, e.g.*, *Valle*, 807 F.3d at 513, 524 (written restriction providing that law enforcement database could only be accessed for "official duties" constituted a computer use restriction, despite being framed in terms of access); *Wentworth-Douglass*, 2012 WL 2522963, at *4 (employer's policy "prohibiting employees from accessing company data for the purpose of copying it to an external storage device is not an 'access' restriction"). As these courts have held, "simply denominating limitations as 'access restrictions' does not convert what is otherwise a use policy into an access restriction." *Id.* at *4.

D. The Military Judge Ignored Basic Rules of Statutory Construction.

The military judge recognized that pursuant to the ‘narrow’ interpretation, violations of written terms of use restrictions do not give rise to CFAA liability but reasoned that because l8 U.S.C. § 1030(a)(l) applies to classified information, the analysis should be different—even though “the definition for ‘exceeds authorized access’ is the same for all of the sections of [the CFAA].” 18 July 2013 Order, 6. According to the court, “access restrictions on classified information can be more stringent than for other information and can include manner of access restrictions[.]” *Id.*

The court’s conclusion is erroneous and inconsistent with the “rule of statutory interpretation” that “identical words used in different parts of the same statute are generally presumed to have the same meaning.” *IBP*, 546 U.S. at 22. In *Nosal I*, the government made the same argument—*i.e.*, that the court could “construe ‘exceeds authorized access’ only” for the subsection at issue and “give the phrase a narrower meaning when [construing] other subsections.” 676 F.3d at 859. But as the Ninth Circuit held, “This is just not so: Once we define the phrase for the purpose of subsection 1030(a)(4), that definition must apply equally to” the *five* other times it appears in the statute—including in subsection 1030(a)(1). *Id.* “Congress provided a single definition of ‘exceeds authorized access’ for all iterations of the statutory phrase" and "obviously" meant the phrase "to have the same meaning throughout section 1030." *Id*.

Here, technological access restrictions may be more stringent for classified information, but what *constitutes* an access restriction versus a use restriction for purposes of the CFAA cannot vary based on the type of information accessed. As in *Nosal I*, the military judge was required to consider how the interpretation it adopted would operate "wherever in the statute the phrase appears." *See id.* Its failure to do so was in error.

There is no question that Appellant possessed technical credentials that generally authorized her to access the information in question. Consistent with the precedent the lower courts cite, violations of computer use restrictions on method of access—or any other written computer use restrictions—do not give rise to CFAA liability. The lower courts' holdings flout both the case law they purport to follow and long-held rules of statutory construction. This Court should correct these errors.

III. The Lower Courts' Broad Reading of the CFAA Renders the Statute Unconstitutionally Vague.

Ensuring that the CFAA remains limited to its original purpose is not merely as a matter of principal; it is essential to ensuring that the statute is not rendered unconstitutionally vague.

Due process requires that criminal statutes provide ample notice of what conduct is prohibited. *Connally v. Gen. Const. Co.*, 269 U.S. 385, 390 (1926). Vague laws that do not "provide explicit standards for those who apply them . . . impermissibly delegate[] basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis." *Grayned v. Rockford,* 408 U.S. 104, 108–09 (1972). A criminal statute that fails to provide fair notice of what is criminal—or threatens arbitrary and discriminatory enforcement—is thus void for vagueness. *Skilling v. United States*, 561 U.S. 358, 412 (2010) (citing *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)).

To avoid fatal vagueness problems, the Rule of Lenity calls for ambiguous criminal statutes to be interpreted narrowly in favor of the defendant. *United States v. Santos*, 553 U.S. 507, 514 (2008). The Rule of Lenity "ensures fair warning by so resolving ambiguity in a criminal statute as to apply [] only to conduct clearly covered." *United States v. Lanier*, 520 U.S. 259, 266 (1997). 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" and does not "unintentionally turn ordinary citizens into criminals." *Nosal I,* 676 F.3d at 863.

Concerns over the CFAA's vague language were at the heart of the Second, Fourth, Fifth, and Ninth Circuits' decisions to adopt narrow interpretations of the statute. These courts recognized that while the CFAA *could* be interpreted to base criminal liability on computer use policies, such an interpretation would violate the Rule of Lenity by conferring on employers or websites the power to outlaw any conduct they wished without the clarity and specificity required of criminal law. *See Nosal I*, 676 F.3d at 860, *WEC Carolina*, 687 F.3d at 205–06; *Thomas*, 877 F.3d at 596; *Valle*, 807 F.3d at 527. "[A]llow[ing] criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read" would create "[s]ignificant notice problems[.]" *Nosal I*, 676 F.3d at 860. It would make it impossible for employees to know what conduct was criminally punishable at any given time. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1586 (2010). It would also enable "private parties to manipulate their computer-use and personnel policies" so as to turn employer-employee or company-consumer relationships—relationships traditionally governed by tort and contract law—into relationships policed by criminal law. *Nosal I,* 676 F.3d at 860. This would grant employers and website operators the power to unilaterally "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id*.

The decisions below specifically create legal uncertainty regarding whether it is a crime to violate computer use restrictions on the method in which people may access information that they are generally authorized to access, such as prohibitions on automated Web browsing tools. Such tools are commonly prohibited in websites' terms of service, but they are used routinely across the Internet, by entities large and small, every day. These tools are critical for gathering information from across the Web, the world's largest and ever-growing data source.

Companies across various industries use automated Web browsing tools to gather data for a wide variety of uses, including: tracking the performance ranking of products in the search results of retailer websites; monitoring competitors' pricing and inventory; keeping tabs on social media to identify issues that require customer support; staying up to date on news stories relevant to their industry; aggregating information to help manage supply chains; detecting fraud; aggregating market data; and collecting images and data for machine learning model training.[26]

Investigative journalists also (increasingly) rely on automated Web browsing to support their work, much of which is protected First Amendment activity; it 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."[27] ProPublica

[26] *See, e.g.,* Import.io, Solutions Overview, https://www.import.io/solutions.

