No. 19-783

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES,

Respondent.

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

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE IN SUPPORT OF PETITIONER

SHARON BRADFORD FRANKLIN
ROSS SCHULMAN
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE
740 15th Street, NW, Suite 900
Washington, DC 20005
(202) 986-2700

Counsel for New America's Open Technology Institute

ANDREW CROCKER
Counsel of Record
JAMIE WILLIAMS
CAMILLE FISCHER
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Counsel for Amici Curiae

293731

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

Cases

Page

Cited Authorities

Page

Statutes

Legislative Materials

Page

Other Authorities

Page

INTEREST OF AMICI CURIAE[1]

The Electronic Frontier Foundation ("EFF") is a nonprofit civil liberties organization that has worked for nearly 30 years to protect innovation, free expression, and civil liberties in the digital world. EFF, with its over 30,000 active donors, represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age. EFF's interest in this case is in the principled and fair application of computer crime laws generally, and the Computer Fraud and Abuse Act ("CFAA") specifically, to online activities and systems—especially as it impacts Internet users, innovators, and security researchers. EFF has served as counsel or amicus curiae in numerous cases addressing the CFAA and/or state computer crime statutes. *See, e.g., hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019) (amicus); *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016) ("*Nosal II*") (amicus); *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016) (amicus); *United States v. Valle*, 807 F.3d 508 (2nd Cir. 2015) (amicus); *United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (co-counsel); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) ("*Nosal I*") (amicus); *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (amicus).

The Center for Democracy & Technology ("CDT") is a nonprofit public interest group that seeks to put democracy

1. Pursuant to Supreme Court Rule 37.2(a), all parties have been given the required notice and have provided their consent to the filing of this brief. Pursuant to Rule 37.6, amici state that no counsel for a party authored this brief in whole or in part, and no person or entity, other than amici, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief.

and individual rights at the center of the digital revolution. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of internet users and represents the public's interest in maintaining an open internet. In furtherance of this mission, CDT supports the clear and predictable application of cybercrime statutes including the Computer Fraud and Abuse Act ("CFAA"). CDT detailed how conflicting interpretations of the CFAA are deleterious to the necessary and important work of security researchers in its report, *Taking the Pulse of Security Research* (2018).[2] CDT has filed in other cases related to the application of the CFAA including *United States v. Manning*, No. 20130739 (Army Ct. Crim. App. 2018) (amicus), *United States v. Valle*, 807 F.3d 508 (2nd Cir. 2015) (amicus), and *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (amicus).

New America's Open Technology Institute ("OTI") works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. New America is a Washington, DC-based think tank and civic enterprise committed to renewing American politics, prosperity, and purpose in the Digital Age. OTI works to ensure that the internet remains an open and secure forum for expression and communication. This includes opposing the criminalization of routine online activities and speech.

---

2. Joseph Lorenzo Hall & Stan Adams, *Taking the Pulse of Hacking: A Risk Basis For Security Researchers*, Center for Democracy & Technology (March 2018), https://cdt.org/wp-content/uploads/2018/04/2018-03-27-Risk-Basis-for-Security-Research-FNL.pdf.

INTRODUCTION AND SUMMARY OF ARGUMENT[3]

Passed in 1986 to target serious computer crimes, the Computer Fraud and Abuse Act is now "one of the most far-reaching criminal laws in the United States Code."[4] As the CFAA has been increasingly invoked in both criminal and civil proceedings over the last fifteen years,[5] courts have become split on key questions of the statute's scope. The disagreement between the courts has translated into widespread public confusion—the very outcome that the Rule of Lenity is supposed to prevent. *United States v. Santos*, 553 U.S. 507, 514 (2008). It has also chilled important security research and investigations of discriminatory practices online.

Much of the confusion lies in the fact that today's interconnected world was beyond Congress' imagination when it passed the CFAA. At that time, the invention and popularization of the World Wide Web was still several years away, and most Americans had never connected to the Internet.[6] Congress could not have foreseen that by

---

3. Except where noted, all cited websites were last visited on January 15, 2020.

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

5. Jonathan Mayer, *Cybercrime Litigation,* 164 U. Penn. L. Rev 1453, 1472–1476 (2016) (documenting the surge in both civil and criminal CFAA litigation in the last fifteen years).

