No. 19-783

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

BRIEF FOR PETITIONER

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 unauthorized purpose.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Statutes

Legislative Materials

Other Authorities

BRIEF FOR PETITIONER

Petitioner Nathan Van Buren respectfully requests that this Court reverse 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 The relevant district court order (transcribed at J.A. 37) is unpublished.

JURISDICTION

The decision of the court of appeals was issued on October 10, 2019. Pet. App. 1a. Petitioner filed a petition for writ of certiorari on December 18, 2019, which the Court granted on April 20, 2020. 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 at Pet. App. 33a-46a.

INTRODUCTION

In a recent series of cases, this Court has repeatedly rejected efforts to stretch the text of federal statutes in ways that would produce "sweeping expansion[s] of federal criminal jurisdiction." *Kelly v. United States*, 140 S. Ct. 1565, 1574 (2020) (quoting *Cleveland v. United States*, 531 U.S. 12, 24 (2000)); *see also Marinello v. United States*, 138 S. Ct. 1101 (2018); *McDonnell v. United States*, 136 S. Ct. 2355, 2372-73 (2016); *Yates v. United States*, 574 U.S. 528, 540 (2015); *Bond v. United States*, 572 U.S. 844, 862-65 (2014). The question presented here regarding the

scope of the Computer Fraud and Abuse Act (CFAA) raises this same concern once again.

Under the CFAA, a person engages in criminal activity whenever he "accesses a computer without authorization or exceeds authorized access, and thereby obtains information" from the computer. 18 U.S.C. § 1030(a)(2)(C). In 1986, Congress defined the key phrase at issue here—"exceeds authorized access"—to mean "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).

Does a person obtain information via computer that he is "not entitled so to obtain" when he has permission to access the information for certain purposes, but does so for an unauthorized purpose (or in contravention of some other stated limitation on its use)? The answer to this question has far-reaching implications. Every waking hour of 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 the CFAA effectively incorporates all of these stated limitations, then any breach of such a limitation—from checking sports scores at work to inflating one's height on a dating website—is a federal crime. *Id.* at 860-62.

Shrugging off these ramifications and ignoring the most natural reading of the pertinent text, the Eleventh Circuit has held that the CFAA does indeed cover obtaining information on computers in breach of

stated use restrictions. Pet. App. 27a-28a (reaffirming *United States v. Rodriguez,* 628 F.3d 1258, 1263 (11th Cir. 2010)). And in a now-familiar pattern, the Government tries to defend this all-embracing rule by promising that "whatever the scope of the CFAA, it won't prosecute minor violations" of the statute. *Nosal*, 676 F.3d at 862; *see also* BIO 16-17 (maintaining that "concerns about the potential breadth" of the CFAA are "ameliorate[d]" by the Department of Justice's current charging policy).

This Court should respond along the same lines it has many times before. Section 1030 was enacted to address a particular problem: unauthorized computer hacking. It was never meant to become a vehicle for enforcing private or public restrictions on the use of data—or to transform routine state-law violations of such use policies into federal felonies. And even if imprecise words in the statute offered some toehold for the Eleventh Circuit's sweeping alteration of the federal-state balance, the Court may not "construe a criminal statute on the assumption that the Government will 'use it responsibly.'" *Marinello*, 138 S. Ct. at 1109 (quoting *McDonnell*, 136 S. Ct. at 2372-73).

STATEMENT OF THE CASE

A. Legal background

1. In the 1980s, computers emerged as "an integral part of our everyday lives, critical to our national defense, financial transactions, and information transmissions." H.R. Rep. No. 98-894, at 8 (1984). With this growth of digital repositories for sensitive information, Congress became concerned about "the activities of so-called 'hackers.'" *Id.* at 10.

Existing legal regimes—from intellectual property statutes to the common law—already prohibited a wide range of individuals from misappropriating trade secrets or other confidential information, whether or not obtained from computers. *See, e.g.*, 18 U.S.C. § 1832(a); Restatement (Second) of Contracts § 346 (1981) (breach of contract). And criminal statutes prohibited the theft of paper documents or other tangible objects from physical repositories. *See* Francis Wharton & Charles E. Torcia, 3 *Wharton's Criminal Law* § 342 (14th ed. 1978). But "hackers" presented a "new dimension of criminal activity"—one that "d[id] not fit well into . . . traditional theft/larceny statutes." H.R. Rep. No. 98-894, at 8-9. These nefarious actors exploited the *digital* pathways of the new technological landscape to obtain sensitive information from governmental and private entities without ever having to breach any physical barriers. All they needed was a "local telephone" paired with a modem. *Id.* at 10.

For example, in a much-publicized event in 1983, a group of individuals known as the 414 Gang "broke into the computer system at Memorial Sloan-Kettering Cancer Center in New York." S. Rep. No. 99-432, at 2-3 (1986). They gained access to thousands of sensitive patient records and even "had at their fingertips the ability to alter the radiation treatment levels that each patient received." *Id.*

Congress realized that these types of hacking events could "cost[] the economy millions now and potentially billions in the future." H.R. Rep. No. 98-894, at 12. Worse yet, Congress believed that hackers threatened our national security. One industry expert told Congress in 1984 that the motion picture

WarGames, released the year before, "showed a realistic representation" of hackers' ability to access restricted computers from a distance. H.R. Rep. No. 98-894, at 10 (1984) (testimony of a representative from GTE Telenet, a telecom company later acquired by Sprint). In the popular film, a tech-savvy teenager living in Seattle hacked into the mainframe computer of the North American Aerospace Defense Command (NORAD), nearly causing a nuclear war with the Soviet Union. The same film also caught President Reagan's attention, setting off "a string of interagency memos, working groups, studies, and meetings." Fred Kaplan, *Dark Territory: The Secret History of Cyber War* 1-2 (2016); *see also* Fred Kaplan, *'WarGames' and Cybersecurity's Debt to a Hollywood Hack*, N.Y. Times, Feb. 19, 2016.

2. Soon after, Congress enacted a new federal computer crime statute as part of an omnibus crime bill. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102, 98 Stat. 2190 (1984). The new statute covered only three types of digitized information: information protected "for reasons of national defense or foreign relations," codified at 18 U.S.C. § 1030(a)(1); information "contained in a financial record of a financial institution," codified at § 1030(a)(2); and information on a computer "used by or on behalf of the Government of the United States," codified at § 1030(a)(3). § 2102, 98 Stat. at 2190-91. An individual violated the statute if he obtained covered information by "knowingly access[ing] a computer without authorization, or having accessed a computer with authorization, us[ed] the opportunity such access provides for purposes to which such authorization d[id] not extend." *Id.*

In subsequent years, Congress amended these provisions, and the statute became known as the Computer Fraud and Abuse Act. *See* Pub. L. No. 99-474, § 1, 100 Stat. 1213 (1986) (conferring this title). Among other things, Congress expanded the statute's coverage beyond financial records, national security information, and government computers. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1566-69 (2010) (discussing amendments). Since 1996, the statute's anti-hacking prohibition has covered any type of information at all, accessed via any "computer . . . used in or affecting interstate or foreign commerce or communication." 18 U.S.C. §§ 1030(e)(1) & (2)(B); *see also* Kerr, *supra*, at 1566-68. This means the statute covers, at the very least, "all computers with Internet access." *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (en banc); *see also* 18 U.S.C. § 1030(e)(1) (defining "computer" to encompass smartphones and other "high speed data processing device[s]").

