No. 19-___

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

PETITION FOR A WRIT OF CERTIORARI

Saraliene Smith Durrett
SARALIENE SMITH DURRETT, LLC
1800 Peachtree Street
Suite 300
Atlanta, GA 30309

Rebecca Shepard
FEDERAL DEFENDER PROGRAM, INC.
101 Marietta Street NW
Suite 1500, Centennial Tower
Atlanta, GA 30303

Jeffrey L. Fisher
Counsel of Record
Pamela S. Karlan
Brian H. Fletcher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@stanford.edu

QUESTION PRESENTED

Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose.

RELATED PROCEEDINGS

United States v. Van Buren, No. 1:16-cr-00243-ODE-JFK-1 (N.D. Ga. May 3, 2018)

United States v. Van Buren, No. 18-12024 (11th Cir. Oct. 10, 2019)

TABLE OF CONTENTS

QUESTION PRESENTED i
RELATED PROCEEDINGS ii
TABLE OF CONTENTS iii
TABLE OF AUTHORITIES iv
PETITION FOR A WRIT OF CERTIORARI 1
OPINIONS BELOW 1
JURISDICTION 1
RELEVANT STATUTORY PROVISIONS 1
STATEMENT OF THE CASE 1
REASONS FOR GRANTING THE WRIT 6
I. The courts of appeals are intractably divided over the reach of the CFAA 7
II. The question presented is extremely important 12
III. This case is the right vehicle for resolving the conflict 15
IV. The Eleventh Circuit's decision is incorrect 16
CONCLUSION 22
APPENDIX
Appendix A, Opinion of the U.S. Court of Appeals for the Eleventh Circuit 1a
Appendix B, Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ..... 33a

TABLE OF AUTHORITIES

Page(s)

Cases

Bond v. United States,
134 S. Ct. 2077 (2014) 20

Cloudpath Networks, Inc. v. SecureW2 B.V.,
157 F. Supp. 3d 961 (D. Colo. 2016) 11

EF Cultural Travel BV v. Explorica, Inc.,
274 F.3d 577 (1st Cir. 2001) 7

Hedgeye Risk Mgmt., LLC v. Heldman,
271 F. Supp. 3d 181 (D.D.C. 2017) 11

Int'l Airport Ctrs., L.L.C. v. Citrin,
440 F.3d 418 (7th Cir. 2006) 8

John v. United States,
568 U.S. 1163 (2013) 11

Kolender v. Lawson,
461 U.S. 352 (1983) 21

Merritt Hawkins & Assocs., LLC v. Gresham,
79 F. Supp. 3d 625 (N.D. Tex. 2015) 8

Sebrite Agency, Inc. v. Platt,
884 F. Supp. 2d. 912 (D. Minn. 2012) 11

Teva Pharms. USA, Inc. v. Sandhu,
291 F. Supp. 3d 659 (E.D. Pa. 2018) 11, 12

United States v. Bass,
404 U.S. 336 (1971) 21

United States v. Drew,
259 F.R.D. 449 (C.D. Cal. 2009) 14, 21

United States v. John,
597 F.3d 263 (5th Cir. 2010) 8, 11

United States v. Kozminski,
487 U.S. 931 (1988) 20

United States v. Lowson,
No. 10-114, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) 21

