No. 19-783

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for Writ of Certiorari to the United States Court of Appeals for the Eleventh Circuit

BRIEF OF THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

JEFFREY T. GREEN
CO-CHAIR, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AMICUS COMMITTEE
1660 L Street, N.W.
Washington, D.C. 20036
(202) 872-8600

CLIFFORD W. BERLOW
Counsel of Record
GRACE C. SIGNORELLI-CASSADY
JENNER & BLOCK LLP
353 N. Clark Street
Chicago, IL 60654
(312) 840-7366
cberlow@jenner.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

RULES AND STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICUS CURIAE* [1]

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit, voluntary bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of a crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers.

NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous *amicus* briefs each year in the United States Supreme Court and other federal and state courts, seeking to provide *amicus* assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

The Petition presents a question of great importance to NACDL and the clients its attorneys represent

---

[1] In accordance with Supreme Court Rule 37, *amicus curiae* states that no counsel for a party authored this brief, in whole or in part, and no counsel or party made a monetary contribution to fund the preparation or submission of this brief. No person other than the *amicus curiae*, its members, and its counsel made any monetary contribution to its preparation and submission. Pursuant to Supreme Court Rule 37.2, counsel of record for all parties received timely notice of *amicus curiae*'s intent to file and both parties have consented to the filing of this brief.

because of the ubiquity of computer use in this country and the possibility that ordinary computer use could be prosecuted as a federal crime. NACDL also believes criminal statutes should be construed consistently with Congress' intent, and narrowly when Congress' intent is not clear. Given NACDL's expertise in these matters, NACDL submits that its perspective on the importance of this Petition and whether to grant certiorari will be of "considerable help" to the Court. Sup. Ct. R. 37.1.

SUMMARY OF THE ARGUMENT

In this case, the Eleventh Circuit reaffirmed that a person violates the Computer Fraud and Abuse Act ("CFAA") by using a computer to access information for an improper purpose, even if that person is otherwise authorized to access that information. As the Petition explains, this holding warrants review because it reinforces a conflict of authority regarding the meaning of "authorized access" under the CFAA, Pet. 7-12, and because the Eleventh Circuit was wrong on the merits, Pet. 16-22.

Review also is warranted because the question presented is important. Computers are ubiquitous in daily life. It is important that the Court clarify that ordinary deviances from terms-of-use requirements—whether imposed by internet websites or private company use guidelines, to name but a few—are not criminal. For that reason, this Court should grant review.

This Court's review also is necessary because the Eleventh Circuit's decision deviates from settled practices for construing federal criminal statutes. The touchstone for statutory interpretation always begins

with the text, where necessary accounts for Congress' intent in enacting a criminal statute, and where multiple readings are reasonable, follows the Rule of Lenity and adopts the narrowest reasonable construction. Because the Eleventh Circuit's decision and those courts on its side of the open and acknowledged split of authority break from this approach at every level, this Court should grant review.

ARGUMENT

I. This Case Presents An Important Issue Impacting Millions Of Ordinary Citizens.

Section 1030(a)(2) of the CFAA makes it a federal crime to "intentionally access[] a computer without authorization" or to "exceed[] authorized access," and "thereby obtain[] information from any protected computer." 18 U.S.C. § 1030(a)(2). The CFAA defines a protected computer as any computer "which is used in or affect[s] interstate or foreign commerce or communication"—in other words, every computer with an internet connection. 18 U.S.C. § 1030(e)(2)(B). The CFAA's undeniably broad sweep thus makes it all the more imperative that the Court resolve the open and acknowledged split of authority identified by the Petition.