At the same time, Congress rejected calls to turn the CFAA into "as sweeping a Federal statute as possible." S. Rep. No. 99-432, at 4 (1986). In 1986, Congress cabined the *acts reus* element of Section 1030(a)(2), eliminating the language about accessing a computer with authorization "for purposes to which such authorization does not extend." § 2, 100 Stat. at 1213, 1215. Since then, the CFAA has provided that "[w]hoever intentionally accesses a computer without authorization or *exceeds authorized access*, and thereby obtains information" from a computer commits a federal crime. 18 U.S.C. § 1030(a)(2) (emphasis added). In the provision most directly at issue here, the statute defines the phrase "exceeds authorized access" to mean "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).

Violations of the CFAA are punishable, at a minimum, by a fine or imprisonment of up to one year, or both. 18 U.S.C. § 1030(c)(2)(A). If "the offense was committed for purposes of commercial advantage or private financial gain," the offense becomes a felony punishable by imprisonment for up to five years. *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).

3. For years following its enactment, the CFAA was sparingly invoked in litigation. But, in the early 2000s, private parties and the Government began asserting more claims under the statute—especially under the "exceeds authorized access" prong.

The first courts of appeals to confront such lawsuits interpreted Section 1030(a)(2)'s "exceeds authorized access" prong broadly. Allowing claims in employment disputes to go forward, the First and Seventh Circuits held that an individual violates the CFAA if he accesses information on a computer that he is authorized to obtain for certain purposes but does so for an unauthorized purpose. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). Shortly thereafter, the Fifth Circuit took the same approach in a criminal case, concluding that when a person is authorized to access information "for limited purposes," he "exceeds authorized access" when he "exceed[s] *the purposes* for which access is authorized." *United States v. John*, 597

F.3d 263, 272 (5th Cir. 2010) (emphasis added). Later that year, the Eleventh Circuit agreed. *See United States v. Rodriguez,* 628 F.3d 1258, 1263 (11th Cir. 2010).

More recently, however, a new chorus of courts has broken from this expansive interpretation. The trigger was an en banc decision in 2012 from the Ninth Circuit. Voting nine-to-two, that court observed that whatever "exceeds authorized access" might mean in a vacuum, the Eleventh Circuit's broad interpretation is a "poor fit with the statutory language" that actually defines that phrase. *United States v. Nosal*, 676 F.3d 854, 856-57 (9th Cir. 2012) (en banc). That language, the Ninth Circuit explained, prohibits obtaining information via computer that a person "is not entitled so to obtain or alter," 18 U.S.C. § 1030(e)(6)—not mere "misuse or misappropriation." *Id.* at 863 (citation omitted). The Ninth Circuit also pointed out that the Eleventh Circuit's construction of the CFAA "transform[s] whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id.* at 860. Computer use policies and website terms of service forbid all sorts of things—from using a work computer to "chat[] with friends, play[] games, shop[] or watch[] sports highlights" to violating age or veracity restrictions on Facebook, eBay, or "dating websites." *Id.* at 860-62. In the Ninth Circuit's view, if Congress had intended to reach "far beyond computer hacking" to criminalize "everyone who uses a computer in violation of computer use restrictions," it would have spoken "more clearly." *Id.* at 857, 859, 863.

The two courts of appeals to consider the issue since *Nosal* have agreed with the Ninth Circuit's

analysis. *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 202, 207 (4th Cir. 2012); *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015). So have at least eighteen district court judges in circuits that have not yet addressed the question presented.[1]

---

[1] *See, e.g.*, *Sandvig v. Barr*, No. 16-1368, 2020 WL 1494065, at *8-10 (D.D.C. Mar. 27, 2020) (Bates, J.); *Integrated Process Sols., Inc. v. Lanix LLC*, No. 19-CV-567 (NEB/LIB), 2019 WL 1238835, at *5-6 (D. Minn. Mar. 18, 2019) (Brasel, J.); *Crabar/GBF, Inc. v. Wright*, No. 8:16-CV-537, 2019 WL 4016122, at *13-14 (D. Neb. Aug. 26, 2019) (Gerrard, J.); *GPMM, Inc. v. Tharp*, No. 8:19-CV-128, 2019 WL 7161229, at *4-6 (D. Neb. Oct. 3, 2019) (Buescher, J.); *Teva Pharms. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 669-70 (E.D. Pa. 2018) (Savage, J.); *Mathey Dearman, Inc. v. H&M Pipe Beveling Mach. Co.*, No. 18-cv-250-GKF-JFJ, 2018 WL 4224897, at *5 (N.D. Okla. Sept. 5, 2018) (Frizzell, J.); *Hedgeye Risk Mgmt., LLC v. Heldman*, 271 F. Supp. 3d 181, 194 (D.D.C. 2017) (Moss, J.); *Brand Energy & Infrastructure Servs., Inc. v. Irex Contracting Grp.*, Civ. A. No. 16-2499, 2017 WL 1105648, at *14 (E.D. Pa. Mar. 24, 2017) (Stengel, J.); *Kappe Assocs., Inc. v. Chesapeake Environ. Equip.*, LLC, No. 5:15-cv-02211-JFL, 2016 WL 1257665, at *8 (E.D. Pa. Mar. 31, 2016) (Leeson, J.); *Econ. Research Servs., Inc. v. Resolution Econ., LLC*, 208 F. Supp. 3d 219, 232 (D.D.C. 2016) (Leon, J.); *TripleTree, LLC v. Walcker*, No. 16-609 (DSD/TNL), 2016 WL 2621954, at *3-4 (D. Minn. May 6, 2016) (Doty, J.); *Cloudpath Networks, Inc. v. SecureW2 B.V.*, 157 F. Supp. 3d 961, 983 (D. Colo. 2016) (Martinez, J.); *Cent. Bank & Tr. v. Smith*, 215 F. Supp. 3d 1226, 1231-32 (D. Wyo. 2016) (Johnson, J.); *Tank Connection, LLC v. Haight*, 161 F. Supp. 3d 957, 969-70 (D. Kan. 2016) (Marten, J.); *Giles Constr., LLC v. Tooele Inventory Sol., Inc.*, No. 2:12–cv–37, 2015 WL 3755863, at *2–3 (D. Utah June 16, 2015) (Shelby, J.); *Roe v. Bernabei & Wachtel PLLC*, 85 F. Supp. 3d 89, 103 (D.D.C. 2015) (Chutkan, J.); *Experian Mktg. Sols., Inc. v. Lehman*, No. 1:15-CV-476, 2015 WL 5714541, at *4-5 (W.D. Mich. Sept. 29, 2015) (Bell, J.); *Dresser–Rand Co. v. Jones*, 957 F. Supp. 2d 610, 616–19 (E.D. Pa. 2013) (Brody, J.); *Sebrite Agency, Inc. v. Platt*, 884 F. Supp. 2d 912, 917-18 (D. Minn. 2012) (Schiltz, J.).

