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

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provision

Statutes

Legislative Materials

Other Authorities

REPLY BRIEF FOR PETITIONER

The Government's construction of the CFAA's "exceeds authorized access" prong is, if anything, more sweeping than the Eleventh Circuit's. According to the Government, a single two-letter word ("so") in the statutory definition of that phrase means that it prohibits obtaining information via computer whenever the user, "under the circumstances," is not supposed to do so. U.S. Br. 18. This conception of the CFAA—apparently incorporating *any* circumstance of which the user is aware—suggests that most Americans violate its criminal prohibition on a daily basis.

Faced with this implication, the Government says that other aspects of the CFAA *might* restrict its coverage. But the Government's suggestions are vaporous. The Government does not necessarily support the potential limitations it discusses; the statutory arguments the Government floats range from debatable to implausible; and even if courts accepted them, they would not meaningfully constrain the statute.

Simply put, the CFAA is an anti-hacking law. Nothing in the statute's text, structure, purpose, or legislative history (even if it were relevant) indicates that it was meant to be a "sweeping Internet-policing mandate," criminalizing everything from routine breaches of contract to transgressions of employee handbooks. *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012) (en banc). And even if there were a whiff of ambiguity in that respect, settled rules of statutory construction require interpretive restraint here. This Court should reverse.

ARGUMENT

I. The text of the CFAA does not encompass obtaining information for an improper purpose.

1. The Government does not defend the Eleventh Circuit's textual reasoning. Instead, the Government offers an entirely different linguistic justification for construing the CFAA to criminalize any misuse of information obtained via computer. According to the Government, the word "so"—nestled in the CFAA's definition of "exceeds authorized access"—dictates that individuals violate the statute whenever they are not entitled, "under the circumstances," to obtain information that they access. U.S. Br. 18.

The Government's own definitions of "so" demonstrate that the word is not that capacious. As the Government notes, "so" means "[i]n the same manner as has been stated," or "[i]n the way or manner described." U.S. Br. 18 (quoting, respectively, *Black's Law Dictionary* 1246 and *The Oxford English Dictionary* 887 (2d ed. 1989)). In other words, the term "so" is a statutory shorthand that refers to a manner of doing something *that the text of the statute has already described*.

Take, for example, the federal statute that prohibits embezzling property from an Indian tribal organization, as well as receiving property "so embezzled." 18 U.S.C. § 1163. The word "so" "refers back" to, and encapsulates, the requirement that the property be taken from an Indian tribal organization. *United States v. Markiewicz*, 978 F.2d 786, 804-05 (2d Cir. 1992). Without that word, the provision would prohibit receiving *any* stolen property. *Id.* at 805.

Applying that ordinary usage of "so" to the CFAA is straightforward. The CFAA's definition of "exceeds authorized access" reads as follows: "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). In this definition, "the manner [that] has been stated" or "described" is "access[ing] a computer with authorization," 18 U.S.C. § 1030(e)(6). Accordingly, a person is "not entitled *so* to obtain" information when he is not entitled to obtain it via a computer he is otherwise authorized to access. *See* Petr. Br. 18.

The Government protests that this ordinary-meaning approach renders the word "so" superfluous. U.S. Br. 19-20. This is simply incorrect. Take the contractor who the Government hypothesizes has access to a government computer but not to "salary files" stored on it. *Id.* That person might well be able to get that salary information through another route. Assuming the salaries are not classified, the contractor could just ask the employees themselves how much money they make. Or he could file a FOIA request.[1] But the term "so" makes clear that the contactor's entitlement to obtain the information in a non-digital manner would not prevent a CFAA prosecution for hacking into the salary database.

---

[1] *See, e.g.*, Letter from Lance Harris, U.S. Office of Pers. Mgmt., to Beryl Lipton, MuckRock News (Nov. 21, 2019), https://perma.cc/5SHD-BXWF (granting FOIA request for employee salary data across multiple federal agencies); Reps. Comm. for Freedom of the Press, *Salary*, https://perma.cc/DA3X-EAS4 (last visited Sept. 24, 2020) (collecting state FOIA laws allowing people to obtain government salary information).

Stated more generally: The Government need not negate the possibility in every CFAA prosecution that the defendant had some authorized means of non-digital access to the information at issue.

