No. 16-1344

IN THE

Supreme Court of the United States

DAVID NOSAL,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PETITIONER

JAMIE WILLIAMS
Counsel of Record
CINDY COHN
ANDREW CROCKER
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
jamie@eff.org

Counsel for Amicus Curiae

273416

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

CASES

Cited Authorities

Cited Authorities

Page

Page

Page

STATUTES

OTHER AUTHORITIES

Cited Authorities

Page

Page

LEGISLATIVE AUTHORITIES

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the digital world. With over 36,000 active donors and dues-paying members, EFF 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 key cases addressing the CFAA and/or state computer crime statutes, including in this case when it was initially before the Ninth Circuit. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) ("*Nosal I*") (en banc) (amicus); *see also Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016) (amicus); *State v. Nascimento*, 379 P.3d 484 (Or. 2016) (interpreting Oregon's computer crime statute, Or. Rev. Stat. § 164.377(4)) (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. Cioni*, 649 F.3d 276 (4th Cir. 2011) (amicus), *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (amicus).

---

1. Pursuant to Supreme Court Rule 37.2(a), *Amicus* has provided timely notice to all counsel, and all parties consent to the filing of this brief. Pursuant to Supreme Court Rule 37.6, *Amicus* states that this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than *Amicus* or their counsel made a monetary contribution to fund the preparation or filing of this brief.

INTRODUCTION

Today's world is an interconnected one. It is difficult to go a single day without connecting to someone else's computer system. It's possible to check your email—and thus access information on a distant server—from a remote campsite, at 30,000 feet above sea level or deep underwater, and even from low Earth orbit.[2]

This world was beyond Congress's imagination when it passed the Computer Fraud and Abuse Act ("CFAA") in 1986. At the start of that year, the total number of networks connected via the Internet was a mere 2,000.[3] Within thirty years, we had exhausted the pool of over 4.2 *billion* possible distinct "IP addresses" using the 32-bit version of the Internet Protocol and are now in the course of switching to a 128-bit version.[4] Perhaps unsurprisingly, Congress's attempt to take on computer breaks-ins so early in the Internet's lifecycle resulted in an ill-defined statute. The CFAA fails to define even its most critical term: what it means to access a computer "without authorization."

---

2. Adrienne LaFrance, "The Internet in Space? Slow as Dial Up," *The Atlantic* (June 11, 2015), https://www.theatlantic.com/technology/archive/2015/06/the-internet-in-space-slow-dial-up-lasers-satellites/395618/.

3. Computer History Museum, "Internet History 1962 to 1992," http://www.computerhistory.org/internethistory/1980s/ (last viewed May 24, 2017).

4. Wikipedia, "IPv4 Exhaustion" (May 3, 2017), https://en.wikipedia.org/wiki/IPv4_address_exhaustion.

In the course of applying this ill-defined statute to today's world, some courts have diverged from Congress's intent and transformed the CFAA into an all-purpose mechanism for policing objectionable online behavior. These courts—including the Ninth Circuit in the decision below—have adopted formulations for assessing whether someone accessed a computer "without authorization" that look to the computer owner's expectations, preferences, and policies regarding use of their networks, rather than whether there was actually any technological intrusion. *See United States v. Nosal*, No. 14-10037, 844 F.3d 1024, 1038–39 (9th Cir. July 5, 2016) ("*Nosal II*").

Other courts—the Second Circuit and Fourth Circuit—have recognized that such a formulation loses sight of the CFAA's intended purpose: prohibiting breaking into computers in order to access or alter information. *See United States v. Valle*, 807 F.3d 508, 527–28 (2nd Cir. 2015); *WEC Carolina Energy v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012).

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). This confusion has lead not only to uncertainty and frustration—such as that felt by someone who needs to log into a sick spouse's account but is unsure if their actions could give rise to federal criminal liability—but it has also chilled important security research and investigations of discriminatory practices online. 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). The Court should make clear that the CFAA must be limited to its original purpose of targeting computer break-ins—not only to stay true to Congress's intent, but to save the statute from becoming an unconstitutionally vague criminal law used to police the Internet and enforce corporate computer use policies.