B. Facts and procedural history

1. After spending time in the military and serving as a police officer another city, petitioner Nathan Van Buren became a police officer in his hometown of Cumming, Georgia. Tr. 110 (Oct. 23, 2017). Several years later, in the course of his service, petitioner came to know Andrew Albo. Albo was a wealthy man who would sometimes call the Cumming Police Department and report that young women whom he had invited back to his home had stolen money from him. Pet. App. 4a. In truth, it seems that Albo may have had a habit of "pa[ying] prostitutes to spend time with him" and then wrongly "accus[ing] the women of stealing the money he gave them." *Id.* In any case, as petitioner periodically responded to these calls, he developed a familiarity and rapport with Albo.

In the summer 2015, petitioner told Albo that he was struggling with financial difficulties and asked for a loan. Pet. App. 4a. Albo agreed. But "unbeknownst to [petitioner, Albo] recorded their conversations." *Id.* Albo then shared the recordings with the Forsyth County Sheriff's Office. *Id.* The Sheriff's Office 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 consulted with the local U.S. Attorney's Office about various favors that Albo might request of petitioner in exchange for the loan. *Id.* 4a-5a; *see also* Tr. 274-75 (Oct. 24, 2017). The record does not catalog all of the "different scenarios," Tr. 274, that the FBI considered or implemented. In one scenario, the FBI instructed Albo to ask if

petitioner would be willing to move drugs for Albo's friends in New York. *Id.* at 297-98. But the FBI was unable to draw petitioner into any drug trafficking scheme. Tr. 370 (Oct. 25, 2017).

As part of a separate attempt to entice petitioner to violate the law, the FBI instructed Albo to ask petitioner to run a computer search for a license plate number. Pet. App. 4a-5a. The FBI directed Albo to say that he had met a dancer at a local strip club that he liked and wanted "to know if she was an undercover officer before he would pursue her further." *Id.* 5a. Petitioner agreed to search a law enforcement database for the dancer's supposed license plate number. *Id.* 5a-6a.

On the FBI's instructions, Albo gave petitioner $5000 in connection with his agreeing to conduct the search. Pet. App. 5a. Petitioner said he would "pay Albo back, but Albo waved that off." *Id.* 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 a database maintained by the Georgia Crime Information Center (GCIC) that contains license plate and vehicle registration information. Pet. App. 6a. Officers with access to the database receive training materials that describe "proper and improper use of the GCIC system." J.A. 12; *see also id.* 16-17, 20. These materials state that officers are allowed to use the GCIC only "for law-enforcement purposes," Pet. App. 28a, and forbid "[a]ny personal use" of the database. J.A. 17. After entering his username and password into the

laptop installed in his police car, petitioner ran a search for the license plate number that Albo had given him. *Id.* 8, 16. He then texted Albo that he had information to provide. Pet. App. 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.

2. As relevant here, 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." Pet. App. 6a.[2]

After the Government presented its case at trial, petitioner moved for a judgment of acquittal. *See* J.A. 35. Petitioner argued that "accessing [information] for an improper or impermissible purpose does not exceed authorized access" under Section 1030(a)(2). J.A. 36. The Government conceded in response that the circuits were "split" over that issue. *Id.* But it asserted that the Eleventh Circuit's decision in *Rodriguez* required the district court to reject petitioner's argument. As the Government put it, *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

---

[2] The Government also alleged that petitioner's license-plate interaction with Albo constituted "wire fraud, in violation of 18 U.S.C. §§ 1343 and 1346." Pet. App. 6a. The jury found him guilty of that charge, but for reasons not relevant here, the court of appeals vacated petitioner's conviction on that count. *Id.* 8a-22a, 32a. Further proceedings on that count are stayed pending this Court's disposition of this case. *See* J.A. 5.

obtains information "for a nonbusiness purpose." J.A. 37. The district court denied petitioner's motion. *Id.*

During closing arguments, the Government again maintained that petitioner "exceeded his authorized access" to that database because he accessed it "for a nonlaw enforcement purpose." J.A. 39; *see also* Tr. 515 (Oct. 26, 2017). To drive the point home, the prosecutor explained to the jury:

> Many of you work on computers in your own jobs. You have access to computers to do your job. If you go on the computer and access personal information and provide it to someone else, you've exceeded your authority.
>
> *You're allowed to be on the network, but once you're using the network that's against what your job or policy prohibits, you've exceeded your access.* You've gone too far, and *this is the concept that this defendant violated*. He violated this federal law when he ran that tag query for his own personal benefit and for a nonlaw enforcement purpose.

J.A. 39 (emphasis added).

The jury found petitioner guilty of violating the CFAA, and the district court sentenced him on that count to eighteen months in prison. U.S. C.A. Br. 3.

3. The Eleventh Circuit affirmed petitioner's CFAA conviction. As relevant here, petitioner renewed his argument that the evidence was insufficient to convict "because he accessed only databases that he was authorized to use, even though he did so for an inappropriate reason." Pet. App. 27a. But the court of

appeals rejected that argument. The Eleventh Circuit acknowledged that other courts have rejected its holding in *Rodriguez* that "misusing" a database a person is entitled to access violates the CFAA. *Id.* 27a-28a. But the Eleventh Circuit explained that it was bound by that holding. *Id.*; *see also EarthCam, Inc. v. OxBlue Corp.*, 703 Fed. App'x 803, 808 n.2 (11th Cir. 2017) (acknowledging that it "decided *Rodriguez* in 2010 without the benefit of [the subsequent] national discourse on the CFAA," but declaring itself "bound by *Rodriguez*"). Because petitioner ran the tag search for "inappropriate reasons," he violated the Eleventh Circuit's conception of the CFAA. Pet. App. 27a-28a.

4. This Court granted certiorari. 140 S. Ct. ___ (2020).

SUMMARY OF THE ARGUMENT

The CFAA's "exceeds authorized access" prong criminalizes accessing information via computer only when a person has no right at all to access the information.

I. 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 most natural reading of the words "not entitled so to obtain or alter" excludes misuse or misappropriation of information. Indeed, when Congress has sought to forbid obtaining information for an unauthorized purpose, it has done so directly and expressly.

II. Construing the CFAA to criminalize accessing information via computer only where an individual is not entitled for any purpose to access that information

aligns with the statute's limited objective. The CFAA is aimed at the problem of breaking into computers without permission. Such "hacking" occurs only when someone accesses information that he has no right at all to obtain. Congress had no reason to reach further, given that state law and certain federal statutes already cover various forms of unauthorized use of information.

III. The Eleventh Circuit's expansive interpretation of the CFAA is all the more flawed because it would transform everyday activities into federal crimes. Whenever people go online at work or at home, their computer use is subject to conditions imposed by employers' policies, websites' terms of service, and other third-party restrictions. As the Government itself has stressed in this very case, the Eleventh Circuit's interpretation of "exceeds authorized access" effectively incorporates all of these stated limitations into the CFAA—turning everything from filling out an NCAA tournament bracket while at work to posting an item on the wrong category on Craigslist into a felony. At least absent far more direct and unambiguous instructions from Congress, this Court should not read a federal statute to criminalize such daily activities of millions of ordinary Americans.