That, however, is as far as the term "so" goes. It does not incorporate into the CFAA access or use conditions that are external to the statute. Indeed, if the Government were right that the term "so" meant "under the circumstances"—that is, not just the circumstances stated in the statute but also *any* external circumstance that is "specifically and explicitly" transmitted to the computer user, U.S. Br. 18-19—then the CFAA's "exceeds authorized access" prong would be practically limitless. Consider the following scenarios:

- Upon returning to the stationhouse after a day on patrol, a police officer's chief tells him not to run suspicious license plates through the GCIC database until he finishes a few hours of tedious paperwork. But the officer gets bored and runs the plates before the paperwork is complete.
- Two parents establish a household rule that their teenagers are not to log into social media accounts on their iPhones after 10:00 pm. Late at night, the teens do it anyway.
- A law professor writes in the course syllabus that students may use laptops during class to take notes but not to surf the internet. A law student nevertheless browses Amazon.com during class.

In each of these scenarios, the computer users are not entitled "under the circumstances," U.S. Br. 18, to access the information they obtain. Yet the

Government gives no indication that it believes its construction of the word "so" encompasses such scenarios—or the nearly infinite array of similar situations that could be readily summoned. Accordingly, its construction must not be right.

2. That other federal statutes expressly prohibit obtaining computerized information for an "unauthorized purpose" confirms that Congress did not sweep such conduct into the CFAA indirectly, through implications subsumed inside the word "so." Had Congress wished to cover such conduct, it had clear language readily at hand. *See* Petr. Br. 19-20.

The Government responds that using express "unauthorized purpose" language in the CFAA would not cover individuals who obtain information "in violation of other types of restrictions." U.S. Br. 22. But if Congress had intended to criminalize not just obtaining information via computer for an unauthorized purpose but also obtaining information in contravention of *any* stated use or access restriction, Congress could easily have included that additional prohibition too. The Government still offers no explanation for why Congress would have used such unconventional and indistinct language to codify basic legal concepts that it has expressed in plain terms elsewhere in the U.S. Code. *See Barton v. Barr*, 140 S. Ct. 1442, 1453 (2020).

3. Finally, the prospect of a "sweeping expansion of federal criminal jurisdiction" cuts against the Government's textual argument. *See Kelly v. United States*, 140 S. Ct. 1565, 1574 (2020) (quoting *Cleveland v. United States*, 531 U.S. 12, 24 (2000)). The Government tries to dismiss the startling breadth of its reading of the CFAA as a mere "policy" matter.

U.S. Br. 34-35. But this Court has repeatedly admonished that such breadth is a significant—often, dispositive—consideration in statutory construction.

To begin, when confronted with a "broad reading" of imprecise terms in federal criminal statutes, this Court takes care "to exercise interpretive restraint." *Marinello v. United States*, 138 S. Ct. 1101, 1107-08 (quoting *United States v. Aguilar*, 515 U.S. 593, 600 (1995)) (quotation marks omitted). Requiring "more clarity" than usual in this context reflects "deference to the prerogatives of Congress" and the related "concern that 'a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed.'" *Id.* at 1108, 1106 (quoting *Aguilar*, 515 U.S. at 600). A growing list of recent decisions has reinforced this enhanced need for textual clarity, often unanimously. *See, e.g.*, *Kelly*, 140 S. Ct. at 1574; *McDonnell v. United States*, 136 S. Ct. 2355, 2372-73 (2016); *Yates v. United States*, 574 U.S. 528, 540 (2015) (plurality opinion); *Bond v. United States*, 572 U.S. 844, 862-65 (2014). There is no basis to discount these cases as based on mere "policy" assessments.

What is more, "in the absence of a clear statement from Congress," federal statutes should not be construed to criminalize "a wide range of conduct traditionally regulated by state and local authorities." *Cleveland*, 531 U.S. at 24; *accord Bond*, 572 U.S. at 862-65. This canon applies here too. State law customarily regulates misuse of information obtained through employment relationships—as well as breaches of contractual relationships between businesses and consumers. *See* Petr. Br. 25. Yet the Government offers not a speck of evidence that, by

enacting the CFAA, Congress intended a "stark intrusion into [this] traditional state authority." *Bond*, 572 U.S. at 866. That confirms that the most natural reading of the CFAA is that it covers only the special problem of hacking.

II. The CFAA's legislative history does not support the Government's expansive conception of "exceeding authorized access."

Unable to shore up the Eleventh Circuit's construction of the CFAA with its novel textual argument, the Government embarks on an extended foray into the statute's legislative history. U.S. Br. 26-34. Legislative history, however, cannot overcome the most natural reading of a statute—or even resolve statutory ambiguity against a criminal defendant. *See* Petr. Br. 40-41; Amicus Br. of Committee for Justice 14-18. But even if it could, the Government's arguments would still come up short.

