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 *AMICI CURIAE* SERGEY BRATUS, GABRIELLA COLEMAN, TOR EKELAND, MARK JAFFE, FREDERIC JENNINGS, MARINA MEDVIN, NATHAN REITINGER, AND YUAN STEVENS IN SUPPORT OF PETITIONER

TOR EKELAND
TOR EKELAND, P.C.
43 West 43rd Street, Suite 50
New York, NY 10036
(718) 737-7264

ROY I. LIEBMAN
Counsel of Record
COUNSEL PRESS
460 W. 34th Street, 4th Floor
New York, NY 10001
(212) 685-9800
rliebman@counselpress.com

Counsel for Amici Curiae

273488

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

Statutes

Other Authorities

Cited Authorities

Cited Authorities

Page

STATEMENT OF INTEREST OF *AMICI CURIAE*[1]

Amici curiae are directly and substantially involved either as researchers or attorneys with individuals and groups that are often targeted, criminally or civilly, under the Computer Fraud and Abuse Act ("CFAA"). *Amici* share a common interest in seeing the current circuit court split on the definition of what constitutes unauthorized access to a computer under the CFAA resolved in favor of a narrow definition with a technical foundation involving, for example, code-based circumvention of access and authentication barriers. *Amici* believe that the current interpretive hodgepodge of theories of CFAA "authorization" in the circuit courts of appeals invite dubious and arbitrary criminal and civil prosecutions of mundane, commonplace, and even virtuous computer behavior.

Sergey Bratus is a Research Associate Professor in the Computer Science Department at Dartmouth College in New Hampshire. At Dartmouth, he is also the Chief Security Advisor for the Institute for Security, Technology, and Society. He holds a Ph.D. in Computer Science from Northeastern University and his undergraduate degree is from the Moscow Institute of Physics and Technology. He

1. Per Supreme Court Rule 37.2(a), all parties received appropriate notice of the filing of this brief. Petitioner consented to the filing of this brief; Respondent provided blanket consent. Copies of the requisite consent letters have been filed with the Clerk. Per Rule 37.6, no counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of the brief. This brief has been entirely paid for by the *amici* and/or their attorney's.

holds a strong interest in ensuring that legal definitions do not become an obstacle in creating effective security policies, particularly in critical infrastructure systems such as hospitals.

Gabriella Coleman holds the Wolfe Chair in Scientific and Technological Literacy at McGill University in Montreal, Canada. Her scholarship examines the ethics and politics of computer hacking and she is now considered one of the world's foremost experts on hackers. She holds a PhD and MA in Anthropology from the University of Chicago, and a BA degree in Religious Studies from Columbia University. She has authored two books, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton University Press, 2012) and *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (Verso, 2014) and speaks regularly to multiple publics about the complex motives, contributions, benefits, and costs of various hacker communities. She is particularly concerned about how the overzealous application of the CFAA chills digital protest activity and security research.

Tor Ekeland, Mark H. Jaffe, and Frederic Jennings are New York City based federal criminal defense lawyers. Through their law firm, Tor Ekeland, P.C. (the "Firm"), they regularly represent individuals accused of violating the CFAA. The Firm has represented, or is representing, defendants accused of computer crimes in federal district courts in California, Kentucky, Massachusetts, Minnesota, New York, New Jersey, Tennessee, Texas, and Virginia. Currently the Firm has CFAA-related appeals before the Fifth and Ninth Circuit Courts of Appeals. *See United States v. Michael Thomas*, No. 16-41264 (5th Cir.); *United*

States v. Matthew Keys, No. 16-10197 (9th Cir.). The Firm is particularly interested in the principled, fair, and just application of computer crime laws, including the CFAA.

Marina Medvin is an attorney who represents criminal defendants charged under the CFAA in the Eastern District of Virginia.

Nathan Reitinger is a lawyer and M.S. Candidate in the Department of Computer Science at Columbia University. Working at the convergence of law and technology, he advocates for a more nuanced understanding between these two disparate fields, aiming to provide solutions not only from a legal and public policy perspective, but also from a software engineering standpoint.