6. *World Wide Web Timeline*, Pew Research Center (March 11, 2014), https://www.pewresearch.org/internet/2014/03/11/world-wide-web-timeline.

2020, it would be difficult to go a single waking hour, let alone a single day, without using the Internet and thereby connecting to someone else's computer system.[7]

Perhaps unsurprisingly, then, the CFAA is a vague and ill-defined statute, with uncertain application to the modern Internet. The CFAA does not define even its most critical terms—"access" and "authorization"—and in applying this unclear statute to today's world, some courts have diverged wildly from Congress' intent to stop serious computer break-ins. These courts—including the Eleventh Circuit in its decision below—have adopted a formulation for assessing whether someone "exceeds authorized access" to a computer under the CFAA that turns on the computer owner's unilateral policies regarding use of its networks. *See United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019). This formulation dangerously broadens the CFAA's scope and transforms it into an all-purpose mechanism for policing objectionable or simply undesirable behavior. But other courts—including the Second, Fourth, and Ninth Circuits—have recognized that such a formulation loses sight of the CFAA's intended purpose of prohibiting breaking into computers in order to access or alter information. *See Valle*, 807 F.3d at 527–28; *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012); *Nosal I*, 676 F.3d at 854.

---

7. Andrew Perrin & Madhu Kumar, *About three-in-ten U.S. adults say they are 'almost constantly' online*, Pew Research Center (July 25, 2019), https://www.pewresearch.org/fact-tank/2019/07/25/americans-going-online-almost-constantly (more than 70% of Americans go online at least several times a day).

Given "the important constitutional issues presented and the conflicting results reached" in CFAA cases, the Court should grant certiorari and resolve this confusion. *See Heffron v. International Society for Krishna Consciousness*, 452 U.S. 640, 646 (1981).

ARGUMENT

I. The Court Should Grant Certiorari to Ensure That the CFAA Functions As Congress Intended.

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[.]" 18 U.S.C. § 1030(a)(2)(C).[8] Although the statute defines "exceeds authorized access" as "to access a computer with authorization and to use such

8. The term "protected computer" has been interpreted—following multiple statutory revisions—to include any computer connected to the Internet. *Valle*, 807 F.3d at 528. The first incarnation of the computer crime statute—enacted in 1984—was a narrower one, intended to criminalize unauthorized access to computers to obtain national security secrets, to obtain personal financial and consumer credit information, and to hack into government computers. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190, codified at 18 U.S.C. § 1030(a)(1)–(3). After multiple revisions, the definition now includes not just computers "used in interstate or foreign commerce or communication," but computers "used in *or affecting* interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2) (West 2000 & Supp. 2009) (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 (2010).

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 define either "with authorization" or "without authorization." Indeed, "the meaning of the term 'without authorization' in the CFAA 'has proven to be elusive[.]'" *Nosal II*, 844 F.3d at 1053 (citing *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001)).

Mr. Van Buren, a police officer in Cumming, Georgia, was convicted under subsection (a)(2)(C) of "exceed[ing] authorized access" to the Georgia Crime Information Center ("GCIC") database because he accessed information he was otherwise entitled to access, but for a purpose not permitted by the written use policy governing the database.[9] As the Eleventh Circuit acknowledged below, Mr. Van Buren's conviction rested on an interpretation of the statute that other circuits have rejected because it "allows employers or other parties to legislate what counts as criminal behavior through their internal policies or their terms of use." *Van Buren*, 940 F.3d at 1208.

Determining the scope of these provisions of the CFAA is therefore essential, not only to resolve a deep split of authority among the federal circuit courts, but also to ensure that the CFAA functions as intended and does not become an all-purpose Internet policing statute.

---

9. Violation of Section 1030(a)(2)(C) is a misdemeanor unless it is committed under aggravating circumstances. *See* 18 U.S.C. § 1030(c)(2). Mr. Van Buren was convicted of a felony because the jury found his violation of Section 1030(a)(2)(C) was done for the purposes of private financial gain.