United States v. Microsoft,
138 S. Ct. 1186 (2018) 15

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

United States v. Rodriguez,
628 F.3d 1258 (11th Cir. 2010) 5, 6, 7, 16

United States v. Stevens,
559 U.S. 460 (2010) 21

United States v. Swartz,
No. 1:11-cr-10260 (D. Mass. July 14, 2011) 20

United States v. Valle,
807 F.3d 508 (2d Cir. 2015) ..... *passim*

WEC Carolina Energy Sols. LLC v. Miller,
687 F.3d 199 (4th Cir. 2012) 9, 11

Yates v. United States,
135 S. Ct. 1074 (2015) 19

Statutes

6 U.S.C. § 482(b)(3)(A) 18

10 U.S.C. § 923(a)(1) 17

17 U.S.C. § 506(a)(1) 19

Computer Fraud and Abuse Act of 1986,
Pub. L. No. 99-474, 100 Stat. 1213 2

18 U.S.C. § 1030 ..... 1, 2, 5, 11

18 U.S.C. § 1030(a)(2) ..... *passim*

18 U.S.C. § 1030(a)(2)(C) 1

18 U.S.C. § 1030(c)(2)(A) 3
18 U.S.C. § 1030(c)(2)(B)(i) 3, 12
18 U.S.C. § 1030(e)(1) 13
18 U.S.C. § 1030(e)(6) 1, 3, 6, 16
18 U.S.C. § 1030(g) 3
18 U.S.C. § 1343 5
18 U.S.C. § 1346 5
18 U.S.C. § 1832 19
18 U.S.C. § 3237 14
28 U.S.C. § 1254(1) 1
38 U.S.C. § 5318(b) 18
42 U.S.C. § 1320d-6(a)(3) 19

Legislative Materials

H.R. Rep. No. 98-894 (1984) 2, 18
S. Rep. No. 99-432 (1986) 18

Other Authorities

Chandler, Adam, *One Worker's Fantasy: A March Madness Holiday*, The Atlantic (Mar. 20, 2015) 13

Kerr, Orin S., *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596 (2003) 14

Kerr, Orin S., *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010) 22

Mayer, Jonathan, *Cybercrime Litigation*, 164 U. Penn. L. Rev. 1453 (2016) 13, 14

Webster's New International Dictionary (2d ed. 1934) 16

Wu, Tim, *Fixing the Worst Law in Technology*, The New Yorker (Mar. 18, 2013) 21

PETITION FOR A WRIT OF CERTIORARI

Petitioner Nathan Van Buren respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Eleventh Circuit.

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Eleventh Circuit (Pet. App. 1a) is published at 940 F.3d 1192. The relevant order of the district court is unpublished.

JURISDICTION

The decision of the court of appeals was issued on October 10, 2019. Pet. App. 1a. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

RELEVANT STATUTORY PROVISIONS

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is reproduced in the appendix to this brief at Pet. App. 33a-46a.

STATEMENT OF THE CASE

The Computer Fraud and Abuse Act (CFAA) makes it a federal crime to "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). Under the Act, to "exceed[] authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6).

This case presents a recurring question about the interpretation of these provisions, on which the

courts of appeals are openly divided: Does a person obtain information on a computer that he is "not entitled so to obtain" when he has permission to access the information, but does so for an improper purpose? The answer to this question has sweeping implications. Every day, "millions of ordinary citizens" across the country use computers for work and for personal matters. *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (en banc). Accessing information on those computers is virtually always subject to conditions imposed by employers' policies, websites' terms of service, and other third-party restrictions. If, as some circuits hold, the CFAA effectively incorporates all of these limitations, then any trivial breach of such a condition—from checking sports scores at work to inflating one's height on a dating website—is a federal crime.

1. In 1984, Congress became concerned about "the activities of so-called 'hackers' who have been able to access (trespass into) both private and public computer systems." H.R. Rep. No. 98-894, at 10 (1984). To deter and punish this "new dimension of criminal activity," *id.*, Congress created a federal crime, codified at 18 U.S.C. § 1030. Two years later, Congress amended the statute, and it became known as the CFAA. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213. In the ensuing years, Congress amended the CFAA several more times, expanding both the types of information and the types of computers it covers.

The provision of the CFAA at issue here provides that "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information" from a "protected computer" commits a federal crime. 18 U.S.C.

§ 1030(a)(2). A "protected computer" is one "used in or affecting interstate or foreign commerce or communication"—in other words, any "computer[] with Internet access." *Nosal*, 676 F.3d at 859. As noted above, the phrase "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 accesser *is not entitled so to obtain* or alter." 18 U.S.C. § 1030(e)(6) (emphasis added).

Violations of Section 1030(a)(2) are punishable by a fine or imprisonment of one year, or both. 18 U.S.C. § 1030(c)(2)(A). That misdemeanor becomes a felony, punishable by imprisonment for up to five years, if "the offense was committed for purposes of commercial advantage or private financial gain." *Id.* § 1030(c)(2)(B)(i). The statute also contains a civil cause of action, allowing any person who suffers damage or loss because of a violation of the CFAA to sue for damages or equitable relief. *Id.* § 1030(g).