IV. Finally, this Court should reject the Eleventh Circuit's all-encompassing construction of the CFAA because it would violate two time-honored principles of judicial restraint. First, construing the CFAA to incorporate use limitations on computer files and websites' terms of service would raise serious constitutional questions—particularly under the void-for-vagueness doctrine and the First Amendment. Second, the Eleventh Circuit's construction would run

afoul of the rule of lenity. The CFAA was written roughly thirty-five years ago—before the advent of the internet, the explosion of personal computing devices, and the seamless interconnection of our personal, financial, and professional lives online. The statute at some point may warrant updating. But any such recalibration or expansion should come from Congress, not this Court. That way, the people are assured of having fair notice of potential criminal liability, and the populace will not have to depend on ongoing prosecutorial grace for their liberty.

ARGUMENT

The CFAA provides two complementary prohibitions that work in tandem to address computer hacking crimes. The statute's core provision prohibits accessing a computer "without authorization." 18 U.S.C. § 1030(a)(2). This prohibition covers outsiders who break into computers. *See, e.g.*, *United States v. Nosal*, 676 F.3d. 854, 858 (9th Cir. 2012) (en banc). To ensure comprehensive coverage, the statute also includes a second prohibition targeting "inside hackers," *id.*—individuals who, as Congress put it, "exceed [their] authorized access" to a computer. 18 U.S.C. § 1030(a)(2).

This case concerns only the latter prong of the CFAA. All agree that petitioner "ha[d] access" to the GCIC database for law-enforcement purposes. J.A. 39; *see also* Pet. App. 27a-28a. The Government, therefore, has claimed only that "petitioner exceeded his authorized access" to the GCIC database. BIO 6; *see also* J.A. 39. The Eleventh Circuit accepted that claim, holding that an individual violates this prong of the CFAA whenever he "misus[es] a database [he] lawfully can access." Pet. App. 28a. That startlingly

broad reading of the CFAA contravenes the statute's text and purpose and raises a bevy of practical and legal problems. This Court should reject it.

I. The most natural reading of the CFAA criminalizes obtaining information via computer only if an individual is not entitled to access that information for any purpose.

In *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), the Eleventh Circuit declared that the "plain language" of the CFAA reaches accessing information on a computer for an unauthorized purpose. *Id.* at 1263. But, as several courts of appeals and district courts have since explained, the Eleventh Circuit's construction of the CFAA's "exceeds authorized access" prong is not the only "plausible" one, or even a persuasive one. *United States v. Valle*, 807 F.3d 508, 523-24 (2d Cir. 2015); *see supra* at 10-11 (citing post-*Rodriguez* cases). The best reading of the provision is that it criminalizes accessing information only when a person has no right at all to access the information because, for instance, it resides in a password-protected file that is separate from the part of the computer the person is entitled to access. The provision does not reach simple misuse or misappropriation of information.

1. 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). This definition pivots on the meaning of the phrase "not entitled so to obtain"—in particular, on the meaning of the words "entitled" and "obtain."

The ordinary meaning of the word "entitle" is "to give a right." Webster's New International Dictionary (2d ed. 1934). The word "obtain" means "to acquire." *Id.* A person is thus "entitled so to obtain" information when she has the right, via some prescribed manner, to acquire that information.

An illustration fleshes out the typical usage of these terms, taken together. Individuals seeking loans often give banks the right to evaluate their creditworthiness by procuring credit history reports from credit-rating agencies. Banks, therefore, are entitled so to obtain such reports. If a loan officer were to access an applicant's credit history for an unauthorized purpose—for example, to figure out additional services the bank might market to the applicant—an ordinary speaker might say that the loan officer acquired that information from the credit-reporting agency for an inappropriate reason. But an ordinary speaker still would *not* say that the loan officer was *not entitled so to obtain* the information.

Translated to the CFAA, a person, such as petitioner, who has permission to use a computer to access a database is "entitled so to obtain" the information in that database. He has the right to acquire the information. And he has the right "so" to obtain it. That is, he has the right to acquire the information in the manner described in the statute—via computer—as opposed to via some other method, such as by calling on the phone or procuring hard copies of records from the warehouse where they are stored.

This analysis does not change if the person accesses the information for an unauthorized purpose (or otherwise in contravention of a stated limitation on

its use). While such "misuse or misappropriation" may well trigger some other form of adverse consequence or liability (typically under state contract or tort law), it does not violate the CFAA. *Nosal*, 676 F.3d at 863 (citation omitted); *see also, e.g.*, *Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (construing the CFAA to "encompass an employee's misuse or misappropriation of information . . . would depart from the plain meaning of the statute"). The statute is concerned only with the right to obtain information from a protected computer at all. *Id.*

2. The limited reach of the phrase "not entitled so to obtain" is reinforced by the fact that where Congress wants to forbid access for an unauthorized purpose, it does so expressly. For instance, a separate federal statute criminalizes "obtain[ing] classified information" by "knowingly access[ing] a Government computer, *with an unauthorized purpose*." 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." Or Congress would have defined "exceeds authorized access" as obtaining or altering information "for an unauthorized purpose." But Congress did neither of those things. Instead, it defined "exceeds authorized

access" to mean "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 Eleventh Circuit has offered no reason—and none is apparent—why Congress would have used such "convoluted" language to codify a basic legal concept (unauthorized purpose) that it has expressed in plain terms elsewhere in the U.S. Code. *Barton v. Barr*, 140 S. Ct. 1442, 1453 (2020); *see also, e.g.*, *Burgess v. United States*, 553 U.S. 124, 130-31 (2008).

Indeed, a short-lived version of the statute that later became the CFAA contained the "unauthorized purpose" concept that the Eleventh Circuit has taken the statute to cover. As originally enacted, an individual violated Section 1030(a)(2) when, "having accessed a computer with authorization," the individual "use[d] the opportunity such access provides *for purposes to which such authorization does not extend*." Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, Tit. II, § 2102(a), 98 Stat. 2190, 2190-91 (1984) (emphasis added). But Congress removed that language in the 1986 amendments to the Act and replaced it with the current definition of "exceeds authorized access." Pub. L. No. 99-474, § 2, 100 Stat. 1213, 1215 (1986); *see also* S. Rep. 99-432, at 9 (1986). As this Court has stressed on other occasions, it should not "read back into [a statute] the very . . . statutory language that [Congress] discarded in favor of other language."

Chickasaw Nation v. United States, 534 U.S. 84, 93 (2001) (internal quotation marks omitted).[3]

3. The Eleventh Circuit has never disagreed with petitioner's straightforward textual analysis of what it means to acquire information via computer that one is "not entitled so to obtain." Indeed, the Eleventh Circuit has never even engaged with that statutory language at all. Instead, the Eleventh Circuit in *Rodriguez* focused solely on what it perceived to be the ordinary meaning of the CFAA's phrase "exceeds authorized access." *See* 628 F.3d at 1263.