ARGUMENT

I. THE COURT SHOULD GRANT CERTIORARI TO ENSURE THAT THE CFAA FUNCTIONS AS CONGRESS INTENDED.

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

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).[5] 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.[6]

---

5. The specific CFAA section Nosal was charged with was 18 U.S.C. § 1030(a)(4), which requires an intent to defraud, but the interpretation of "without authorization" must apply equally to the statute's various subsections "pursuant to the 'standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be given the same meaning.'" *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) ("*Nosal I*") (en banc) (quoting *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007)).

6. The first incarnation of the computer crime statute—enacted in 1984—was a narrow statute intended to criminalize

Congress passed the law "to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data." *Id.* 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)). 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."[7] *Id.* The House Committee Report to the original computer

---

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 merely 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) (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). According to Professor Kerr, the CFAA has an even broader reach than the Second Circuit acknowledged. He argues 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." *Id.* at 1570–71.

7. Similarly, the Senate Committee Report to the bill's 1986 amendments "specifically described 'exceeds authorized access' in terms of trespassing into computer systems or files." *Valle*, 807 F.3d at 525 (S. Rep. No. 99–432, 1986 U.S.C.C.A.N. 2479, at 2483).

crime bill,[8] for example, explained that "the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense." H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3706 (1984). As an example of what Congress intended to target, the Report described an individual who "stole confidential software" from a previous employer "by tapping into the computer system of [the] previous employer from [a] remote terminal." *Id.* at 3691–92. 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. *Id.* at 3692.

The Report called on a statutory solution to ensure that such computer break-ins would not evade prosecution. It referred to a "recent flurry of electronic trespassing incidents" and described "so-called 'hackers'" who had been able to "access (trespass into) both private and public computer systems, sometimes with potentially serious results" thanks to the "proliferation of computer networking[.]" *Id.* at 3695, 3696. The Report (incorrectly) characterized the 1983 techno-thriller film *WarGames*—in which a young Matthew Broderick breaks into a U.S. military supercomputer programmed to predict possible outcomes of nuclear war and unwittingly almost starts World War III[9]—as "a realistic representation of the automatic dialing and access capabilities of the personal computer." *Id.* at 3696. It was this sort of serious

8. *See* Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190, codified at 18 U.S.C. § 1030(a)(1)–(3).

9. Wikipedia, "WarGames" (May 14, 2017), https://en.wikipedia.org/wiki/WarGames.

technological intrusion—breaking into a computer system for the purpose of accessing or altering information—that Congress sought to outlaw.

B. Some Courts—Including the Ninth Circuit Below—Have Diverged From Congress's Intent and Transformed the Statute Into an All-Purpose Mechanism for Policing Objectionable Behavior Using a Computer.

Containing the CFAA to the purpose Congress intended—breaking into computers—is critical to ensuring that the statute does not become an all-purpose Internet policing mechanism. Yet, the statute's undefined and vague language has caused much confusion in the lower courts and has lead some courts—including the Ninth Circuit below—to stray far from Congress's intent. While the statute defines "exceeds authorized access,"[10] it does not define either "authorization" or "without authorization"—terms essential for determining whether the statute has been violated. And "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)).

Both the Second Circuit and Fourth Circuit have narrowly interpreted the CFAA to ensure that the statute remains consistent with Congress's intent and to thereby

10. 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 accessor is not entitled so to obtain or alter[.]" 18 U.S.C. § 1030(e)(6).

avoid an interpretation that would criminalize common, innocuous online behavior. In *Valle*, the Second Circuit held that a narrow interpretation was "consistent with the statute's principal purpose of addressing the problem of hacking, *i.e.*, trespass into computer systems or data." 807 F.3d at 526. In *WEC Carolina*, the Fourth Circuit put it more bluntly: "[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." 687 F.3d at 207. The courts in both cases—along with various other district courts[11]—