2. Petitioner was a police sergeant in Cumming, Georgia, a small town in the northern part of the state. Pet. App. 3a. As a result of patrolling the town over the years, petitioner knew a local man named Andrew Albo. *Id.* 3a. Albo "allegedly paid prostitutes to spend time with him" and then called the police to "accuse[] the women of stealing the money he gave them." *Id.* 4a. Claiming to fear retaliation from these women, he sometimes also asked officers to run searches of allegedly suspicious license plate tags. Tr. 409 (Oct. 25, 2017).

In the summer of 2015, petitioner was struggling with financial difficulties and asked Albo for a loan. Pet. App. 4a-5a. "Unbeknownst to [petitioner],

however, Albo recorded their conversations." *Id.* 3a-4a. Albo shared the recordings with the Forsyth County Sheriff's Office, which referred the matter to the Cumming Police Department, which in turn referred the matter to the FBI. U.S. C.A. Br. 4-5.

The FBI devised a sting operation "to test how far [petitioner] was willing to go for money." Pet. App. 4a. To set up the operation, the FBI invented a favor for Albo to request of petitioner in exchange for the loan. *Id.* 4a-5a. In particular, the FBI instructed Albo to ask petitioner to run a computer search for the supposed license plate number of a dancer at a local strip club. *Id.* It directed Albo to say that he liked her and wanted "to know if she was an undercover officer before he would pursue her further." *Id.* 5a.

Petitioner agreed to complete the search. When Albo gave him $5000 in return, petitioner "offered to pay Albo back, but Albo waved that off." Pet. App. 5a. Still, petitioner insisted, "I'm not charging for helping you out." *Id.* 25a. Several days later, Albo "followed up" with petitioner on the request, bringing him an additional $1000 and the "fake license plate number created by the FBI." *Id.* 5a.

After that meeting, petitioner accessed the Georgia Crime Information Center (GCIC) database, which contains license plate and vehicle registration information. Pet. App. 6a. As a law enforcement officer, petitioner was authorized to access this database "for law-enforcement purposes." *Id.* 28a. He ran a search for the license plate number that Albo had given him. He then texted Albo that he had information to provide. *Id.* 6a.

The next day, the FBI "arrived at [petitioner's] doorstep" and revealed that it had been tracking his interactions with Albo and believed petitioner had engaged in criminal activity. Pet. App. 6a.

3. The Government charged petitioner in the U.S. District Court for the Northern District of Georgia with "one count of felony computer fraud, in violation of 18 U.S.C. § 1030" and "one count of honest-services wire fraud, in violation of 18 U.S.C. §§ 1343 and 1346." Pet. App. 6a.

After the Government presented its case at trial, petitioner moved for a judgment of acquittal on the CFAA count. Petitioner argued that "accessing [information] for an improper or impermissible purpose does not exceed authorized access as meant by" Section 1030(a)(2). Tr. 391 (Oct. 25, 2017). The Government conceded in response that the circuits were "split" over that issue. *Id.* at 396-97. But it claimed that the Eleventh Circuit's decision in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), required the district court to reject petitioner's argument. As the Government explained, *Rodriguez* held that a defendant violates the CFAA not only when he obtains information that he has no "rightful[]" authorization whatsoever to acquire, but also when he obtains information "for a nonbusiness purpose." Tr. 396-97 (Oct. 25, 2017).

The district court denied petitioner's motion. Tr. 399 (Oct. 25, 2017). The jury then convicted on both counts. Pet. App. 6a. The district court sentenced petitioner on each count to eighteen months in prison, to be served concurrently. U.S. C.A. Br. 3.

4. The Eleventh Circuit affirmed petitioner's CFAA conviction, rejecting petitioner's argument that he was "innocent of computer fraud because he accessed only databases that he was authorized" to access. Pet. App. 26a-28a.[1] Like the Government in the district court, the Eleventh Circuit acknowledged that "other courts have rejected *Rodriguez*'s interpretation of 'exceeds authorized access.' " *Id.* at 27a. But the court of appeals declared itself bound by *Rodriguez*, barring "abrogation by the Supreme Court" or new precedent otherwise rendering the case defunct. *Id.* at 28a. Under *Rodriguez*, the Eleventh Circuit observed, it is enough that petitioner ran the tag search for "inappropriate reasons." *Id.* at 27a.