1. The 1986 amendments to the CFAA demonstrate that the statute does *not* reach "misappropriation," U.S. Br. 27. Those amendments *removed* language allowing liability for accessing information with authorization but "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, *amended by* Pub. L. No. 99-474, § 2(c), 100 Stat. 1213, 1213 (1986).

The Government nonetheless insists that when Congress replaced the CFAA's improper-purpose language with the phrase "exceeds authorized access" (and its accompanying definition), Congress did nothing more than "clarify" that the statute covered obtaining information for an improper purpose. U.S.

Br. 28 (citation omitted). Common sense dictates otherwise. So does precedent: The Court should not "read back into the [statute] the very . . . statutory language that [Congress] has earlier discarded in favor of other language." *Chickasaw Nation v. United States*, 534 U.S. 84, 93 (2001) (internal quotation marks and citations omitted).

The committee reports that the Government refers to do not help it either. The 1986 Senate Report explains that the pertinent amendments "refocuse[d] that legislation on its principal objectives" and that the deletion of the improper-purpose language from a parallel provision of the Act "remove[d] from the sweep of the statute one of the murkier grounds of liability"—namely, the situation where "access to computerized data might be legitimate in some circumstances." S. Rep. No. 99-432, at 20-21 (1986).

The Senate Report accompanying the 1996 amendments to the CFAA, which extended the "exceeds authorized access" prohibition to federal employees, is simply silent on the question presented here. The Government quotes a sentence saying the amendment was meant to cover those "who *abuse* their computer access privileges to obtain Government information that may be sensitive and confidential." U.S. Br. 29 (quoting S. Rep. No. 104-357 at 4 (1996)) (emphasis added). But the Report never says that misappropriation—as opposed to obtaining sensitive information an employee is forbidden from obtaining for any purpose—constitutes a targeted "abuse."

That leaves the Government's reliance on Senator Leahy's 1996 floor statements. U.S. Br. 29. The Court has observed that "floor statements by individual legislators rank among the least illuminating forms of

legislative history." *NLRB v. SW General, Inc.*, 137 S. Ct. 929, 943 (2017) (citing *Milner v. Dep't of Navy*, 562 U.S. 562, 572 (2011)). That certainly is true here. In 1986, Senator Leahy was adamant that the CFAA should not reach "'whistleblowers,' who disclose information they have gleaned from a government computer." S. Rep. No. 99-432, at 8 (1986). In 1996, Senator Leahy offered no way to exclude that conduct (which typically violates employer use restrictions) from the CFAA's reach while criminalizing violations of *other* use restrictions, such as those in this case. Nor does the Government here. Better to stick to the language Congress actually enacted, as opposed to cross-cutting examples of potential coverage from a single legislator.

2. The Government also goes astray attempting to leverage loose analogies in the legislative history to "traditional property crimes like theft." U.S. Br. 33. It is one thing to construe a statute in accordance with common-law concepts where the statute actually uses a term that had a settled common-law meaning. *See, e.g.*, *Evans v. United States*, 504 U.S. 255, 259-64 (1992) (construing "extortion" according to its common-law roots). But "a 'cluster of ideas' from the common law should be imported into statutory text only when Congress employs a common-law *term*, and not when, as here, Congress simply describes an offense analogous to a common-law crime without using common-law terms." *Carter v. United States*, 530 U.S. 255, 265 (2000) (quoting *Morissette v. United States*, 342 U.S. 246, 263 (1952)). Accordingly, the common law is "beside the point" in this case. *Id.* at 264.

Looking to the common law (or modern definitions of theft) would be particularly misguided here in light of Congress's recognition at the inception of the CFAA that "[c]omputer technology simply does not fit some of the older, more traditional legal approaches to theft or abuse of property." S. Rep. No. 99-432, at 13-14 (1986); *see also* H.R. Rep. No. 98-894, at 8-9 (1984) (targeted computer activity "does not fit well into . . . traditional theft/larceny statutes"). The Government, for example, maintains that someone can commit theft when he uses property "in a manner beyond his authority." U.S. Br. 33 (quoting Model Penal Code, Pt. II, § 223.2 cmt. 2, at 166 (1980)). But that is so only in an "embezzlement situation." *See id.* at 165-66. Embezzlement generally is a separate crime that "do[es] not overlap" with common-law (or, in many states, modern-day) theft. Wayne R. LaFave, 3 Substantive Criminal Law § 19.6(a), at 125 (3d ed. 2018). And to prove embezzlement, the prosecution must *also* prove that the wrongdoer deprived the owner of the use of his property, *see id.* § 19.6(b)—something that need not be shown in a CFAA case, *see* U.S. Br. 30-31.[2]