11. *See, e.g.*, *Cloudpath Networks, Inc. v. SecureW2 B.V.*, 157 F. Supp. 3d 961, 2016 WL 153127, at *17 (D. Colo. Jan. 13, 2016); *Lane v. Brocq*, 2016 WL 1271051, at *10 (N.D. Ill., March 28, 2016); *Experian Marketing Solutions, Inc. v. Lehman*, 2015 WL 5714541, at *5 (W.D. Mich. Sept. 29, 2015); *Giles Const., LLC v. Tooele Inventory Solution, Inc.*, 2015 WL 3755863, at *3 (D. Utah Jun. 16, 2015); *Enhanced Recovery Co., LLC v. Frady*, 2015 WL 1470852, at *6–*7 (M.D. Fla. Mar. 31, 2015); *Cranel Inc. v. Pro Image Consultants Group, LLC*, 57 F. Supp. 3d 838, 845–46 (S.D. Ohio 2014); *Advanced Fluid Systems, 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 Equipment Maintenance, Inc. v. AIRCO Power Services, Inc.*, 953 F. Supp. 2d 1290, 1295 (S.D. Ga. 2013); *Lewis-Burke Associates, LLC v. Widder*, 725 F. Supp. 2d 187, 194 (D.D.C. 2010); *Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010); *Clarity Servs., Inc. v. Barney*, 698 F. Supp. 2d 1309, 1315 (M.D. Fla. 2010); *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 615 (M.D. Tenn. 2010); *Nat'l City Bank, N.A. v. Republic Mortgage Home Loans*, 2010 WL 959925, at *3 (W.D. Wash. Mar. 12, 2010); *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929, 934 (W.D. Tenn. 2008); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008); *Diamond Power Int'l., Inc. v. Davidson*, 540

held that violations of computer use agreements (often called "terms of service" or "terms of use") cannot trigger CFAA liability. Both courts understood that basing CFAA liability on whether someone uses a computer contrary to the computer owner's interests, preferences, or policies would be unworkable; to do so would criminalize innocuous activities like checking the score of a sporting event on a work computer in violation of an employer's computer use restriction. *See WEC Carolina,* 687 F.3d at 206 ("[W]e do not think Congress intended . . . the imposition of criminal penalties for such a frolic."); *Valle*, 807 F.3d at 527 (noting that such far-reaching, unintended effects are "the very concern at the heart of the rule of lenity").

But other circuits have broadly interpreted "without authorization" and "exceeds authorized access" to include acts of disloyal employees who misuse their access to corporate information, in contravention of the employer's—*i.e.*, the computer owner's—preferences, expectations, or polices. *See, e.g., EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582–84 (1st Cir. 2001); *United States v. John*, 597 F.3d 263, 272–73 (5th Cir. 2010); *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). Unlike the Second and Fourth Circuit, these courts failed to recognize the harm in basing federal criminal liability on corporate computer use policies.

F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005).

The Ninth Circuit, in its decision below,[12] joined this latter set of courts that consider violations of a computer owner's preferences, expectations, and policies relevant for determining whether an individual has accessed a computer "without authorization." The question presented was whether Nosal's associate, Becky Christian,[13] violated the CFAA when she accessed Korn/Ferry's corporate database with the legitimate login credentials of a current Korn/Ferry employee, "FH," who had voluntarily and consensually provided access to Christian and Nosal. Christian and Nosal were both former Korn/Ferry employees whose own credentials had been revoked when they left the company.

Rather than look at whether Christian's access to Korn/Ferry's database entailed a technological break-in of a computer, the Ninth Circuit instead looked implicitly to Korn/Ferry's corporate policy, which prohibits such password sharing. Pursuant to Korn/Ferry's policy, anyone accessing any Korn/Ferry system or information

12. This decision represents a sea change in Ninth Circuit CFAA law. Prior to this case, the court appeared to have adopted a position that violations of corporate computer use policies and preferences could not give rise to CFAA liability. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009) (rejecting 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"); *Nosal I*, 676 F.3d at 863–64 (holding that "'exceeds authorized access' in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its use"). As explained below, the Ninth Circuit's decision below usurps that precedent.