Yuan Stevens is a researcher at the Berkman Klein Center for Internet and Society, and a research assistant for Gabriella Coleman at McGill University. She contributes to writing, policy, and legal developments to ensure the constitutional rights of computer users.

All *Amici* are deeply concerned that the present lack of definitional clarity of the concept of authorization under the CFAA is detrimental to our federal criminal and civil law and leads to potentially detrimental unintended consequences.

SUMMARY OF ARGUMENT

The federal appellate courts of this nation have been issuing contradictory decisions interpreting "without authorization" under the CFAA for over a quarter of a century. Although the law was passed in 1984, and

amended numerous times since, this Court has yet to rule on the issue. The Petition for a Writ of Certiorari for *United States v. Nosal* 844 F.3d 1024 (9th Cir. 2016) is an opportunity for this Court to provide necessary clarity on the meaning of "without authorization," a concept central to liability under the dual criminal and civil CFAA.

The prohibition against accessing a computer without authorization has always been central to the CFAA. Yet, despite courts' repeated claims that the meaning of authorization is plain and unambiguous, a pronounced circuit split persists. The Ninth Circuit's most recent conclusion—essentially, that private relations between parties may govern the meaning of "authorization"—will over-criminalize the already expansive CFAA, leading to detrimental and unintended consequences. This Court should grant certiorari and bring clarity to a debate that has gone unresolved for over a quarter of a century.

ARGUMENT

The CFAA fails to define the concept central to the majority of its prohibitions: authorization. Since *United States v. Morris*, courts have often concluded that "authorization" is a word of common usage, lacking in technical or ambiguous meaning. 928 F.2d 504, 511 (2d Cir. 1991). However, this word is at the heart of an indisputable and pronounced circuit split. And most recently, with the Ninth Circuit's conclusion that "once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by [sharing a password and] going through the back door," the opaque term threatens to give rise to unintended consequences and the excessive criminalization of common computer use. *United States*

v. Nosal, 844 F.3d 1024, 1028 (9th Cir. 2016) ("*Nosal II*"). To bring much needed clarity to this debate, *amici*—attorneys, professors, and computer scientists—urge the Court to grant certiorari.

I. THE COURT SHOULD GRANT CERTIORARI TO CLARIFY THE MEANING OF AUTHORIZED ACCESS TO A COMPUTER UNDER THE CFAA

Generally speaking, the CFAA prohibits three categories of conduct. First, it prohibits unauthorized access,[2] or exceeding authorized access, to a computer.[3] *See* 18 U.S.C. § 1030(a)(1)-(4). Second, it prohibits unauthorized damage to a computer (without any requirement that there be unauthorized access). *See* 18 U.S.C. § 1030(a)(5)(A). And third, it prohibits unauthorized access to a computer that recklessly causes damage, or that causes loss. *See* 18 U.S.C. § 1030(5)(b)-(c).

---

2. While the CFAA does not explicitly refer to "unauthorized access" and instead uses "without authorization or exceeding authorized access," courts and legal scholarship tend to agree that the lodestar issue turns on whether access was authorized. For ease of reading, this brief will refer to "without authorization" interchangeably with "unauthorized access."

3. The CFAA's definition of "exceeds authorized access" is circular, as are many circuit courts' definitions of CFAA "authorization." 18 U.S.C. 1030(e)(6) states "the term '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." This says nothing more than exceeding authorized access means obtaining or altering information that one is not authorized to. *See* Orin Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1146 & fn. 16 (2016) (discussing the circularity of definitions of authorization).

In each of these statements, "authorization" or the absence of it, remains critical.[4] When reviewing CFAA jurisprudence, two landmarks come into focus: (1) the importance of defining the CFAA's use of "without authorization," not only for its impact on CFAA proceedings, but also for its broad influence on the field of computer law as a whole; and (2) as the case law demonstrates, the meaning of "without authorization" is not plain or unambiguous.

A. The Definition of Authorization Under the CFAA is of Critical Importance

The meaning of unauthorized access has far reaching implications,[5] even beyond the CFAA. Many states,[6]

---

4. *See Cyber Security: Protecting America's New Frontier: Hearing Before the H. Subcomm. on the Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong., 3 (2011) (statement of Orin S. Kerr, Prof. of Law, G.W. Law School) (finding that the lodestar issue in the CFAA is unauthorized access).