A. The CFAA Was Meant to Target Computer Break-Ins.

The CFAA's historical and statutory context establishes that Congress sought to "prevent intentional intrusion onto someone else's computer—specifically, computer hacking." *hiQ Labs*, 938 F.3d at 1000. Congress passed a precursor computer crime bill to the CFAA in 1984 "to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data." *Valle*, 807 F.3d at 525 (citing H.R. Rep. No. 98–894, 1984 U.S.C.C.A.N. 3689, 3691–92, 3695–97 (1984); S. Rep. No. 99–432, 1986 U.S.C.C.A.N. 2479, 2480 (1986)). After a "flurry of electronic trespassing incidents," lawmakers were concerned about nightmare scenarios such as depicted in the film *WarGames,* where a teenaged hacker played by Matthew Broderick breaks into a U.S. military supercomputer and unwittingly nearly starts a nuclear war. The 1984 House Committee Report (incorrectly) stated that the film was 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).

As a result, Congress passed the 1984 precursor to the CFAA to target serious and 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). 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 Congress intended to prohibit, 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.

Two years later, the 1986 CFAA was passed to extend the prohibition on unauthorized access to any "protected computer" under section 1030(a)(2)(C). Yet, again, Congress characterized its intent as prohibiting computer break-ins. *Valle*, 807 F.3d at 525. As another example of the conduct targeted by this broadened language, the 1986 Senate Committee Report 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 thus "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 technical, exploitative behavior—breaking into a computer system for the purpose of accessing or altering non-public information—that Congress sought to outlaw. It did not intend the CFAA to

be applied so broadly as to cover every crime involving a computer. *Id.* at 2482.

B. Several Appellate Courts Correctly Interpret the CFAA Narrowly, But Others—Including the Eleventh Circuit—Have Transformed the Statute into an All-Purpose Internet-Policing Mechanism.

Limiting the CFAA to the purpose Congress intended—breaking into computers—is critical to ensuring that the statute does not become an all-purpose mechanism to police objectionable behavior on the Internet and make it criminal. Yet, the statute's undefined and vague language has caused much confusion in the lower courts and has led some—including the Eleventh Circuit below—to stray far from Congress' intended purpose.

Indeed, no question of CFAA interpretation has more deeply divided the appellate courts than the one at issue here: whether the statute's prohibition on "exceed[ing] authorized access" applies to defendants like Mr. Van Buren who have authorization to access data but do so for a purpose that violates a contractual terms of service or computer use policy, such as the one that limited Mr. Van Buren's use of the GCIC database to "law enforcement purposes." *Van Buren*, 940 F.3d at 1208.

As the Second Circuit has observed, the statutory definition of "exceeds authorized access" does not provide a clear answer to this question. Using authorized access to "obtain or alter information in the computer that the accessor is not entitled so to obtain or alter" could narrowly "refer to the *particular files or databases* in the computer

to which one's authorization extends," or construed much more broadly, it could refer "to the *purposes* for which one is authorized to access a computer." *Valle*, 807 F.3d at 524. In other words, the narrower interpretation turns on whether a defendant accessed "unauthorized data or files—what is colloquially known as 'hacking,'" while the broad interpretation applies to someone who has "unrestricted physical access to a computer" but is "limited in the use" of information he can access by a written policy. *Nosal I*, 676 F.3d at 856–57.

Amici agree with Mr. Van Buren that the most natural interpretation of the CFAA language, which is also consistent with Congress's purpose in passing the law, is the narrow one, under which mere violations of written terms of services or computer usage policies *do not* constitute "exceed[ing] authorized access." *See Valle*, 807 F.3d at 526-27; Pet. for cert. at 16.

It is also the trend among courts to consider the issue. At least three circuit courts—as well as numerous district courts[10]—have adopted this narrow construction to ensure

10. *See, e.g.*, *Sandvig v. Sessions*, 315 F. Supp. 3d 1, 24 (D.D.C. 2018); *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1110–12 (N.D. Cal. 2017); *Lane v. Brocq*, 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.

consistency with the statute's "anti-hacking" purpose and avoid an interpretation that would criminalize common, online innocuous behavior.

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.