In short, the whole point of the CFAA was to deal with a "new dimension" of criminal activity—"the activities of so-called 'hackers.'" H.R. Rep. No. 98-894, at 8-10. Even if resort to legislative history were otherwise appropriate in this case, analogies to the very criminal-law concepts that Congress believed

---

[2] Analogies to common-law trespass would be equally fruitless. While trespass does not require a deprivation of property, the gravamen of the crime is a physical intrusion on another's property. *See* LaFave, 3 Substantive Criminal Law § 19.6(a), at 125. That does not occur in a CFAA case.

were a mismatch for the modern digital landscape would be perverse.

3. The Government lastly suggests that Congress would have expected the CFAA to reach certain forms of digital misconduct beyond hacking. The Government, however, overlooks other statutes that already cover that misconduct.

The Government, for instance, mentions the possibility of someone selling "computerized national-security information" to a foreign government. U.S. Br. 24. But another federal statute already prohibits accessing a government computer, "with an unauthorized purpose, and thereby obtain[ing] classified or other protected information." 10 U.S.C. § 923(a)(2). The Government also imagines a car-company employee obtaining GPS data "to stalk" a customer. U.S. Br. 21. The federal stalking statute, however, already prohibits using "any interactive computer service" or "electronic" facility of interstate commerce for such a nefarious purpose. 18 U.S.C. § 2261A(2). Finally, the Government frets over the notion of a medical assistant accessing patient records without first procuring the requisite "permission." U.S. Br. 22. Yet federal law already prohibits obtaining individually identifiable medical records without authorization. 42 U.S.C. § 1320d-6(a)(2).

The Government no doubt carefully selected the examples it features in its brief to suggest a need for an all-inclusive reading of the CFAA. It is telling that they actually show just the opposite.

III. The legal consequences of the Government's position are unacceptable.

Confronted with the fact that its conception of "exceed[ing] authorized access" under the CFAA would sweep in vast swaths of everyday conduct, the Government urges this Court to look the other way. It says that cases involving routine computer use are unlikely to be brought. The Government also suggests that, even when such cases are brought, courts might turn them away for reasons not at issue here. Neither of these ploys works.

1. It does not matter whether the Department of Justice's current "computer-crime charging policy" dissuades its lawyers from bringing "real-world prosecutions" based on the outer reaches of the CFAA. U.S. Br. 42. "[T]he Founders did not fight a revolution to gain the right to government agency protocols." *Riley v. California*, 573 U.S. 373, 398 (2014). What matters is what the *law* prohibits. *See* Petr. Br. 33-34.

Accordingly, in *Marinello*, the Court emphasized that the Government's interpretation of the tax statute there would have forbidden people from paying babysitters in cash or "leav[ing] a large cash tip in a restaurant." 138 S. Ct. at 1108. The Court did not ask whether any such prosecutions had been brought. In *United States v. Kozminski*, 487 U.S. 931 (1988), the Court similarly expressed concern, without looking for "real-world" cases, that the Government's argument would allow prosecuting parents for "threatening [to] withdraw[] affection" from their kids. *Id.* at 949. The same approach applies here. The only relevant question is whether the Government's interpretation of the CFAA would permit it to bring prosecutions for "a broad range of day-to-day activity." *Id.* It does.

In any event, the Government provides little solace to the many Americans whom its interpretation of the CFAA would expose to criminal liability. Amici explain that the imperiled would include academic and security researchers; a variety of journalistic enterprises; technology companies (especially small businesses and startups); whistleblowers; and even medical device reprocessors. These entities explain that many of their activities have already been chilled by decisions like the Eleventh Circuit's here. If this Court were to ratify a sprawling conception of "exceeds authorized access," these entities' litigation risks—not just from the Government, but also from private parties, *see* Petr. Br. 34-35—would surely redouble.[3]

Employees engaged in everyday activities would face serious risks too. The Government points out that the CFAA's primary civil cause of action authorizes private parties to bring suit "only in cases involving losses of at least $5000." U.S. Br. 42. But it is not hard to imagine an employer plausibly asserting that a "violation" as modest as personal use of a company-issued computer caused that much harm in terms of lost productivity. Many lawyers in private firms bill more than that in a single day. And the Government has no way of preventing employers or other private parties from filing lawsuits based on the most far-reaching applications of the CFAA.