This was a mistake. It is hornbook law that courts should look to the ordinary meaning of statutory terms only when the terms are not specifically defined. "When a legislature defines the language it uses, its definition is binding upon the court," regardless of what the "ordinary meaning" of the defined phrase may be. 1A Sutherland Statutory Construction § 20:8 (7th ed. 2019); *see also* Antonin Scalia & Brian Garner, *Reading Law: The Interpretation of Legal Texts* 226

---

[3] Citing legislative history, the Government has previously argued that Congress removed the unauthorized-purpose language from the CFAA merely "to simplify the language" of Section 1030(a)(2). U.S. Br. at 19, *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015) (No. 14-4396) (quoting S. Rep. 99-432 at 9). The Senate Report that the Government cites, however, elsewhere praises the 1986 amendment as "refocus[ing] the legislation on its principal objects" and describes the deletion of the very same "purposes" language from an analogous provision as "remov[ing] from the sweep of the statute one of the murkier grounds of liability." S. Rep. 99-432, at 20-21. At any rate, these dueling pieces of the legislative history are ultimately immaterial. By its plain language, the revision clearly worked a substantive change. *See, e.g.*, *Milner v. Dep't of Navy*, 562 U.S. 562, 572 (2011) (refusing to "allow[] ambiguous legislative history to muddy clear statutory language").

(1st ed. 2012) ("[When] a definitional section says that a word 'means' something, the clear import is that this is its *only* meaning.").

Accordingly, this Court has held time and again that "[w]hen a statute includes an explicit definition, we must follow that definition." *Stenberg v. Carhart*, 530 U.S. 914, 942 (2000); *see also, e.g.*, *Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 162 n.18 (2012); *Burgess*, 553 U.S. at 126-27; *Meese v. Keene*, 481 U.S. 465, 484–85 (1987); *Western Union Telegraph Co. v. Lenroot*, 323 U.S. 490, 502 (1945). "In such circumstances definition by the average man or even by the ordinary dictionary with its studied enumeration of subtle shades of meaning is not a substitute for the definition set before us by the lawmakers." *Fox v. Standard Oil Co.*, 294 U.S. 87, 96 (1935) (Cardozo, J.).

To take but one example: In *Burgess*, the Court considered whether a statute requiring a sentencing enhancement when the defendant has been previously convicted of a "felony drug offense" covered a prior conviction for something classified, under state law, as a "misdemeanor." 553 U.S. at 126. The Court did not contemplate the ordinary meaning of the phrase "felony drug offense"—or even whether a misdemeanor can somehow be a felony. Instead, the Court simply observed that the statute "define[d] the precise phrase" "felony drug offense" to constitute *any* offense punishable by more than one year. *Id.* at 129-30. Finding that definition "coherent, complete, and by all signs exclusive," the Court held that the defendant's prior misdemeanor conviction qualified as a "felony drug offense" because it was punishable by more than one year. *Id.* at 129, 135.

The same principle of statutory construction applies here as well. Because the CFAA defines "exceeds authorized access," it does not matter how that phrase might be best understood in a vacuum. The CFAA's statutory definition controls—most notably, the phrase "not entitled so to obtain." And the best reading of that definition excludes acting for an unauthorized purpose.

II. Stretching the CFAA to cover obtaining information for an unauthorized purpose would go far beyond the statute's limited objective.

The Eleventh Circuit's broad interpretation of the CFAA also loses sight of the statute's limited purpose.

1. The CFAA is not an all-purpose statute covering any misdeed that occurs on a computer. The relevant language in the statute was written in 1984 and 1986 to address a specific phenomenon—the emergence of "a new type of criminal" who exploits vulnerabilities in computer networking to access information stored in restricted computer files. S. Rep. No. 99-432, at 2 (1986). Responding to this concern, Congress enacted the CFAA to target such computer "hackers"—individuals who invade computer files without permission. H.R. Rep. No. 98-894, at 10 (1984); *see also supra* at 5-7 (additional drafting history).

Consistent with the CFAA's anti-hacking focus, the drafters repeatedly framed the key issue in terms of whether an individual has permission to "enter" computer files or data. S. Rep. No. 99-432, at 21; *accord* H.R. Rep. No. 98-894, at 10. The legislation sought to forbid "breaking and entering" into computerized records. H.R. Rep. No. 98-894, at 20 (1984); *see also* S. Rep. No. 99-432, at 9 (targeting those who "break into [a] computer system"). And to

ensure that hackers do not escape punishment merely because they are entitled to access certain files or programs on a computer system containing many different types of information, Congress drafted the CFAA to cover not just "outside hackers," but also "inside hackers." *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012) (en banc).

"Inside" hacking can arise when an employee is allowed to access certain types of company data but "enter[s] another computer file" beyond those that she is "authorized to sign onto and use." S. Rep. No. 99-432, at 6. For instance, a company might issue login credentials to an in-house accountant that give her access to a database containing customer accounts. But the company might wish to limit the accountant's access to other sensitive information not relevant to her job—information such as employees' social security numbers and tax records, executive succession plans, results of internal investigations into discrimination or harassment complaints, or confidential plans for the research and development of new products. The company, therefore, might categorically forbid the accountant from viewing those other databases. If the accountant were nevertheless to access one of those databases—perhaps by stealing a co-worker's password to circumvent the technological firewall ordinarily blocking her ability to view them—then she would "exceed[her] authorized access" under Section 1030(a)(2)C).

But that is as far as the statute goes. Nothing suggests the CFAA is intended to reach people who are authorized to obtain information on a computer for certain purposes but do so for an unauthorized purpose. If, for example, the accountant discussed

above were to use her access to the customer-accounts database to find out whether a particular client likes to dine at Italian restaurants while traveling—because she has designs of asking him out on a date—she might well transgress a company use restriction. But she would not obtain information she is "not entitled so to obtain," 18 U.S.C. § 1030(e)(6)—and, therefore, would not violate the CFAA.

2. Other features of the legal landscape confirm that it would be inappropriate to stretch the CFAA to cover conduct beyond prohibiting breaking into computers without permission.

"Employer-employee and company-consumer relationships are traditionally governed by tort and contract law." *Nosal*, 676 F.3d at 860. And misappropriating information on a computer can subject individuals to various state common-law claims, as well as state statutory misappropriation claims. *See, e.g.*, *Viking Grp., Inc. v. Bruckman*, No. 347778, 2020 WL 2296903 (Mich. Ct. App. May 7, 2020) (breach of contract); *Shamrock Chi. Corp. v. Wroblewski*, No. 1-18-2354, 2019 WL 7373359 (Ill. Ct. App. Dec. 31, 2019) (common-law misappropriation); *Erlich Prot. Sys., Inc. v. Flint*, No. 345323, 2019 WL 5851938 (Mich. Ct. App. Nov. 7, 2019) (statutory misappropriation); *Applied Gen. Agency, Inc. v. Greenleaf Fin. & Ins. Servs., Inc.*, No. G055737, 2019 WL 5255271 (Cal. Ct. App. Oct. 17, 2019) (statutory misappropriation, common-law misappropriation, breach of contract, and tortious interference); *KNC Techs., LLC v. Tutton*, No. 19 CVS 793, 2019 WL 6219035 (N.C. Super. Ct. Oct. 9, 2019) (common-law misappropriation, breach of contract, and tortious interference).

Insofar as accessing information for an inappropriate purpose merits the imposition of federal criminal sanctions, statutes besides the CFAA have long prohibited such conduct. For example, 18 U.S.C. § 1832 criminalizes the theft of trade secrets. Many other criminal statutes similarly forbid accessing or using information for improper purposes. *See, e.g.*, 17 U.S.C. § 506(a)(1) (prohibiting unauthorized distribution of a copyrighted work); 42 U.S.C. § 1320d-6(a)(3) (prohibiting disclosure of individually identifiable health information).