[27] Leanpub, Scraping for Journalists (2nd edition): About the Book (last updated Sep. 11, 2017), https://leanpub.com/scrapingforjournalists.

journalists, for example, uncovered that Amazon's pricing algorithm was hiding the best deals from many of its customers using a "software program that simulated a non-Prime Amazon member" and scrapped data from product pages.[28]

Online discrimination researchers also rely on automated access tools, for audit testing. One recent study of racial discrimination on Airbnb—which found that distinctively African American names were 16 percent less likely to be accepted relative to identical guests with distinctively white names—"sent inquiries to Airbnb hosts using web browser automation tools" and "collected all data using scrapers[.]"[29] 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. Discrimination research has historically proven necessary for ensuring compliance with federal and state anti-discrimination laws.[30] In today's increasingly data-driven world, in order to uncover whether and how any particular website is

[28] Julia Angwin and Surya Mattu, "How We Analyzed Amazon's Shopping Algorithm," *ProPublica* (Sep. 20, 2016), https://www.propublica.org/article/how-we-analyzed-amazons-shopping-algorithm.

[29] Benjamin Edelman, Michael Luca, and Dan Svirsky, *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, 9 American Economic Journal: Applied Economics 1, at 1, 7 (Apr. 2017), available at https://www.aeaweb.org/articles?id=10.1257/app.20160213.

[30] 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).

treating users differently, researchers need to use a variety of techniques—including automated Web browsing tools that many websites ban.

And in the academic research community, 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 scholarly conversations."[31]

Imposing potential CFAA liability for violating terms of service prohibitions on automated access would chill the use of these societally valuable research tools. It would also chill the creation of news or information aggregation tools, including important public safety tools like Google's Crisis Map, which during California's 2017 wildfires was a critical resource for aggregated information about fires, topology, traffic, shelter availability, and resource needs.[32]

[31] Jonathan P. Tennant, *et al*., *The academic, economic and societal impacts of Open Access: an evidence-based review,* F1000Research (2016), https://f1000research.com/articles/5-632/v3.

[32] *See* Google, Crisis Map Help: About Google Crisis Map (2017), https://support.google.com/crisismaps ("Crisis Map collects [authoritative as well as crowd-sourced] information that's normally scattered across the Web and other resources and makes it easily available through a single map.").

Terms of service prohibitions on automated Web browsing are rarely enforced via litigation except against competitors,[33] underscoring how private companies are already abusing the CFAA to selectively enforce their terms of service via the force of criminal law. Indeed, even the computer use restriction against unauthorized software at issue here—which applies to computer games in addition to Wget—is not routinely enforced by the chain of command, let alone prosecuted.[34] This raises not only significant notice concerns, but it also enables prosecutors, employers, and websites to pick and choose which violations of method/manner restrictions, and by whom, "are so morally reprehensible that they should be punished as crimes[.]" *See United States v. Kozminski*, 487 U.S. 931, 949 (1988). By giving employers and websites inherently legislative power, the lower courts have "invit[ed] discriminatory and arbitrary enforcement." *See Nosal I*, 676 F.3d at 862. The Constitution, however, "does not leave us at the mercy of noblesse oblige" by the government. *United States v. Stevens*, 559 U.S. 460, 480 (2010). Rather, it requires that criminal statutes be clear.

[33] *See* Sellars, *supra* note 8, at 19 (the "vast majority" of the 61 opinions in the last 20 years concerning Web scraping "concern claims brought by direct commercial competitors or companies in closely adjacent markets to each other").

[34] *See* 18 July 2013 Order, 6.

The lower courts' expansive interpretation of the CFAA does not meet the Constitution's standards. The Court should grant review to save the statute from being rendered unconstitutionally vague.

CONCLUSION

This Court should grant the petition for review.

Date: August 30, 2018

Respectfully submitted,

/s/ Jamie Williams
Jamie Williams
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
jamie@eff.org

Counsel for *Amici Curiae*
Electronic Frontier Foundation and
National Association of Criminal
Defense Lawyers

CERTIFICATE OF COMPLIANCE WITH RULE 24

This brief complies with the type-volume limitation of Rule 24(c) and Rule 26(f) because:

X This brief contains 6,996 words, no more than one-half the maximum length authorized by Rule 24 for a brief for an appellant/petitioner,

or

__ This brief contains [less than 650] lines of text.

This brief complies with the typeface and style requirements of Rule 37.

/s/ Jamie Williams
Jamie Williams

Counsel for *Amici Curiae*
Electronic Frontier Foundation and
National Association of Criminal
Defense Lawyers

Dated: August 30, 2018

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the unopposed Motion for Leave to File Brief of *Amici Curiae* Electronic Frontier Foundation and National Association of Criminal Defense Lawyers, Brief of Electronic Frontier Foundation and National Association of Criminal Defense Lawyers as *Amici Curiae* in Support of Appellant, and Motion to Appear Pro Hac Vice, transmitted by electronic means with the consent of the counsel for Appellant, Nancy Hollander, nh@fbdlaw.com, and Vincent J. Ward, vjw@fdbdlaw.com, counsel for Appellee, CPT Catharine Parnell, catharine.m.parnell.mil@mail.mil, and the Clerk of the Court, on August 30, 2018.

/s/ Jamie Williams
Jamie Williams
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333

Counsel for *Amici Curiae*
Electronic Frontier Foundation and
National Association of Criminal
Defense Lawyers