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, according to the Ninth Circuit, had a different 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

---

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).

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.

That same year, the Fourth Circuit also 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 case was brought by a welding company against two employees for violating the company's policy against using its confidential or trade secret information without authorization or downloading it to a personal computer. *Id.* at 202. The policy did not, however, restrict the defendants' authorization to access the information. *Id.* The Fourth Circuit 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, too, adopted a narrow interpretation of the phrase "exceeds authorized access." *Valle*, 807 F.3d at 527–28. In the case, a police officer was 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. Although the policy was phrased in terms of "access," the Second Circuit reversed, recognizing that such purpose-based limits are de facto restrictions on use. *Id.* at 528. And according to the court, the legislative history demonstrated Congress's clear intent to criminalize trespassing into portions of a computer beyond which one's access rights extend—not violations of computer use policies. *Id.* at 525.

However, other courts have adopted broader constructions that stray beyond the statute's intended scope. *See, e.g., United States v. Rodriguez*, 628 F.3d 1258, 1263–64 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 272–73 (5th Cir. 2010);[11] *Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006); *EF Cultural Travel*, 274 F.3d at 582–84. And in this case, although the Eleventh

11. In *John*, the Fifth Circuit adopted what might be termed a "middle-of the-road" interpretation, holding that written restrictions on "access" are enforceable via the CFAA only if they prohibit criminal acts (such as fraud), and the wrongdoer accesses the computer in furtherance of the criminal act. 597 F.3d at 271–73. However, in *United States v. Thomas*, 877 F.3d 591 (5th Cir. 2017), a case construing the CFAA's unauthorized "damage" provision, 18 U.S.C. § 1030(a)(5)(A), a panel of the Fifth Circuit acknowledged 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 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." *Id. (*citing Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1663 (2003)).

Circuit acknowledged the deep split of authority on this issue and criticisms of the broad interpretation, the panel determined it was bound to adhere to its earlier ruling in *Rodriguez*. *Van Buren*, 940 F.3d at 1208.

In *Rodriguez*, the court held that a Social Security Administration employee exceeded his authorized access in accessing databases for personal reasons in violation of the agency's policies. 628 F.3d at 1260. The court reasoned, without elaboration, that the defendant violated the "plain" language of the statute when he accessed information in the database "for a nonbusiness reason." *Id.* at 1263.

But as the split of authority on this question demonstrates, the CFAA's language is anything but "plain." Moreover, the construction adopted by the Eleventh Circuit "look[s] only at the culpable behavior of the defendants before them, and fail[s] to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of 'exceeds authorized access.'" *Nosal,* 676 F.3d at 863; *Valle*, 807 F.3d at 527. *See* Section II, *infra.*

This Court should grant certiorari to correct the error of the Eleventh Circuit below, resolve widespread confusion about the reach of the statute, and ensure that lower courts apply the CFAA to further Congress's intended purpose: targeting computer break ins.

II. The Court Should Grant Certiorari to Ensure That the CFAA Is Not Rendered Unconstitutionally Vague.

Ensuring that the CFAA remains limited to its original purpose is not important merely as a matter of

principle; 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. *Santos*, 553 U.S. at 514. 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. We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals." *Nosal I*, 676 F.3d at 863.

The competing interpretations of the CFAA outlined above demonstrate that the statutory language is ambiguous and should thus, consistent with the Rule of Lenity, be interpreted narrowly. Indeed, vagueness concerns were at the heart of the decisions by courts adopting a narrow interpretation of the statute. These

courts recognized that while the CFAA *could* be interpreted to base criminal liability on policies instituted by an employer, such an interpretation would violate the Rule of Lenity by conferring on employers the power to outlaw any conduct they wish without the clarity and specificity required of criminal law. *See Valle*, 807 F.3d at 527; *WEC Carolina*, 687 F.3d at 205–06; *Nosal I*, 676 F.3d at 860; *cf. Sandvig*, 315 F. Supp. 3d at 25 (narrowly interpreting the CFAA to avoid running afoul of the First Amendment, in light of terms of service restrictions "that purport to prohibit the purposes for which one accesses a website or the uses to which one can put information obtained there . . . threaten[ing] to burden a great deal of expressive activity").