5. *See United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) ("*Nosal I*") (discussing how the term should be consistently interpreted throughout the statute).

6. *See e.g.*, Cal. Penal Code § 502 ("unauthorized access"); Colo. Rev. Stat. § 18-2.5-102(1)(a) ("without authorization"); Del. Code tit. 11, § 932 ("unauthorized access"); Iowa Code § 716.6B(1) ("without authorization"); Utah Code Ann. § 76-6-702 ("without authorization"). For a list of applicable statutes for all fifty states, see NCSL, *Computer Crime Statutes* (Dec. 5, 2016), at https://perma.cc/7C38-V3GA.

foreign countries,[7] and other federal statutes[8] use "unauthorized access" to define the scope of computer crimes. *See* Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 Bus. Law. 1395, 1395-96 (2007) ("Statutes forbidding 'unauthorized access' to computers have come to serve as a central pillar of the legal protections governing networked computer systems, both in the United States and throughout the world.").

Additionally, the ambiguity of "unauthorized access" makes it easy for a prosecutor to turn a CFAA violation into a felony punishable with a maximum sentence of 5-20 years. *See* 18 U.S.C. 1030(c) *et seq.* For example, there is felony liability if the loss incurred from the unauthorized access or damage is greater than $5000.00, a relatively easy threshold to meet. *See id.* at 1030(c)(B)(3); *id.* at (c)(4)(A)(i)(I); *id.* at (4)(B). And $5000.00 is also the threshold for a civil CFAA lawsuit. *See id.* at 1030(g). Moreover, under 18 U.S.C. 1030(a)(2)(c), the most common provision of the statute used by prosecutors, there is felony liability if the "offense was committed in furtherance of any criminal or tortious act," or if the value of information obtained is over $5000. *See id.* at 1030(c)(2)(B)(ii). Thus, a broad-based interpretation of CFAA authorization not only increases the scope of computer crime felonies as

---

7. *See* Convention on Cybercrime, Nov. 23, 3001, E.T. S. No. 185, art. 2, *available at* https://perma.cc/7VQ3-P2TW ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.").

8. *See e.g.* Stored Communications Act, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C.A. §§ 2701-12 (2000)).

a whole, but also invites dubious, docket-clogging civil litigation.

Therefore, the meaning of "unauthorized access," perhaps more than any other term found in the CFAA, is critical—not only to the CFAA's breadth and scope, but also to the field of computer law as a whole. Overbroad interpretation has detrimental, unintended consequences and leads to the over-criminalization of innocuous behavior. This is a direct result of the competing and contradictory interpretations of "authorization."

B. The CFAA's Ambiguity as to "Authorization" is Indisputable

At the outset, Amici would like to note that, generally, they agree with Petitioner's framing of the circuit split—there exist circuits that define authorization in terms of "intended use" by the owner, an owner-agency relationship, or a contractual-based relationship; likewise, there exist circuits that define authorization in terms of the CFAA's anti-hacking purpose or in an ad hoc, hybrid sense. Any explanation of the case law provided by Amici, therefore, is illustrative, aiming to provide context for both the owner-centric and hacking-based views of the statute.

It is difficult to argue the definition of "without authorization" is plain and unambiguous given the pervasive circuit split currently dividing our federal courts. *See, e.g., Nosal I*, at 862; *United States v. Valle*, 807 F.3d 508, 523 (2d Cir. 2015) (discussing the problem of defining the scope of exceeding authorized access and noting that "[o]ver the past fourteen years, six other circuits have wrestled with the question before us"); Orin Kerr, *Norms of Computer Trespass*, 116 Colum. L.

Rev. 1143, 1144-46 1153-61 (2016) (discussing the circuit split at length and arguing for a normative definition of authorization).

Courts have been struggling with the meaning of unauthorized access under the CFAA since 1991. *See, e.g.*, *Morris*, 928 F.2d at 511); *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009); *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 303-04 (6th Cir. 2011); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012); *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015); *Nosal II*, at 1028.