REASONS FOR GRANTING THE WRIT

The courts of appeals are openly divided four-to-three over whether a person with permission to access information on a computer violates the Computer Fraud and Abuse Act when he accesses that information for an improper purpose. This Court should use this case to resolve the conflict. This case squarely presents the issue, and the Eleventh Circuit's expansive construction of the CFAA is incorrect. The most natural reading of the CFAA is that a person "obtain[s] information in the computer that [he] is not entitled so to obtain," 18 U.S.C. § 1030(e)(6), only if he had no right at all to access the information. Reading the statute more broadly would criminalize ordinary computer use throughout

---

[1] For reasons not relevant here, the court of appeals also vacated petitioner's conviction for honest-services wire fraud. Pet. App. 8a-22a, 32a.

the country, thereby inviting arbitrary enforcement and flouting the principle that a federal criminal statute should not be construed to encompass a broad swath of everyday behavior unless the statute's text unambiguously demands that result.

I. The courts of appeals are intractably divided over the reach of the CFAA.

1. In this case, the Eleventh Circuit reaffirmed its view that a person violates Section 1030(a)(2) of the CFAA if he uses a computer to access information that he is otherwise authorized to access but does so for an improper purpose. The Eleventh Circuit first adopted that position in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), holding that a person with access to a computer for business reasons "exceed[s] his authorized access" whenever he "obtain[s] . . . information for a nonbusiness reason." Pet. App. 27a. The Eleventh Circuit asserted that "the plain language of the Act" requires this result. *Rodriguez*, 628 F.3d at 1263.

The Eleventh Circuit's interpretation of the CFAA accords with decisions by the First, Fifth, and Seventh Circuits. In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), the First Circuit concluded that a person "exceeds authorized access" when he uses information for purposes prohibited by a confidentiality agreement. The defendant there had "authorization . . . to navigate around EF's [public] [web]site." *Id.* at 583. But, in the First Circuit's view, he "exceeded that authorization" by his "wholesale use" of "proprietary information and know-how" to collect data from the website to aid a competitor's strategy. *Id.* at 582-83.

Agreeing with the First Circuit, the Fifth Circuit has concluded that the CFAA's prohibition against "exceed[ing] authorized access" includes "exceeding the *purposes* for which access is 'authorized.' " *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010), *cert. denied*, 568 U.S. 1163 (2013) (emphasis added). In other words, when a person is authorized to access information on a computer "for limited purposes," the Fifth Circuit holds that the person violates the CFAA by accessing the information for an unauthorized purpose. *Id.*; *see also Merritt Hawkins & Assocs., LLC v. Gresham*, 79 F. Supp. 3d 625 (N.D. Tex. 2015) (applying *John* to a civil defendant's breach of a confidentiality agreement with his employer).

The Seventh Circuit has also held that the CFAA is violated when a person accesses data on his work computer for a purpose that his employer prohibits. *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). As in the Eleventh, First, and Fifth Circuits, it is no defense in the Seventh Circuit that the person was entitled to obtain the information for certain purposes. *Id.* at 419-20.[2]

---

[2] The Seventh Circuit suggested that once an employee violates a purpose restriction, he breaches a duty of loyalty to his employer, which actually "terminate[s] his . . . authority to access" the computer at all. *Citrin*, 440 F.3d at 420-21. But this reasoning—whatever its merit—does not seem to apply to the initial violation of the purpose restriction that constitutes the breach. Accordingly, subsequent courts have treated the facts of *Citrin* itself as an "exceeds authorized access" case, rather than a "without authorization" case. *See, e.g.*, *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015); *United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) (en banc).

2. In contrast to the preceding four circuits, the Second, Fourth, and Ninth Circuits have each held that the CFAA's "exceeds authorized access" prong does not impose criminal liability on a person with permission to access information on a computer who accesses that information for an improper purpose. A person violates the CFAA in those circuits only if he accesses information on a computer that he is prohibited from accessing at all, for any reason.

The Ninth and Fourth Circuits adopted this position in nearly simultaneous decisions seven years ago. Declaring that it was "unpersuaded by the decisions of [its] sister circuits," the Ninth Circuit "decline[d] to follow" them. *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (en banc). The nine-judge majority reasoned that the text of Section 1030(a)(2) does not cover a person "who has unrestricted physical access to a computer, but is limited in the use to which he can put the information." *Id.* at 857, 862-63. The Ninth Circuit explained, moreover, that reading the CFAA to cover "use restrictions" and thereby to reach activities "routinely prohibited by many computer-use policies" would improperly turn "millions of ordinary citizens" into criminals. *Id.* at 860-63.