In light of these other prescriptions, there is no good reason to "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Nosal*, 676 F.3d at 857. "[I]n the absence of a clear statement by Congress," a court should not construe a federal criminal statute to cover "a wide range of conduct typically regulated by state and local authorities." *Cleveland v. United States*, 531 U.S. 12, 24 (2000); *accord Bond v. United States*, 572 U.S. 844, 862-65 (2014). Furthermore, Congress has specified in other statutes the particular situations in which it believes that misappropriating information implicates federal law enforcement interests. When it comes to using information for an unauthorized purpose (whether obtained from a computer, or otherwise), the CFAA has no proper role to play.

III. The Eleventh Circuit's expansive construction of the statute would produce improbable consequences.

The Eleventh Circuit's interpretation of the CFAA is flawed for yet another reason: It would extend the statute's coverage to "whole categories of otherwise innocuous behavior," *United States v. Nosal*, 676 F.3d

854, 860 (9th Cir. 2012) (en banc), in contravention of this Court's repeated warnings against construing statutes to criminalize routine and benign conduct.

1. Most people do not break into computers or databases without permission. But the Eleventh Circuit's extension of the CFAA beyond such hacking reaches most everyone who uses a computer (which is to say, most everyone). Under the Eleventh Circuit's interpretation of the CFAA, computer users "exceed[their] authorized access" whenever they obtain information on a computer "for an inappropriate reason," or in violation of "computer-use policies" or websites' terms of service. Pet. App. 27a-28a. To say this is an everyday, commonplace occurrence is putting it mildly.

Obtaining "information" from a computer encompasses virtually anything one does on the internet or an internet-connected device. On a technological level, a person obtains information from a website whenever it is visited. To display a website, the person's computer must download digital content and otherwise procure information from the host server. Even on merely a human level, "obtaining information" "includes mere observation of [] data." S. Rep. No. 99-432, at 6 (1986). That is, visiting any website involves reading and internalizing information, "even if it is only the prompts or graphic interface." Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1567 (2010). Accordingly, consider the following scenarios:

Many law students have access to the Westlaw legal database for educational use only, as specified by their school's Westlaw license agreement. But a

student might obtain information from that database for personal purposes—perhaps to look up local housing laws to negotiate rent or to demand a refund of a security deposit. The Eleventh Circuit's construction of the CFAA renders this conduct a federal crime—indeed, a felony punishable by up to five years in prison because it is perpetrated for "private financial gain." 18 U.S.C. § 1030(c)(2)(B)(i).

To take another example, tens of millions of American workers participate in annual office pools for the NCAA men's basketball tournament ("March Madness").[4] When these employees use their company computers to generate their brackets, they likely violate their employers' policies prohibiting using "work computers for personal purposes." *Nosal*, 676 F.3d at 860. Given that these pools typically involve money stakes, the employees also are likely in pursuit of financial gain. Thus, as the Government itself indicated in this case during closing argument, this activity is also a felony under the Eleventh Circuit construction of the CFAA. *See* J.A. 39 ("[O]nce you're using the network [in your office] that's against what your job or policy prohibits, you've exceeded your access").

Finally, virtually every public website or internet-based application contains terms of service. Zoom, for example, prohibits users from "engag[ing] in activity

---

[4] Adam Chandler, *One Worker's Fantasy: A March Madness National Holiday*, The Atlantic (Mar. 20, 2015) (citing an estimate that 77.7 million workers will spend time on March Madness during work hours). The tournament was canceled in 2020 due to the ongoing public health crisis.

that is . . . false, or misleading."[5] eBay prohibits posting two "[l]istings that aren't significantly different."[6] By and large, these are policies "that most people are only dimly aware of and virtually no one reads or understands." *Nosal*, 676 F.3d at 861. But because these agreements define boundaries of appropriate use, any violation is potentially grounds for a criminal prosecution under the Eleventh Circuit's interpretation of the CFAA.

2. The virtually boundless reach of the Eleventh Circuit's construction of the CFAA demonstrates that the interpretation cannot be right. As this Court has repeatedly stressed in recent years, imprecisely worded federal statutes should not be construed expansively where, as here, it would lead to "a sweeping expansion of federal criminal jurisdiction." *See Kelly v. United States*, 140 S. Ct. 1565, 1574 (2020) (quoting *Cleveland v. United States*, 531 U.S. 12, 24 (2000)); *Marinello v. United States*, 138 S. Ct. 1101, 1108 (2018); *McDonnell v. United States*, 136 S. Ct. 2355, 2372-73 (2016); *Yates v. United States*, 574 U.S. 528, 540 (2015); *Bond v. United States*, 572 U.S. 844, 862-65 (2014).

For instance, in *Marinello*, the Court considered a federal statute, 26 U.S.C. § 7212(a), making it a crime to "impede the due administration" of the Internal Revenue Code. Under the lower court's conception of the statute, it would have "cover[ed] routine administrative procedures that are near-universally

---

[5] Zoom, Terms of Service 3(d) (April 13, 2020), at https://perma.cc/AB8T-V5GZ.

[6] eBay, Duplicate listings policy, at https://perma.cc/8WTZ-VDHT.

applied to all taxpayers." 138 S. Ct. at 1104. Indeed, it would have criminalized even "a person who pays a babysitter $41 per week in cash without withholding taxes" or a person who "leaves a large cash tip in a restaurant." *Id.* at 1108. The Court rejected this construction, holding that the statute reaches only conduct that "target[s] governmental tax-related proceedings, such as a particular investigation or audit." *Id.* at 1104. "Had Congress intended [the broader] outcome, it would have spoken with more clarity." *Id.* at 1108.

Holdings of this sort are nothing new. In *United States v. Kozminski*, 487 U.S. 931 (1988), the Court considered whether federal statutes prohibiting "involuntary servitude" exclude psychological coercion. *Id.* at 944. The facts of the case were quite troubling: The defendants used "various [psychologically] coercive measures—including denial of pay, subjection to substandard living conditions, and isolation from others"—to convince two intellectually disabled men "to believe they had no alternative but to work" on defendants' farm "seven days a week, often 17 hours a day." *Id.* at 934-36. But the Court held this was not enough to constitute "involuntary servitude." Interpreting the statute to include psychological coercion, the Court explained, would mean that even a "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.*; *see also*

Bond, 572 U.S. at 862 (refusing to "transform a statute passed to implement the international Convention on Chemical Weapons into one that also makes it a federal offense to poison goldfish").

The Court has taken the same approach in civil cases, rejecting constructions of statutes that would give them vast and surprising coverage. Just last Term, in *County of Maui v. Hawaii Wildlife Fund*, 140 S. Ct. 1462 (2020), the Court refused to construe a provision of the Clean Water Act in a way that would "require a permit in surprising, even bizarre circumstances, such as for pollutants carried to navigable waters on a bird's feathers, or, to mention more mundane instances, the 100-year migration of pollutants through 250 miles of groundwater to a river." *Id.* at 1471. Similarly, in *Lozman v. City of Riviera Beach*, 568 U.S. 115 (2013), the Court rejected an interpretation of the definition of "vessel" (for purposes of triggering admiralty jurisdiction) that would have swept in floating objects like "a wooden washtub, a plastic dishpan, a swimming platform on pontoons, a large fishing net, [or] a door taken off its hinges." *Id.* at 121.