The through line through these cases is the struggle to determine the meaning of unauthorized access. Indeed, as the following section entails, the last twenty-six years portray myriad attempts (amassed around five roughly-categorized theories) at defining what exactly authorization to access a computer means. These include: (1) the intended use theory; (2) the breach of contract theory; (3) the agency theory; (4) the anti-hacking theory; and (5) "hybrid" theories.[9] However, the Court should take note that, to date, no single theory has received a dominant position among the scholarship. Truly, no one knows what "unauthorized access" means.[10]

---

9. To muddy the waters further, circuit and district courts are often inconsistent in the use of a particular theory within their own circuit. *Compare Valle*, 807 F.3d at 524-25 (asserting an anti-hacking theory), *with Morris*, 928 F.2d at 510 (2d Cir.) (applying the intended use theory).

10. *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse*

1. Intended Use Theory of CFAA Authorization

Dating from 1991, the intended use theory of the CFAA's definition of "authorization" is the first theory to emerge from the Circuit Courts. In *United States v. Morris*, defendant Robert Morris—the first person convicted under the CFAA, now a tenured professor at MIT—sought to demonstrate security flaws in the nascent internet by releasing what he believed to be a harmless "worm" on networked university computers. *Morris*, 928 F.2d at 505-06. Unfortunately, Morris's worm was not exactly harmless, and eventually crashed a large number of computers throughout the country. *Id.* at 505-06.

On appeal, Morris argued that he acted with "authorization" when he released his worm onto university computers because he had valid access credentials for those computers. *Id.* at 510. The Second Circuit disagreed, holding that Morris's access was unauthorized because the computer's software was not written with the intent that its flaws be exploited, even though Morris was authorized to access and use the computers. *Id.* at 510.

Discussing the interpretation of authorization, the Second Circuit found "the word is of common usage, without any technical or ambiguous meaning." *Id.* at 511. However, disparities of the circuit courts' defining this term over the 26 years since *Morris* belie this

---

Statutes, 78 N.Y.U. L. Rev. 1596, 1597-98 (2003) ("[T]he result [of such an elusive term] is an odd situation in which nearly every Anglo-American jurisdiction has an unauthorized access statute that carries series felony penalties, but no one seems to know what these new laws cover.").

statement—courts across the country largely disregarded the intended use test. The Fifth Circuit is the only other circuit to explicitly endorse it, though it remains largely undeveloped in that circuit. *See generally United States v. Phillips*, 477 F.3d 215, 219-220 (5th Cir. 2007).

2. Contract Law Theory of CFAA Authorization

The contract law theory of authorization at least has the virtue of straightforwardness. Under this theory, a breach of a computer use contract, such as an online terms of service agreement, may constitute "unauthorized access" under the CFAA. Unfortunately, it essentially criminalizes contract law by allowing private actors—and not Congress—to define the boundaries of criminal conduct. Rarely do people expect that a breach of contract will lead to felony charges, especially with the prevalence of "clickwrap" or "browserwrap" terms. *See United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Ca. 2009) ("Thus, while 'ordinary people' might expect to be exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties.").

United States v. Drew provides a good illustration of the pitfalls of the contract theory of authorization. The defendant in *Drew* was charged with "access without authorization" under 18 U.S.C. § 1030(a)(2)(C) for violating a website's terms of service. *See Drew*, 259 F.R.D. at 449. The defendant conspired with others to create a fake profile on a social networking site for the purpose of harassing a 13-year-old girl, her daughter's classmate, eventually leading to the victim's death. *Id.* at 452. The site's terms of service provided that users

were "only authorized to use" the site if they agreed to abide by its terms of service, which prohibited creating a false profile. *Id.* at 462. Drew was convicted on the theory that she accessed the site after her violation of the terms terminated her authorization. *Id.* at 453.

Ultimately, the District Court in *Drew* granted the defense's Rule 29 motion for an acquittal on the basis that the conviction was void for vagueness under the Fifth Amendment's Due Process clause.[11] *See* FED. R. CRIM. P. 29; *Drew*, 259 F.R.D. at 464-65; *see also* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1562-63 (May 2010).