The Fourth Circuit likewise "reject[ed] an interpretation of the CFAA that imposes liability" when people have permission to access information on a computer but their "purpose in accessing the information [i]s contrary to company policies regulating use." *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 202, 207 (4th Cir. 2012) (internal quotation marks and citation omitted).

More recently, the Second Circuit adopted the same view of the CFAA in *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015). The defendant in that case was a New York City police officer who used a computer program to access the federal National Crime Information Center database, which he was authorized to access for his official duties. *Id.* at 512-13. He retrieved information about various personal acquaintances, in violation of the department's policies regarding proper use of the database. *Id.*

The Second Circuit noted that "six other circuits have wrestled with the question" whether "exceeds authorized access" is limited "to a scenario where a user has permission to access the computer but proceeds to . . . enter[] an area of the computer to which his authorization does not extend." *Valle*, 807 F.3d at 524. Rejecting the broader approach of "the First, Fifth, Seventh, and Eleventh Circuits," the Second Circuit "agree[d] with the Ninth and Fourth Circuits" that the CFAA is indeed limited to situations where the user does not have access for *any* purpose at all. *Id.* at 524, 527.

The Second Circuit reasoned that the "ordinary tools of legislative construction" do not resolve the issue; the language of the statute is "readily susceptible to different interpretations." *Valle*, 807 F.3d at 524, 526. The court therefore turned to "the rule of lenity," which requires courts to resolve ambiguity in criminal statutes by "adopt[ing] the interpretation that favors the defendant." *Id.* at 526. Stressing that the broader interpretation of the CFAA "would criminalize the conduct of millions of ordinary computer users," the Second Circuit rejected it. *Id.* at 527.

Several district courts in circuits that have not yet addressed the issue have also recognized the conflict and followed the approach taken by the Second, Fourth, and Ninth Circuits. *Teva Pharms. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 669-70 (E.D. Pa. 2018) (citing eight other district court decisions within the Third Circuit that have done the same); *Hedgeye Risk Mgmt., LLC v. Heldman*, 271 F. Supp. 3d 181, 194 (D.D.C. 2017); *Cloudpath Networks, Inc. v. SecureW2 B.V.*, 157 F. Supp. 3d 961, 983 (D. Colo. 2016); *Sebrite Agency, Inc. v. Platt*, 884 F. Supp. 2d. 912, 917-18 (D. Minn. 2012).

3. This issue has sufficiently percolated in the courts of appeals, and the split will not abate without this Court's intervention.

Opposing review of the Fifth Circuit's decision in *John*, the Government conceded that "[t]he circuits have disagreed about whether a person 'exceeds authorized access' of a protected computer, in violation of 18 U.S.C. 1030, when she has access to a computer system for certain legitimate purposes but then accesses the system for a prohibited purpose." Br. in Opp. at 7, *John v. United States*, 568 U.S. 1163 (2013) (No. 12-5201). But the Government maintained that "review of the reach of Section 1030 would be premature" because "the Fourth Circuit's decision in *WEC Carolina* and the Ninth Circuit's decision in *Nosal* [had been] issued within the last seven months." *Id.* at 13.

It has now been seven years, and there is an entrenched four-to-three split. The arguments on both sides of the conflict have now been fully vetted in various majority and dissenting opinions, and courts are just choosing sides. *See, e.g.*, *Teva*

Pharms., 291 F. Supp. 3d at 668-71 (laying out the conflict and siding with the Second, Fourth, and Ninth Circuits). Only this Court can establish a uniform meaning of the CFAA.

II. The question presented is extremely important.

For three reasons, it is critical that this Court resolve the conflict over the scope of the CFAA.

1. At its core, the question presented is whether the CFAA applies only to hacking and related activities or whether it extends to "whole categories of otherwise innocuous behavior." *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (en banc). Most people are not hackers. But most everyone who uses a computer (which is to say, most everyone) regularly runs up against conditions on accessing information on the computer—such as "corporate polic[ies] that computers can be used only for business purposes." *Id.*

For example, many law schools provide students with access to the Westlaw legal database for educational use only. But a student might use that access for personal purposes—perhaps to look up local housing laws to negotiate rent or to demand a refund of a security deposit. Whether this conduct constitutes a felony hinges on the answer to the question presented. *See* 18 U.S.C. § 1030(c)(2)(B)(i) (violations of the CFAA committed for "private financial gain" are punishable by five years in prison); *Nosal*, 676 F.3d at 860-62.