Specifically, "'allow[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. Indeed, attaching criminal punishment to breaches of vague, boilerplate policies[12]—which companies typically reserve the right to modify at any time[13]—would make

12. One sample Internet and email usage policy, for example, warns that "Internet use on company time or using company-owned devices that are connected to the company network is authorized to conduct Company business only," and "[o]nly people appropriately authorized, for company purposes, may use the Internet[.]" Susan M. Heathfield, Internet and Email Policy (Nov. 22, 2019), http://humanresources.about.com/od/policiesandsamples1/a/email_policy.htm.

13. *See, e.g.*, hrVillage, *Employee Handbook Template*, http://www.hrvillage.com/downloads/Employee-Handbook Template.pdf ("The policies stated in this handbook are subject to change at any time at the sole discretion of the Company."); Dartmouth

it impossible for employees to know what conduct is criminally punishable at any given time. It would 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 ones policed by the 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.* Corporations already knowingly wield this power in jurisdictions that have broadly interpreted the CFAA. As the Seventh Circuit noted in one case, an employee of a corporate plaintiff advised in an internal email that the company "could make screen-scraping or web-harvesting illegal with a 'simple disclaimer that states the information can't be scraped from the image.'" *Fidlar Techs. v. LPS Real Estate Data Sols., Inc.*, 810 F.3d 1075, 1082 (7th Cir. 2016).

The Eleventh Circuit's decisions below in this case and *Rodriguez* create legal uncertainty regarding whether it is a crime to violate terms of service prohibitions on usage of a computer. Under the court's reasoning, nearly anyone who violates a written computer use policy—whether a website's terms of service or an employer or school acceptable use policy, commits a potential criminal offense. Indeed, while the statute permits a private party to bring a civil suit only when the party has suffered a loss

---

College, *Employment Policies and Procedures Manual*, http://www.dartmouth.edu/~hrs/policy ("The policies are intended as guidelines only, and they may be modified, supplemented, or revoked at any time at the College's discretion.").

of at least $5,000 during a one-year period, a prosecutor need not meet any monetary threshold for damages or loss; a single act of "unauthorized access" would be enough.[14]

Moreover, the Eleventh Circuit's rule could transform millions of people into criminals because users routinely violate computer use policies in the course of their employment or as a part of their daily lives. For instance, Walmart, which is simultaneously one of the largest employers and retailers in the U.S., states that it is a violation of the company's Wi-Fi use policy for any guest or employee to send, receive, access, or use any communication or material while connected to their Wi-Fi network that may be considered "harmful, obscene, pornographic, indecent, lewd, violent, abusive, profane, insulting, threatening, tortuous, harassing, hateful or otherwise harmful."[15] Thus, a shopper who connects to in-store Wi-Fi and views certain products for sale on Walmart's own website violates the terms of service and is potentially guilty of a federal crime.[16]

Meanwhile, the U.S. Department of the Interior prohibits all employees—including over 2 million National Park Service volunteers—from "[a]ny type of continuous

14. *See* 18 U.S.C. §§ 1030(c)(4)(A)(i) (I), (g).

15. Walmart, *Wi-Fi Terms of Use*, https://corporate.walmart.com/privacy-security/wi-fi-terms-of-use.

16. *See* Chris Morris, *Walmart Was Once Again Forced to Pull an Offensive Shirt From Its Website*, Fortune (July 12, 2018), https://fortune.com/2018/07/12/walmart-sauce-hockey-offensive-shirt-amazon (describing multiple incidents in which clothing available on Walmart.com from third-party sellers displayed racist, sexist, and other objectionable material).

audio or video streaming from commercial, private, news, [or] financial organizations" on a government issued device or while connected to a government network.[17] And the U.S. Postal Service states that employees can use government devices for personal purposes only to the extent that they make "minimal" use of Postal Service resources, such as sending a brief email that is limited to text, but does not include images or links.[18] Employees of these agencies who access CNN or C-SPAN at work to view a presidential news conference or a congressional hearing are arguably in violation of these policies and, under a broad reading of the CFAA, in criminal jeopardy.