The CFAA, of course, has *both* criminal and civil applications. It also deals with computerized data and the internet—technologies that are "so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow." *Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (2017). Under these circumstances, temperance in construing the statute is all the more warranted. Construing the decades-old CFAA in a wide-ranging manner might yield especially bizarre results as our digital landscape continues to evolve.

Better to stick to the statute's anti-hacking focus and allow "the People's representatives" to recalibrate the statute in the future if necessary to account for "our changing world." *Henson v. Santander Consumer USA, Inc.*, 137 S. Ct. 1718, 1726 (2017).

3. The Government has never disputed that its reading of the CFAA reaches commonplace activities prohibited by employers' computer use policies and websites' terms of use. To the contrary, in its most recent brief to an appellate court considering the issue as a matter of first impression, the Government fully embraced the Eleventh Circuit's all-encompassing interpretation of the statute. Br. for the United States at 14, 24-25 *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015) (No. 14-4396). The Government defended that position on the ground that, even if it "turn[ed] ordinary citizens into criminals, . . . the Government promise[d] to use [the statute] responsibly." *Valle*, 807 F.3d at 528 (citation omitted); *accord* BIO 16-18; *Nosal*, 676 F.3d at 862. For several reasons, this pledge does not suffice.

First, the Government's assurance appears questionable: Over the past decade, the Government has, in fact, brought cases against individuals who allegedly violated companies' terms of service agreements. *See, e.g.*, Indictment, *United States v. Swartz*, No. 1:11-cf-10260 (D. Mass. July 14, 2011), ECF No. 2 (violation of JSTOR terms of service); *United States v. Lowson*, No. 10-114 (KSH), 2010 WL 9552416, at *5-6 (D.N.J. Oct. 12, 2010) (alleged evasions of technological barriers and "violations of the terms of service on Ticketmaster's website"); *United States v. Drew*, 259 F.R.D. 449, 452 (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*, New Yorker (Mar. 18, 2013).

The Government suggests that its current guidance to federal prosecutors discourages such prosecutions. BIO 16-18. But that charging policy counsels only that "if the defendant exceeded authorized access solely by violating an access restriction contained in a contractual agreement or terms of service with an internet service provider or website, federal prosecution *may* not be warranted." Memorandum from U.S. Att'y Gen. to the U.S. Att'ys and Asst. Att'y Gens. for the Crim. and Nat'l Sec. Divs., at 5 (Sept. 11, 2014) ("Charging Policy") (emphasis added). And the Government pointedly declined in a recent case to forswear such prosecutions in the future. *Sandvig v. Barr*, No. 16-1368 (JDB), 2020 WL 1494065, at *4-5 (D.D.C. Mar. 27, 2020), (finding a credible threat of prosecution under the CFAA for terms-of-service violations in part because of "the absence of a specific disavowal of prosecution by the Department"), *appeal filed* (No. 16-1368).

Second, even if the Government did, in fact, promise not to pursue such everyday conduct, a free society should not be required to entrust its liberty to the grace of federal prosecutors. "It is the statute," not any bureaucratic pronouncement, "that prescribes the rule to govern conduct and warns against transgression." *Lanzetta v. New Jersey*, 306 U.S. 451, 453 (1939). Time and again, therefore, the Court has emphasized that it cannot "construe a criminal statute on the assumption that the Government will 'use it responsibly.'" *Marinello*, 138 S. Ct. at 1109 (quoting

McDonnell, 136 S. Ct. at 2372-73; *see also United States v. Stevens*, 559 U.S. 460, 480 (2010).

In this respect, a mere prosecutorial charging policy is a particularly inappropriate basis for construing a statute. The Government often changes its view regarding the reach of criminal statutes within and between administrations. *See, e.g.*, Pet. for Cert. at 13, *United States v. Wheeler*, 886 F.3d 415 (4th Cir. 2018) (No. 18-420) (noting the Department of Justice's "reconsider[ation]" and "change of position" regarding the scope of a criminal statute); Br. for the United States at 12, 15-16, *Koons v. United States*, 138 S. Ct. 1783 (2018) (No. 17–5716) (same). And when it does, defendants have no recourse or right to claim any reliance interest on the previous policy. *See* Charging Policy, *supra*, at 2.

Finally, whatever the Government's prosecutorial policy at any given time might be, it cannot prevent private parties from bringing civil suits based on the full range of conduct that the CFAA prohibits. The CFAA's private cause of action, 18 U.S.C. § 1030(g), derives from exactly the same operative language as its criminal prohibition. And a single statute with criminal and civil applications must mean the same thing in both contexts. *See, e.g.*, *Clark v. Martinez*, 543 U.S. 371, 380 (2005).

Businesses have already shown themselves prone to invoke the CFAA in aggressive and problematic ways against competitors. For instance, businesses have sought to stymie competition from start-up businesses seeking to make innovative use of publicly available data. *See* Nicholas A. Wolfe, *Hacking the Anti-Hacking Statute: Using the Computer Fraud and Abuse Act to Secure Public Data Exclusivity*, 13 Nw.

J. Tech. & Intell. Prop. 301 (2015). For example, in *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927 (E.D. Va. 2010), the plaintiff sued a small business for allegedly aggregating publicly available information from the plaintiff's website, in order to assemble a "venue directory" of hotels, restaurants, bars, and meeting venues. *Id.* at 930. The plaintiff claimed that the start-up business had exceeded its authorized access to the plaintiff's website because it violated the website's terms of use. *Id.* at 932. The court granted the defendant's motion to dismiss, *id.* at 934, but under the rule adopted by the Eleventh Circuit, the case could have gone forward.

An expansive interpretation of the CFAA would also deliver employers a potentially potent source of leverage in disputes with current and former employees. For example, an employer facing accusations of discrimination or other misconduct could easily identify some minor breach of a computer policy and threaten to seek damages (or even to refer these minor breaches for criminal prosecution) unless the employee agrees to drop her complaint. *See, e.g.*, *Lee v. PMSI, Inc.*, No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028, at *1 (M.D. Fla. May 6, 2011) (counterclaim under CFAA for using the internet at work to "visit[] personal websites such as Facebook" and send "personal email"). A related area of concern is the use of the CFAA to bring retaliatory claims against whistleblowers. Jonathan Mayer, *Cybercrime Litigation*, 164 U. Penn. L. Rev. 1453, 1465 (2016); *see, e.g.*, *Wyndham Vacation Ownership, Inc. v. Miloszewski*, at *1, No. 6:14–cv–68–Orl–40KRS, 2014 WL 5472454 (M.D. Fla. Oct. 22, 2014).

IV. If any doubt remains, two time-honored canons of judicial restraint require the more limited interpretation of the CFAA that courts besides the Eleventh Circuit have adopted.

On top of everything else, the Eleventh Circuit's expansive interpretation of the CFAA runs afoul of two time-honored canons of judicial restraint: the canon of constitutional avoidance and the rule of lenity.