To take another example, every March, tens of millions of American workers participate in office

pools for the NCAA men's basketball tournament ("March Madness").[3] Such pools typically involve money stakes. When these employees use their company computers to generate their brackets or to check their standing in the pools, they likely violate their employers' computer policies. Again, the answer to the question presented determines whether these employees are guilty of a felony.

One could go on and on. The question whether such commonplace activities violate the CFAA should not be left unresolved. It is intolerable for a broad swath of conduct to be entirely innocent in parts of the country but to constitute a federal crime in others.[4]

2. The CFAA is also invoked frequently. The Government regularly brings criminal prosecutions under the CFAA. *See* Jonathan Mayer, *Cybercrime Litigation*, 164 U. Penn. L. Rev. 1453, 1474-76 (2016) (noting that "trial and appellate courts are increasingly addressing criminal issues under [the] CFAA"). And reported cases likely undercount the actual frequency of the statute's use. While many

---

[3] Adam Chandler, *One Worker's Fantasy: A March Madness National Holiday*, The Atlantic (Mar. 20, 2015), https://www.theatlantic.com/business/archive/2015/03/one-workers-fantasy-a-march-madness-national-holiday/388327/ (citing an estimate that 77.7 million workers will spend time on March Madness during work hours).

[4] Indeed, the question presented is critical not only for every computer user, but also for every user of a smartphone and many other internet-connected devices that "affect" interstate commerce and thus fall under the Act's broad definition of "computer." *See* 18 U.S.C. § 1030(e)(1).

criminal prosecutions under the CFAA result in convictions and appeals, even more end in pleas without any further proceedings. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1617 n.86 (2003).

On the civil side, businesses also often bring claims under the statute against employees and competitors. In fact, "[c]ivil cybercrime litigation has unambiguously exploded." Mayer, *supra* at 1472-73. Thus, the answer to the question presented will not only determine the scope of a federal criminal statute but will also bring important clarity for "commercial quarrels" that arise under the Act. *Id.* at 1481.

3. Uniformity in the law is particularly vital under the CFAA because of how the federal venue provision intersects with the statute.

Under federal law, a crime that is "begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237. In a CFAA case, therefore, venue is typically appropriate not only where the defendant resides but also wherever any computer server he accessed is located. And information that a person accesses on the internet can be stored on one or more servers located in different jurisdictions. Thus, venue in a single CFAA case can routinely be found in several districts around the country, often in different circuits. *See, e.g.*, *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (defendant lived in Missouri but was charged in California—where the website Myspace happened to have its server). This

phenomenon gives rise to a serious danger of forum shopping where, as here, some jurisdictions criminalize conduct that others do not.

The multiplicity of venue options not only raises the risk of forum shopping; it also raises fair notice concerns. Most computer users do not know, and cannot easily ascertain, the location of the servers they are using. Indeed, companies "frequently" transfer data among remote servers without warning or any "human intervention" at all. Br. for the United States at 43, *United States v. Microsoft*, 138 S. Ct. 1186 (2018) (No. 17-2). Therefore, at any given moment, a person using a computer in, say, New York, Virginia, or California has little way of knowing whether he may be committing a crime because he happens to be using a server located in Massachusetts, Texas, Illinois, or Georgia. As the Government itself recently argued in an analogous context, the application of federal law should not "depend on the happenstance of where the data is located at the precise moment when" someone accesses a provider's network. *Id.*

III. This case is the right vehicle for resolving the conflict.

This case is an excellent vehicle for resolving whether the CFAA covers using a computer for an unauthorized purpose. There is no question that, as a Georgia law enforcement official, petitioner had authorization to access the GCIC database. Pet. App. 28a. And petitioner accessed the database in exactly the same way he would have accessed it for a law enforcement purpose; there are no complicating factors like downloads, erasure, or corruption of data. *See* Pet. App. 6a, 28a.

The Eleventh Circuit was able to affirm petitioner's conviction only by applying its broad interpretation of "exceeds authorized access" under the CFAA. Pet. App. 26a-28a. If the Second, Fourth, and Ninth Circuits are correct that the CFAA does not reach violations of conditions placed on access, then petitioner's conviction must be reversed for insufficient evidence.