By subjecting an untold number of Internet users to potential prosecution, the Eleventh Circuit's expansive interpretation of the CFAA enables prosecutors to pick and choose which types of terms of service violations "are so morally reprehensible that they should be punished as crimes[.]" *See United States v. Kozminski*, 487 U.S. 931, 949 (1988). By giving that inherently legislative power to prosecutors, the panel has "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.

---

17. U.S. Dept. of the Interior, *Use of Government Property*, https://www.doi.gov/ethics/use-of-government-property.

18. U.S. Postal Service, *Personal Use of Government Office Equipment Including Information Technology*, https://about.usps.com/handbooks/as805/as805c5_002.htm.

The expansive interpretation of the CFAA adopted by the Eleventh Circuit and other courts does not meet the Constitution's standards. The Court should grant certiorari to correct their interpretation and thereby save the statute from being rendered unconstitutionally vague.

III. The Court Should Grant Certiorari to Prevent Chilling of Valuable Research and Journalism, Including Audit Testing for Online Discrimination.

The Eleventh Circuit's broad reading of the CFAA also threatens to chill socially valuable research, journalism, and online testing, much of which is protected First Amendment activity. This includes not only computer security research, but also audit testing for online discrimination. It could also criminalize—and therefore will undoubtedly chill[19]—a specific form of online activity that is critically important to holding companies accountable: the investigative techniques employed by journalists and academic researchers to uncover online discrimination.

---

19. The uncertainty created via courts' overbroad interpretation of the CFAA has already proven to chill the work of computer security researchers. *See* Letter from Computer Security Experts to Congress and Members of the Senate and House Committees on the Judiciary (Aug. 1, 2013), https://www.eff.org/document/letter-def-con-cfaa-reform ("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.").

The investigative techniques of these journalists and academic researchers sometimes require violating specific company prohibitions on certain activities, and are often adversarial to a company's business interests. Nonetheless, the panel's broad interpretation could render it criminal for a researcher or journalist to access a website or gather information from that website where it is clear that the company has prohibited access by researchers for research purposes.

The chill imposed on researchers and journalists is of particular concern when it comes to ensuring compliance with federal and state anti-discrimination laws. 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 ("FHA") and Title VII's prohibition on employment discrimination. *Cf. Havens Realty Corp v. Coleman*, 455 U.S. 363, 373 (1982).

Online, there is growing evidence 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.[20] In order to uncover whether any particular website is treating users differently, researchers need to use a variety of techniques, such as creating test accounts that vary on the basis of race or gender and comparing the job advertising or housing offers that are displayed to,

20. *See*, e.g., Executive Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* (May 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

say, male versus female users. In this case, researchers may need to access the accounts of actual users to compare housing or job offers that are given to people of different genders or races. Such techniques are often adversarial to a company's interests. Pursuant to the Eleventh Circuit's opinion below, if a company disagrees with the purpose of a researcher's access to its website, it can not only seek to bar such research but can actually render that research criminal by merely stating in terms of use or by letter that researchers are not authorized to access its website.[21] Websites could therefore rely on the criminal justice system to shut down any unwanted anti-discrimination research or testing, even where the researcher did not break into a computer. Under a broad interpretation, the company's choice to prohibit such research could be enforceable as a criminal CFAA violation. As a result, many researchers and journalists will likely refrain from conducting their socially valuable and constitutionally protected research to avoid the threat of criminal prosecution. The Court should grant certiorari to prevent this result.

21. *See*, e.g., Knight First Amendment Institute, *Knight Institute Calls on Facebook to Lift Restrictions on Digital Journalism and Research* (Aug. 7, 2018), https://knightcolumbia.org/content/knight-institute-calls-facebook-lift-restrictions-digital-journalism-and-research.

CONCLUSION

The Court should grant the petition for writ of certiorari.

Dated: January 16, 2020

Sharon Bradford Franklin
Ross Schulman
New America's Open Technology Institute
740 15th Street, NW, Suite 900
Washington, DC 20005
(202) 986-2700

Counsel for New America's Open Technology Institute

Respectfully submitted,

Andrew Crocker
Counsel of Record
Jamie Williams
Camille Fischer
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Counsel for Amici Curiae