13. Petitioner David Nosal was charged under the CFAA as an accomplice, liable for the actions of Christian and another former Korn/Ferry employee. *See Nosal II*, 844 F.3d at 1029, n.1.

needs "specific authority." The majority held that under the CFAA, only Korn/Ferry—and not an employee with company-authorized login credentials—could provide an individual with "authorization" to access its computers. It reasoned that "[i]mplicit in the definition of authorization is the notion that" a single entity—the computer owner—"can grant or revoke that permission." *Nosal II*, 844 F.3d at 1035. The majority held that the authorization granted by FH therefore simply did not count for purposes of the CFAA: "Nosal had 'no possible source of authorization' since the company revoked his authorization and, while FH might have been wrangled into giving out her password, she and the others knew that she had no authority to control system access." *Id.* at 1035, n.7. 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.

But there is a fatal flaw in the majority's reasoning: 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 a computer. *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."). Neither the statute, nor any dictionary definition, specifies or limits who exactly has the authority to provide the requisite authorization for accessing a computer or website. As the dissent rightly recognized, "[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." *Nosal II*, 844 F.3d at 1052 (Reinhardt, J., dissenting) (emphasis added). Given that password sharing is a routine online practice,[14] this broader definition is certainly more consistent with pervasive societal practices and expectations.

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. It's thus no wonder that the dissent found the majority's definition of authorization "somewhat circular." *Nosal II*, 844 F.3d at

14. Matthew Humphries, "Up to 60 Percent of Streaming Account Passwords Are Shared," *PC Magazine* (May 26, 2017), http://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.com* (Feb. 18, 2016), https://www.inc.com/will-yakowicz/infographic-95-percent-share-6-passwords-with-friends.html (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 Passwords Closer," *The LastPass Blog* (Feb. 18, 2016), https://blog.lastpass.com/2016/02/infographic-keep-your-friends-close-your-passwords-closer-2.html ("[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."). *Amicus* does not condone password sharing, but Internet users do it *all the time*.

1052 (Reinhardt, J., dissenting). Despite claiming not to, the majority's construction "base[s] criminal liability on system owners' access policies." *Id.* at 1054 (Reinhardt, J., dissenting). And as a result, the majority's test—whether authorization came directly from the computer owner—not only "loses sight of the [CFAA's] anti-hacking purpose" but it also "threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens." *Id.* at 1049 (Reinhardt, J., dissenting). Indeed, 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. And not only is such password sharing routinely done without the computer owner's express permission, but website operators commonly explicitly restrict password sharing in their terms of use. There is thus no "workable line . . . separat[ing] 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." *Id.* at 1049 (Reinhardt, J., dissenting).

The Court should grant certiorari to correct the error of the Ninth Circuit, resolve widespread confusion about the CFAA's reach, and ensure that lower courts limit the statute to the purpose intended by Congress: 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 Second and Fourth Circuits' decisions to adopt a narrow interpretation of the statute. Both 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 wished without the clarity and specificity required of criminal law. *See Valle*, 807 F.3d at 527; *WEC Carolina*, 687 F.3d at 205–06. "'[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[.]" *Valle*, 807 F.3d at 527 (quoting *Nosal I*, 676 F.3d at 860). Specifically, attaching criminal punishment to breaches of vague, boilerplate policies[15]—which companies typically reserve the right to modify at any time[16]—would make it impossible for employees to know what conduct

15. One sample Internet and email usage policy, for example, warns that "Internet use, on Company time, . . . is authorized to conduct Company business only" and "[o]nly people appropriately authorized, for Company purposes, may use the internet[.]" Susan M. Heathfield, Sample Internet and Email Policy, The Balance (Jan. 14, 2017), http://humanresources.about.com/od/policiesandsamples1/a/email_policy.htm; *see also* Virginia Dep't of Human Resource Management, Use of the Internet and Electronic Communications Systems (Mar. 17, 2011), http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf?sfvrsn=2 (stating that computer use restrictions include, "but are not limited to" seven specific prohibitions, as well as "any other activities designated as prohibited by the agency").