After *Drew* was decided, both the Ninth Circuit (in *Nosal I*) and Second Circuit (in *Valle*) followed suit, reversing convictions raising similar notice issues. *See Nosal I*, at 860; *Valle*, 807 F.3d at 527. Noting that employment relationships are "traditionally governed by tort and contract law," the Ninth Circuit rejected an "interpretation of the CFAA [that] allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law." *Nosal I*, at 860. The court found "[s]ignificant notice problems" with criminal prohibitions that "turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read." *See id.*

But, as with intended use, the majority of courts have not adopted this theory. The Ninth Circuit, along with the

---

11. The United States did not appeal the District Court's ruling.

Second and Fourth Circuits rejected the theory outright. Only the First and the Eleventh Circuits have endorsed it, while other circuits have considered the issue in passing. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 (1st Cir. 2001); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010).

3. Agency Theory of CFAA Authorization

Turning to the third theory, using principles of agency to define authorization, we find perhaps the broadest approach. Invoking the common law of agency, courts here base authorization almost entirely on the relationship between a plaintiff and defendant. Under this theory, although the defendant has full technical authorization to access a computer, a court will nonetheless infer unauthorized access solely on the basis of a change in the relationship's status. In this way, agency theory is unmoored from any code-based, technical access circumvention or authorization principles.

Only the Seventh Circuit has explicitly adopted this theory, and that was only in the context of 18 U.S.C. § 1030(a)(5)(A), interpreting damage without authorization, not unauthorized access.[12] In *Citrin*, an employee decided

12. *Citrin* raises the interesting issue, nowhere definitively resolved in any circuit court, of whether authorization in the access context is the same as authorization in the unauthorized damage context of 1030(a)(5)(A). Generally, "[a] term appearing in several places in a statutory text is generally read the same way each time it appears." *Ratzlaf v. United States*, 510 U.S. 135, 143 (1993). But caution is in order, because 18 U.S.C. 1030(a)(5)(A) does not require access for criminal liability, only unauthorized damage. Thus, a system user acting at all times with authorized access theoretically may be prosecuted for unauthorized damage to that system.

to start a business competing with his employer. *Citrin*, 440 F.3d at 419. Before quitting, he deleted valuable files from his company laptop. *Id.* The Seventh Circuit held that an employee terminates the agency relationship when they breach their duty of loyalty, and thus authorization is passively and constructively rescinded. *Id.*

However, just like intended use and contract theory, the theory embodied by *Citrin* has not taken hold either. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) (rejecting *Citrin* and stating that *Citrin*'s expansive interpretation "has far-reaching effects unintended by Congress"); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) (noting that interpreting "authorization" from a cessation-of-agency standpoint nullifies other parts of the statute prohibiting access *in excess* of authorization).

4. Anti-Hacking Theory of CFAA Authorization

The anti-hacking theory interprets authorization according to the CFAA's underlying purpose—to penalize sophisticated computer hacking. *See Nosal I*, at 857-58 (discussing the CFAA as an "anti-hacking" statute); 132 Cong. Rec. 9160, statement by Representative William J. Hughes (finding the focus of the CFAA placed squarely on "technologically sophisticated criminal[s] who break [ ] into computerized data files."). On the whole, the anti-hacking theory of CFAA authorization rejects use of the CFAA to criminalize employment disputes, to bypass the difficult burdens of proof of trade secret laws, or to punish copying unprotected data from public servers.

The Second Circuit's recent decision in *Valle* is illustrative. *Valle*, 807 F.3d 508, 524-25 (2d Cir. 2015). The defendant in *Valle* was a New York City police officer who participated in online fantasy forums where he wrote of his "desire to kidnap, rape, torture, and eat women whom he knows." *Id.* at 516. Valle exploited his access to a police database to obtain the personal information of a high school classmate whom he had discussed kidnapping with an online acquaintance. *Id.* at 513. He was charged with "exceeding authorized access" under § 1030(a)(2) for violating a department rule prohibiting access for non-law enforcement purposes. *Id.* at 524.

Applying the Rule of Lenity, the Second Circuit reversed Valle's CFAA conviction. *Id.* at 528. It recognized that NYPD policy prohibited Valle from accessing the police database for non-law enforcement purposes, but allowed him to use it for other purposes. *Id.* at 524. Finding support for the government and defendant's interpretations of "authorized access," the Court recognized the CFAA's origins as a statute meant to criminalize computer hacking. Thus, it vacated the conviction, citing *Nosal I* to find that "the government's interpretation of 'exceeds authorized access' makes every violation of a private computer use policy a federal crime." *Id.* at 528.