1. Regardless of "the presence or absence of constitutional concerns in [any] given case," the Court must construe statutes to avoid "constitutional doubts regarding other litigants or factual circumstances." *Clark v. Martinez*, 543 U.S. 371, 381-82 (2005); *see also, e.g.*, *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 516 (2009). That imperative applies here: A broad reading of the CFAA's "exceeds authorized access" provision would raise both First Amendment and void-for-vagueness problems.

a. As Judge Bates of the U.S. District Court for the District of Columbia recently recognized, the CFAA must be construed narrowly to avoid "thorny First Amendment concerns." *Sandvig v. Barr*, No. 16-1368, 2020 WL 1494065, at *13 (D.D.C. Mar. 27, 2020), *appeal filed*, (No. 16-1368). The plaintiffs in that case were academic researchers who intended to create fictitious profiles on employment websites, in violation of terms of service forbidding users from providing of false information or creating fake accounts. *Id.* at *1. Through this strategy, they intended to test whether the websites discriminate based on race and gender, *id.*—thereby carrying forward a long tradition of using "testers" who provide false information to smoke out discrimination. *See, e.g.*, *Havens Realty Corp. v.*

Coleman, 455 U.S. 363, 368-75 (1982). The court held that this conduct would not violate the CFAA, reasoning that the Eleventh Circuit's broader reading of the statute "presents a significant risk that [the First Amendment] will be infringed." *Sandvig*, 2020 WL 1494065, at *11 (citation omitted).

The district court's concern was well-founded. The First Amendment protects untrue statements so long as they do not cause "legally cognizable harm" or provide "material gain" to the speaker. *United States v. Alvarez*, 567 U.S. 709, 719, 723 (2012). When, therefore, individuals use fictitious online profiles for benign reasons, their speech on public websites retains First Amendment protection.

In fact, many individuals besides researchers and testers have compelling reasons to conceal their identities online, in violation of websites' terms of service. These people include survivors of domestic abuse, harassment, and stalking who will be in danger if found by their abusers; political dissidents, religious minorities, and others involved in online advocacy disfavored by their real-world communities; and prominent figures, including politicians and judges, who may wish to follow online activity through monikers unassociated with their public identities. If the Eleventh Circuit were correct that all of this conduct violated the CFAA, it would chill this important expression and consumption of speech.[7]

---

[7] The Eleventh Circuit's construction of the CFAA similarly threatens the freedom of the press. "Data journalists"—reporters focused on bringing empirical and statistical analysis to bear on current events—often assemble their datasets using digital tools

b. An expansive conception of the CFAA would also raise serious vagueness concerns. A criminal statute is unconstitutionally vague, in contravention of due process, if it is "so standardless that it invites arbitrary enforcement." *Johnson v. United States*, 135 S. Ct. 2551, 2556 (2015). As explained above, the Eleventh Circuit's sweeping construction of the CFAA would leave prosecutors with free rein to prosecute virtually anyone for violating the statute. *See supra* at 29-31; Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1575-83 (2010). Such a construction would practically "invit[e] discriminatory and arbitrary enforcement." *United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) (en banc).

That (as the facts here indicate) federal law enforcement officials consider the CFAA fodder for devising sting operations only magnifies these concerns. It is no stretch to say that, if this Court were to uphold the Eleventh Circuit's construction of the CFAA, every federal prosecutor across the country would acquire an easy way "pick some person whom he dislikes or desires to embarrass," and then "put[] investigators to work, to pin some offense on him." Robert H. Jackson, *The Federal Prosecutor*, 24 J. Am. Judicature Soc'y 18, 19 (1940). This is where "the

---

that "scrape" data from public websites in violation of the site's terms of service. Criminalizing this form of information-gathering could run afoul of this Court's warning that "freedom of the press could be eviscerated" absent "protection for seeking out the news." *Branzburg v. Hayes*, 408 U.S. 665, 681 (1972); *see also Florida Star v. B.J.F.*, 491 U.S. 524 (1989) (recognizing the media's First Amendment right to gather and print truthful information obtained from publicly available sources).

greatest danger of abuse of prosecuting power lies"—where law enforcement has the potential to "become[] personal, and the real crime [can] become[] that of being unpopular with the predominant or governing group, being attached to the wrong political views, or being personally obnoxious to or in the way of the prosecutor himself." *Id.*

Any attempt to refine the Eleventh Circuit's interpretation of the CFAA to restrain prosecutorial discretion—covering some instances of access for unauthorized purposes but not others—would still leave the statute hopelessly indeterminate. The Due Process Clause requires crimes to 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 a subset of violations of terms of service, terms of use, employer use policies, or other contract-based conditions of access. *See* Kerr, *supra*, at 1575-83.

Perhaps the amendments to the CFAA that the Department of Justice has proposed in the past to Congress—which would revise the statute to cover certain particularized misconduct beyond hacking while also "mak[ing] clear that trivial conduct does not constitute a crime"—would solve this notice problem. Statement of Sujit Raman, Associate Deputy Attorney General, U.S. Dep't of Justice, *Hearing before the Senate Subcommittee on Crime and Terrorism: Cyber Threats to Our Nation's Critical Infrastructure*, 115th Cong., at 7-8 (Aug. 21, 2018); *see also* U.S. Dep't of Justice, Prosecuting Privacy Abuses by Corporate and Government Insiders (Mar. 16, 2015), https://perma.cc/937W-8L36 (proposing similar

"update[s]" to the CFAA). But that is a matter for another day. The Court's job is to interpret statutes, not rewrite them. *See, e.g.*, *Jennings v. Rodriguez*, 138 S. Ct. 830, 836 (2018). And the language in the statute presently before the Court is not susceptible to any construction along these lines.

2. If nothing else, the rule of lenity requires rejecting the Eleventh Circuit's construction of the CFAA. The rule of lenity mandates that "when [a] 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); *see also United States v. Davis*, 139 S. Ct. 2319, 2333 (2019) (reaffirming that "ambiguities about the breadth of a criminal statute should be resolved in the defendant's favor").

This "venerable rule," *United States v. R.L.C.*, 503 U.S. 291, 305 (1992) (plurality opinion), has deep roots in the American tradition of justice. As Chief Justice Marshall explained, it "is perhaps not much less old than construction itself." *United States v. Wiltberger*, 18 U.S. 76, 95 (1820). And the rule continues to play an important role in federal criminal jurisprudence. *See United States v. Santos*, 553 U.S. 507, 513-14 (2008) (plurality opinion) (applying rule); *Cleveland v. United States*, 531 U.S. 12, 25 (2000) (same); *R.L.C.*, 503 U.S. at 305 (plurality opinion) (same); *Liparota v. United States*, 471 U.S. 419, 427 (1985) (same). Indeed, resting on the rule of lenity is "particularly appropriate" where, as here, "the act underlying the conviction"—exceeding a use restriction on digitized

information or violating a website's terms of service—is "not inherently malign." *Arthur Andersen LLP v. United States*, 544 U.S. 696, 703-04 (2005).

At the very least, the "ordinary tools of legislative construction" fall short of sustaining the Eleventh Circuit's construction of the CFAA with the clarity required to subject "millions of ordinary computer users" to criminal liability. *United States v. Valle*, 807 F.3d 508, 526-27 (2d Cir. 2015). That alone is enough to compel rejection of the court of appeals' far-reaching interpretation of the statute.

CONCLUSION

For the foregoing reasons, this Court should reverse the judgement of the court of appeals.

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

July 1, 2020