IV. The Eleventh Circuit's decision is incorrect.

The entrenched conflict over how to construe the CFAA provides ample reason to grant certiorari regardless of which circuits have the better reading of the statute. But the fact that the Eleventh Circuit's interpretation is wrong makes review all the more warranted here.

1. The Eleventh Circuit has pronounced that the CFAA's "plain language" reaches accessing information on a computer for an unauthorized purpose. *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010). But the Eleventh Circuit's textual reading is not the only "plausible" one, *United States v. Valle*, 807 F.3d 508, 523-24 (2d Cir. 2015)—or even the better one. The most natural reading of the CFAA does not cover conditions placed on otherwise authorized access to information on a computer.

The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The ordinary meaning of the word to "obtain" is "to acquire, in any way." And "entitle" means "to give a right." *Webster's New International Dictionary* (2d ed. 1934). In

common usage, then, whether a person is entitled to obtain information turns on whether he has the right to acquire the information *at all*, not on the purpose for his access.

As an illustration of this typical usage, individuals seeking loans often give banks access to their credit history to verify their eligibility for the loans. If a bank were to access that credit information for an improper purpose—such as marketing credit cards—an ordinary speaker would not say that the bank was not entitled *to obtain* the information. Rather, the speaker would say that the bank was entitled to obtain the information but misused it.

Translated to the CFAA, a person, such as petitioner, who has permission to access information on a database is "entitled" to "obtain" that information. That fact does not change if he accesses that information for an improper purpose. While such misuse might trigger some other form of liability, it does not violate the CFAA, which is concerned only with the entitlement to *obtain* information. A person violates the CFAA only if he has no right whatsoever to access that information—because, for instance, it resides in a separate password-protected file.

Indeed, where Congress wants to forbid access merely for an unauthorized purpose, it does so expressly. For instance, a separate computer-crime statute criminalizes "knowingly access[ing] a Government computer, *with an unauthorized purpose*, and by doing so obtain[ing] classified information." 10 U.S.C. § 923(a)(1) (emphasis added). Another federal statute requires safeguards to ensure that certain Social Security Administration information "is not used for unauthorized purposes."

38 U.S.C. § 5318(b). Yet another statute establishes procedures to ensure that homeland security information "is not used for an unauthorized purpose." 6 U.S.C. § 482(b)(3)(A).

If Congress had wanted the CFAA to criminalize accessing information on computers for unauthorized purposes, it would have simply said "without authorization or *for an unauthorized purpose*." That Congress did not do so is telling.

2. The CFAA's structure confirms the ordinary meaning of its text. Section 1030(a)(2) criminalizes accessing a computer "without authorization" or "exceed[ing] authorized access"—different but related terms. Accessing a computer "without authorization" refers to a scenario where a user lacks permission to access *any* information on the computer. The meaning of "exceeds authorized access" is complementary, referring to a distinct scenario in which a user has permission to access *some* information on the computer, but then accesses *other* information to which her authorization does not extend. *Nosal*, 676 F.3d at 858.

3. The Eleventh Circuit's broad reading of the CFAA also goes far beyond the statute's objective, which is to forbid computer hacking.

The CFAA is not an all-purpose statute covering any misdeed that occurs on a computer. Congress enacted the CFAA to address the problem of computer "hackers." H.R. Rep. No. 98-894, at 10. Congress thus consistently described "authorization" in terms of "computer files or data" that an individual has permission to "enter" and sought to forbid "trespass[ing]" into such computerized records. *See id.*; S. Rep. No. 99-432, at 6 (1986).

Interpreting the statute's prohibition against "exceeding authorized access" as limited to scenarios where the user is categorically forbidden from accessing particular information on the computer "maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate." *Nosal*, 676 F.3d at 858. The statute's "without authorization" prong applies to "outside hackers" (those who break into a computer they are not allowed to access at all) and its "exceeds authorized access" prong applies to "inside hackers" (those who have authorization to use a computer but obtain information they are not allowed to access). *Id.*

There is no reason to stretch the CFAA any further. Insofar as accessing information for an inappropriate purpose merits the imposition of criminal sanctions, other federal statutes prohibit such conduct. For example, 18 U.S.C. § 1832 criminalizes the theft of trade secrets. Many other criminal statutes similarly prohibit accessing or using information for improper purposes. *See, e.g.*, 17 U.S.C. § 506(a)(1) (prohibiting distribution of a copyrighted work); 42 U.S.C. § 1320d-6(a)(3) (prohibiting disclosure of individually identifiable health information). Misappropriating information on a computer can also subject people to state criminal laws and common-law contract and tort claims.