Viewing "without authorization" within the context of the CFAA's purpose as an anti-hacking statute is the most popular authorization theory to date—the Second, Fourth, and Sixth circuits generally agree with this theory. *See Valle*, 807 F.3d at 524-25; *Miller*, 687 F.3d at 200 ("Today, the CFAA remains primarily a criminal statute designed to combat hacking"); *Pulte Homes*, 648 F.3d at 300, 307. However, as with other theories, no single position has

been able to receive a majority's favor. Until this Court grants certiorari and answers the real question, defining authorization, the anti-hacking theory is no more tenable than any of the other theories currently serving as fodder in this pervasive circuit split.

5. Hybrid Theories of CFAA Authorization

The final class of theories is a catch all for *ad hoc* notions of unauthorized access based on particular fact patterns combining components of the other theories. These cases typically arise when access to a computer is arguably authorized under one of the previous theories, either by a third party (such as in password sharing cases) or where a party accessed publicly available information with no circumvention of a technical access barrier, but some intervening factor renders a court to hold the computer access unauthorized. That intervening factor may be the computer owner stating the access is now unauthorized, that the computer owner did not intend for its information to be publicly available, or that otherwise authorized access becomes unauthorized because the access is used to commit a separate crime. *See, e.g., Nosal II*, at 1029 (holding that affirmative revocation by a computer owner may render authorized access unauthorized); *Facebook v. Power Ventures, Inc.*, 828 F.3d 1068 (9th Cir. 2016), *opinion amended and superseded after of denial on reh'g en banc by* 844 F.3d 1058, 1062 (9th Cir. 2016) (same); *United States v. Auernheimer*, 748 F.3d 525, 541 (3d Cir. 2014) (vacating conviction for unauthorized access to unprotected data on publicly facing servers on venue grounds); *Craigslist Inc. v. 3 Taps Inc.*, 942 F. Supp. 2d 962, 969-70 (N.D. Cal. 2013).

Over the last quarter century there have been numerous attempts at defining the meaning of unauthorized access. Yet, none of these legal theories have gained broad acceptance. What is more, the circuits often struggle to consistently apply a single theory from case to case. Even when narrowed to criminalizing "hacking," courts remain split on what, exactly, that means. This Court should grant certiorari to resolve the circuit split and alleviate the confusion.

II. THE COURT SHOULD GRANT CERTIORARI TO LIMIT THE UNINTENDED, DETRIMENTAL CONSEQUENCES THE CURRENT CIRCUIT SPLIT FACILITATES

Amici submit this brief to the Court because they witness firsthand the consequences and confusion generated under the CFAA's ambiguous terms. The majority's interpretation in *Nosal II* of "without authorization," combined with the pervasive circuit split, should not be viewed by this Court as consequence free. Without clarity in this area of the law, unintended consequences are sure to continue, including: (1) over-criminalizing ordinary computer usage; (2) de-incentivizing critical information security research; and (3) impacting critical industries in unforeseen ways.

A. Broad Based Definitions of CFAA Authorization Over-criminalize Normal Computer Use

As the dissent in *Nosal II* pointed out, the difficulty in drawing the line where the majority did—defining "without authorization" in terms of private parties'

agreements[13]—is that it is impossible to distinguish *Nosal II* from the ordinary practice of password sharing. This, in turn, over-criminalizes computer law, paralleling the problems faced in the contract theory of authorization. *See supra*, Part II.B.2 (criminalizing behavior large numbers of people view as innocuous or normal, not criminal).

But over-criminalization has yet another facet often lost in legal scholarship. Take Judge Reinhardt's hypothetical in *Nosal II* for example: "We would not convict a man for breaking and entering if he had been invited as a houseguest, even if the homeowner objected." *Nosal II*, at 1051 (Reinhardt, J., dissenting). What Judge Reinhardt's analogy does not say is equally as important. While it may seem obvious that the invitee would not be convicted for breaking and entering, it is also true that we would not expect the prosecutor to bring *exceptional* penalties just because the man was "invited" by a third party. Yet, this is what the CFAA often does.