As the Petition explains, in the Second, Fourth, and Ninth Circuits, a person using a computer with an internet connection only violates the CFAA if that person accesses a computer without permission. *See United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 202, 207 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012). In the First, Fifth,

Seventh, and Eleventh Circuits, however, a person using a computer with an internet connection violates the CFAA if that person uses a computer with permission, but "exceeds" the scope of that person's permitted use. *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010), *cert denied*, 568 U.S. 1163 (2013); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). In practice, this has resulted in indefensible inconsistencies. For example, the Second Circuit reversed a police officer's conviction for violating the CFAA by accessing a law enforcement database to obtain information for a non-official purpose, *Valle*, 807 F.3d at 513, 523, 528, while the Eleventh Circuit in this case affirmed Petitioner's conviction for doing the same. *United States v. Van Buren*, 940 F.3d 1192, 1197–98, 1208 (11th Cir. 2019), *petition for cert. filed*, 88 U.S.L.W. 3211 (U.S. Dec. 18, 2019) (No. 19-783).

The urgency for the Court to address this split of authority now stems from the fact that the computer access rights of most, if not all, computer users are governed by access and use policies, including websites' terms of service and "the typical corporate policy that computers can be used only for business purposes." *Nosal*, 676 F.3d at 860–61. This means in the First, Fifth, Seventh, and Eleventh Circuits, violating commonplace computer use policies can constitute a CFAA violation, transforming seemingly innocuous activities—such as utilizing a work computer to "chat[] with friends," "shop[]," "watch[] sports highlights," or "check the weather report" for a "vacation to Hawaii"—into federal crimes. *See Nosal*, 676 F.3d at 860–61. "This would make

criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *Id.* at 859.

Indeed, crimes this ubiquitous "invite arbitrary and discriminatory enforcement." *Id.* at 860. Some overzealous prosecutors already have utilized the CFAA to do exactly that—to bring federal criminal charges against defendants under the CFAA premised on terms-of-use violations. For instance, in *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), defendant Lori Drew and her conspirators "registered and set up a profile for a fictitious 16 year old male juvenile . . . on the www.My Space.com website ("MySpace")," "posted a photograph of a boy without that boy's knowledge or consent," and cyber-bullied a young girl, all in violation of MySpace's terms of service. *Id.* at 452, 454. Federal prosecutors indicted Drew for three counts of violating a felony portion of the CFAA, and at trial informed the jury that they could also "consider whether the [d]efendant was guilty of the 'lesser included' misdemeanor" CFAA violation. *Id.* at 452–53.

A jury found Drew guilty of the misdemeanor CFAA violation—a conviction predicated entirely on Drew's violation of MySpace's terms of service. *Id.* at 453. Although it was overturned on appeal, Drew's case demonstrates that in the First, Fifth, Seventh, and Eleventh Circuits, prosecutors can treat any computer use violation as a federal crime that is, nonsensically, equated to computer hacking by Russian nationals. *Compare Drew*, 259 F.R.D. at 452 (explaining that "Drew was charged with . . . three counts of violating a

felony portion of the CFAA, *i.e.*, 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii)") *with* Indictment at 13, *United States v. Yakubets et al.*, No. 19-CR-342 (W.D. Pa. Nov. 12, 2019) *available for download at* https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens (indicting two Russian nationals for, among other things, computer hacking pursuant to 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)).

The need for this Court's resolution of the question presented is even more acute because of the substantial criminal penalties that CFAA violations carry. An initial conviction under 18 U.S.C. § 1030(a)(2)—the one at issue in this case—is punishable by fines and imprisonment of up to one year, or up to five years in certain situations, including where the offense was committed for "private financial gain." 18 U.S.C. § 1030(c)(2)(A), (B). Applying the First, Fifth, Seventh, and Eleventh Circuits' framework, this means someone who uses a work computer to make changes to a retirement savings account, in violation of their employer's computer use policy, could face up to five years in federal prison. Permitting such weighty penalties for such commonplace, innocuous activity serves no legitimate purpose, and needlessly promotes over-criminalization. Given the uncertainty among lower courts as to whether that is how the CFAA is meant to be applied, review from this Court is warranted.

II. This Case Presents An Important Question Regarding Congress' Intent In Enacting The CFAA.

This Court also should grant review to ensure the CFAA is being interpreted in a way that is consistent with the CFAA's text, with Congress' intent in enacting the CFAA if the text is unclear, and, if still subject to multiple interpretations, construed narrowly as required by the Rule of Lenity.