16. *See, e.g.*, hrVillage, Employee Handbook Template, http://www.hrvillage.com/downloads/Employee-Handbook Template.pdf (last viewed May 31, 2017) ("The policies stated in this handbook are subject to change at any time at the sole discretion of the Company."); Dartmouth College, Employment Policies and Procedures Manual, http://www.dartmouth.edu/~hrs/policy (last viewed May 31, 2017) ("The policies are intended as guidelines only, and they may be modified, supplemented, or revoked at any time at the College's discretion.").

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) (expansive or uncertain interpretations of unauthorized access would provide "insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited"). 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 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.*

The Ninth Circuit's decision below specifically creates legal uncertainty regarding whether it is a crime to use another person's password without permission from the computer owner.[17] Under the majority's reasoning, nearly anyone who logs into someone else's online or computer account, even with their consent, in violation of a prohibition on password sharing is a potential criminal. Indeed, while the CFAA allows a private party to bring a civil suit only when the party has suffered a loss 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 password sharing could be enough.[18]

17. While the majority tries to distinguish sharing passwords to a proprietary corporate database from sharing passwords to social media accounts or bank websites, as outlined previously, the dissent rightly notes that it fails to provide a "workable line" separating the two. *See Nosal II*, 844 F.3d at 1049 (Reinhardt, J., dissenting).

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

As noted above, password sharing is a common practice. People routinely share their passwords or access credentials—even when such sharing is explicitly banned in a website's terms of use—with family members, caregivers, colleagues, or other trusted individuals to enable them to send an email on their behalf, check their social networking information or contact lists, post a tweet, pay a bill, or check a bank or credit card statement. Under the panel majority's interpretation, a husband who, with his wife's permission, logs into her Facebook account has acted without authorization and is guilty of a federal crime.[19] The same would be true if the husband used the wife's login credentials (rather than his) to access their joint bank account to pay family bills, or if a paralegal accessed a lawyer's email account, in violation of policies against password sharing. *See Nosal II*, 844 F.3d at 1051 (Reinhardt, J., dissenting). The decision below turns all such "agents" into potential criminals simply because such access was banned by the computer owner—likely via boilerplate language hidden deep within a terms of service agreement that the vast majority of users did not and will never read. And as the public's use of online services requiring passwords and other forms of authentication prior to access increases, the scenarios for serious criminal liability for such behaviors do too.

By subjecting an untold number of Internet users to potential prosecution, the expansive interpretation adopted by the Ninth Circuit below enables prosecutors to pick and choose which types of password sharing or

19. Facebook's terms of service specifically state, "You will not share your password . . . , let anyone else access your account, or do anything else that might jeopardize the security of your account." Facebook, Statement of Rights and Responsibilities 4.8 (Jan. 30, 2015), https://www.facebook.com/legal/terms.

account access "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.

The expansive interpretation of the CFAA adopted by the Ninth Circuit and other courts does not meet the Constitution's standards. The Court should grant certiorari to correct their erroneous interpretation and 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 panel majority's broad reading of the CFAA also threatens to chill socially valuable research, journalism, and testing online, much of which is protected First Amendment activity. This includes not only computer security research, but also audit testing for online discrimination. Judge Reinhardt's dissent lists examples of innocuous behavior that could be rendered criminal by an expansive reading of the CFAA. *See Nosal II*, 844 F.3d at 1052 (Reinhardt, J., dissenting). It could also

criminalize—and therefore *will* undoubtedly chill[20]—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.

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 majority's interpretation of access "without authorization" 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—or, specifically, sharing passwords 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,

---

20. The uncertainty created via courts' overbroad reading 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), available at 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.").

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.[21] 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, say, male versus female users. In the latter 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 panel's opinion, if a company disagrees with the purpose of a researcher's access to its website, it can render that research criminal by merely stating in its terms of use or by letter that researchers are not authorized to access its website, or that individual users are not allowed to share their access credentials with researchers or journalists. Websites could therefore shut down any unwanted anti-discrimination research or testing, even

21. *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.

where the researcher did not break into a computer. Under the panel opinion, 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.

CONCLUSION

The Court should grant the petition writ of certiorari.

Dated: June 5, 2017

Respectfully submitted,

Jamie Williams
Counsel of Record
Cindy Cohn
Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
jamie@eff.org

Counsel for Amicus Curiae