In other words, the use of a computer to violate a perceived norm should not make the offense inherently worse in the eyes of the law. *See* Andrea M. Matwyshyn, *The Law of the Zebra* 28 Berkeley Tech. L.J. 155, 160-62 (2013) (noting how courts routinely complicate

13. *See Nosal II*, at 1055 (Reinhardt, J., dissenting) ("It is impossible to discern from the majority opinion what principle distinguishes authorization in Nosal's case from one in which a bank has clearly told customers that no one but the customer may access the customer's account, but a husband nevertheless shares his password with his wife to allow her to pay a bill. So long as the wife knows that the bank does not give her permission to access its servers in any manner, she is in the same position as Nosal and his associates.").

straightforward issues by searching high and low for "technology-specific paradigms").

B. Broad Base Definitions of CFAA Authorization are Detrimental to Computer Security Research

Another consequence resulting from hinging major parts of criminal and civil CFAA liability on broad based definitions of "authorization" is that security research and threat analysis is likely to be chilled. *See, e.g.*, Christopher Soghoian, *Legal Risks for Phishing Researchers*, eCrime Res. Summit 2008, p. 11 (acknowledging the high likelihood of certain computer science research to violate legal standards); Cassandra Kirsch, *The Gray Hat Hacker: Reconciling Cyberspace Reality and Law*, 41 N. Ky. L. Rev. 383, 387 (2014) ("The vagueness of CFAA . . . gives cyber security researchers a disincentive to find security flaws, which makes the rest of us less safe on the Internet.").

Unless clarity is brought to the meaning of "authorization," the term will continue to hinder well-intentioned research. *See generally Cybersecurity Research: Addressing the Legal Barriers and Disincentives, Berkeley Center for Law & Technology Workshop* (Sept. 28, 2015), *available at* https://perma.cc/JZR2-9YAM.

C. Broad Based Definitions of CFAA Authorization May Have Unintended Consequences for Critical Industries.

A final unintended consequence of note comes from cyber security research in healthcare. Here, it is

important to consider that a company's "security policy" governs the scope of what users may do on their computer. Yet, research shows it is often necessary to bypass security policies in order to effectively complete a job. Here, circumvention of computer security policies is not only common, but essential.

To understand this result, consider that, from a security-design standpoint, security professionals create policy rules (i.e., "permission management"[14]) based on their understanding of the workers' roles and responsibilities. Their concepts of policy and of the required permissions to access data are enshrined in how those users interact with the software. However, that view and, as a result, these policy concepts, are far removed from the actual clinical practice. *See* Koppel, Smith, Blythe & Kothari, at 217 ("[I]n healthcare, we see endemic circumvention of password-based authentication. In hospital after hospital and clinic after clinic, we find users write down passwords everywhere.") This is the new normal when it comes to complex computing systems. *Id.* at 216 ("We find, in fact, that workarounds to cyber security are the norm, rather than the exception. They not only go unpunished, they go unnoticed in most settings—and often are taught as correct practice."). Without knowledge of the practical norms of the computer security industry, courts have criminalized routine security practices through broad definitions of unauthorized access under the CFAA.

14. "Permission management, or provisioning, refers to the business process of specifying which individuals or groups are allowed access to which files and data." Ross Koppel, Sean Smith, James Blythe, and Vijay Kothari, *Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?*, Info. Tech. & Comm. in Health 215, 217 (2015).

Thus, criminalizing password sharing can have severe, unintended consequences, as it is a routine practice in certain critical industries. This Court should bring clarity to what constitutes unauthorized access to a computer under the CFAA and reverse the decision in *Nosal II*.

CONCLUSION

The Court should grant the Petition for Certiorari.

Respectfully submitted,

TOR EKELAND
TOR EKELAND, P.C.
43 West 43rd Street, Suite 50
New York, NY 10036
(718) 737-7264

ROY I. LIEBMAN
Counsel of Record
COUNSEL PRESS
460 W. 34th Street, 4th Floor
New York, NY 10001
(212) 685-9800
rliebman@counselpress.com

Counsel for Amici Curiae