Here, the meaning of "exceeds authorized access" in the statute's text, 18 U.S.C. § 1030(a)(2), is "readily susceptible to different interpretations," as evidenced by the numerous Circuits which have "wrestled" with the question and reached opposite conclusions. *Valle*, 807 F.3d at 524. Because the statute's text is unclear, Congress' intent in enacting the CFAA must be considered.

Congress enacted the CFAA "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, *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691–91, 3695–97 (1984); S. Rep. No. 99–432, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2480 (1986)).

The House Committee Report written in conjunction with the original 1984 bill referenced "'hackers' who have been able to access (trespass into) both private and public computer systems." *Id.* (citing H.R. Rep. No. 98–894, at 3695). Likewise, the Senate Committee Report, written in conjunction with the CFAA's 1986 amendment, provided examples of the type of activity it intended the CFAA to address. The first example

concerned "a group of adolescents" who "broke into the computer system at Memorial Sloan-Kettering Cancer Center in New York" and thereby "gained access to the radiation treatment records of 6,000 past and present cancer patients and had at their fingertips the ability to alter the radiation treatment levels that each patient received." S. Rep. No. 99-432, 2, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2480. Similarly, the second example concerned "pirate bulletin boards" created "for the sole purpose of exchanging passwords to other people's computer systems." *Id.* Importantly, both examples involved access to a computer system that the person was not permitted to access, for any reason. This supports that Congress' intent in enacting the CFAA was to address "hacking" and computer "trespass." *Valle*, 807 F.3d at 526.

Moreover, "[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect [Congress] to use language better suited to that purpose." *Nosal*, 676 F.3d at 857. But Congress did not. Thus it can be inferred that Congress did not intend the CFAA to apply this broadly.

That said, there is no doubt that when Congress passed the CFAA, Congress did not—and could not—have taken into account the ubiquity of computer use today, nor the way that computer use is regulated by employers and others. At the start of 1986, the year Congress enacted the CFAA, there were 2,000 total networks connected via the Internet. *Internet History 1962 to 1992*, Comput. Hist. Museum,

https://www.computerhistory.org/internethistory/. For 2020, "forecasts suggest that there will be around 6.58 network connected devices *per person* around the globe," meaning that "there could be nearly 50 billion network connected devices." *Forecast on Connected Devices Per Person Worldwide 2003-2020*, Statista, https://www.statista.com/statistics/678739/forecast-on-connected-devices-per-person/. The explosion in computer use since the CFAA's passage may explain why Congress' intent regarding the CFAA's scope has been difficult to discern.

Even if Congress' intent regarding the CFAA's scope were not clear, however, the Rule of Lenity still requires that the CFAA be construed "strictly" and that "the interpretation that favors the defendant" be adopted. *Valle*, 807 F.3d at 526–27 (citations omitted). This "vindicates the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed." *United States v. Santos*, 553 U.S. 507, 514 (2008). Here, that means criminalizing only instances where a person accesses information on a computer they are not permitted to access, for any reason.

The Eleventh Circuit's decision below is inconsistent with Congress' intent, violates the Rule of Lenity, and reinforces an already open and acknowledged split of authority. The Court should grant review.

CONCLUSION

For the foregoing reasons, as well as those expressed in the Petition, *amicus curiae* the National Association

of Criminal Defense Lawyers urge this Court to grant the Petition for a Writ of Certiorari.

January 17, 2020

Respectfully submitted,

JEFFREY T. GREEN
CO-CHAIR, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AMICUS COMMITTEE
1660 L Street, N.W.
Washington, D.C. 20036
(202) 872-8600

CLIFFORD W. BERLOW
Counsel of Record
GRACE C. SIGNORELLI-CASSADY
JENNER & BLOCK LLP
353 N. Clark Street
Chicago, IL 60654
(312) 840-7366
cberlow@jenner.com

Counsel for Amicus Curiae The National Association of Criminal Defense Lawyers