4. The dramatic consequences of the Eleventh Circuit's reading of the CFAA provide still further reason to reject that construction.

This Court has consistently refused to construe imprecisely worded federal statutes so expansively as to criminalize (and federalize) vast swaths of conduct. *See, e.g.*, *Yates v. United States*, 135 S. Ct. 1074,

1083 (2015); *Bond v. United States*, 134 S. Ct. 2077, 2091-92 (2014). It has been especially leery of doing so where, as here, such constructions would criminalize everyday conduct of ordinary people. In *United States v. Kozminski*, 487 U.S. 931 (1988), for instance, the Court held that the term "involuntary servitude" excludes "psychological coercion." *Id.* at 944. Otherwise, the Court reasoned, even the "parent who coerced an adult son or daughter into working in the family business by threatening withdrawal of affection" would commit a criminal act, as would the "political leader who uses charisma to induce others to work without pay." *Id.* at 949. Absent an explicit directive, a federal criminal statute does not reach such "a broad range of day-to-day activity," "subject[ing] individuals to the risk of arbitrary or discriminatory prosecution." *Id.* at 949, 952.

The Eleventh Circuit's interpretation of the CFAA would similarly reach commonplace activities of nearly all computer users, going far beyond the objectives of the statute. It would attach criminal liability to the multitude of private computer-use policies—policies "that most people are only dimly aware of and virtually no one reads or understands," *Nosal*, 676 F.3d at 861—and grant the Executive Branch virtually unfettered prosecutorial discretion.

The Government has responded that "whatever the scope of the CFAA, it won't prosecute minor violations." *Nosal*, 676 F.3d at 862; *see also United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015). That assurance appears questionable: Over the past decade, the Government has, in fact, brought cases against individuals who have violated companies' terms of service agreements. *See, e.g.*, Indictment, *United States v. Swartz*, No. 1:11-cr-10260 (D. Mass.

July 14, 2011), ECF No. 2 (violation of JSTOR terms of service); *United States v. Lowson*, No. 10-114, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (violation of Ticketmaster terms of service); *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (violation of Myspace terms of service). "The Justice Department has repeatedly taken the position that such violations are felonies." Tim Wu, *Fixing the Worst Law in Technology*, The New Yorker (Mar. 18, 2013). But even if the Government did, in fact, promise to forego pursuit of such minor CFAA violations, a free society should not be required to entrust its liberty to the grace of prosecutors. *See United States v. Stevens*, 559 U.S. 460, 480 (2010).

If there is any lingering doubt, the rule of lenity mandates that "when choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before [choosing] the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *United States v. Bass*, 404 U.S. 336, 347 (1971) (internal quotation marks and citation omitted). Here, the "ordinary tools of legislative construction fail to establish that the Government's position is unambiguously correct." *Valle*, 807 F.3d at 526. Moreover, any attempt to wrest an intermediate rule out of the CFAA that would cabin prosecutorial discretion—covering some instances of access for improper purposes but not others—would render the statute hopelessly vague. Crimes must be defined "with sufficient definiteness that ordinary people can understand what conduct is prohibited." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). And there is no textual footing in the CFAA to intelligibly criminalize only certain violations of terms of service, terms of

use, employer use policies, or other contract-based conditions of access. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1575-83 (2010).

Accordingly, if nothing else, time-honored principles of leniency and constitutional avoidance require adopting petitioner's more limited reading of the CFAA's "exceeds authorized access" prong.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

Saraliene Smith Durrett
SARALIENE SMITH DURRETT, LLC
1800 Peachtree Street
Suite 300
Atlanta, GA 30309

Rebecca Shepard
FEDERAL DEFENDER PROGRAM, INC.
101 Marietta Street NW
Suite 1500, Centennial Tower
Atlanta, GA 30303

Jeffrey L. Fisher
Counsel of Record
Pamela S. Karlan
Brian H. Fletcher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@stanford.edu

December 18, 2019