2. The Government's discussion of other components of the CFAA only magnifies these

---

[3] After these amicus filings, a larger group of security researchers spoke out about this case, reiterating the "chilling effects" of the Government's position. *See Security Community Response to Voatz's Supreme Court Amicus Brief*, Disclose (Sept. 14, 2020), https://perma.cc/2D7M-G43T.

litigation risks. For starters, the Government pointedly declines to endorse some of the narrowing arguments it floats. In that respect, the Government's brief exacerbates the statute's already-intolerable fair-notice shortcomings—particularly within "today's criminal justice system," in which the mere possibility of charges often drives the plea bargaining process. *Missouri v. Frye*, 566 U.S. 134, 143-44 (2012). And there obviously is no mechanism to have a "do over" in this Court on the question presented if, in future cases, courts reject the narrowing arguments the Government conjures up here.

At any rate, none of the other aspects of the CFAA that the Government discusses meaningfully cabins the statute.

a. *Authorization.* The Government first suggests that the CFAA "may not" apply at all to websites that "offer[] access to the public on general terms" because "authorization"—as the statute uses that word—may not be needed to access such websites. U.S. Br. 37. There are several problems with this suggestion.

As an initial matter, it is inconsistent with the Government's own position in past cases, in which it has maintained that the CFAA *does* apply in that setting. *See, e.g.*, *United States v. Auernheimer*, 748 F.3d 525, 529-31 (3d Cir. 2014) (alleging violation of the CFAA for procuring information from AT&T's "general login webpage"). Courts have likewise repeatedly held that the CFAA applies to information on publicly accessible websites. *See, e.g.*, *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003); *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595-97 (E.D. Pa. 2016); *Sw. Airlines Co. v. Farechase,*

Inc., 318 F. Supp. 2d 435, 437, 439-40 (N.D. Tex. 2004).[4]

The Government's suggestion is also difficult to square with the ordinary meaning of "authorization." The Government contends that "authorization" connotes formal, advance, enabling action. U.S. Br. 36. But a typical speaker might well say she is authorized to enter a commercial establishment during business hours or to hike a certain trail in a national park. *See, e.g.*, 1 *Webster's New International Dictionary* 186 (2d ed. 1956) (defining "authorized" as "possessed of, or endowed with, authority"). Listeners would not trip over the fact that the speaker had not obtained individualized, advance approval for such activities. And similarly, it is perfectly natural to speak of an individual as having "authorization" to use a publicly available website in the absence of similar formalities.

Even if "authorization" did require some sort of official approval or authentication, it would scarcely narrow the CFAA. Virtually every computer in every workplace requires employees to log in before accessing the internet—or, indeed, any information at all. And many commonly used websites—from Facebook to Uber to Westlaw—require people to

---

[4] The Government suggests (U.S. Br. 37) that the Ninth Circuit held to the contrary in *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1002 (9th Cir. 2019), *pet'n for cert pending*, No. 19-1116. But that case concludes merely that users do not obtain information "*without* authorization" under 18 U.S.C. § 1030(a)(2) when they obtain it from publicly accessible websites. The Ninth Circuit made clear in *Nosal* that users can obtain information, as described in 18 U.S.C. § 1030(e)(6), "*with* authorization" from such websites. *See* 676 F.3d at 860.

establish usernames and passwords to access information. Even under an artificially constricted conception of "authorization," that is all that would be required to expose someone to a criminal prosecution for violating a term of service.[5]

b. *Use.* Next, the Government suggests that the CFAA's word "use" in the definition of "exceeds authorized access" might "require that the violator's authorized access be instrumental to acquiring the information—not merely the technical means by which he views such information." U.S. Br. 38. The Government cites no case in the decades-long history of the CFAA that has ever so held. And we confess we do not really even know what the Government means. The Government, for instance, suggests that "sending an e-mail at work" would not necessarily constitute "using" computer access to obtain information, because it would not capitalize on access to "restricted" computer files. *Id.* 38-39. But Gmail and other email services *do* contain restricted data; as the Government puts it elsewhere, they require individuals to enter a "username and password" to send or receive information. *Id.* 38. Suffice it to say that whatever precisely the word "use" means, it does not erect a

[5] Insofar as the Government suggests that even when people have to enter a username and password to access information on a website, that still might not establish "authorization," U.S. Br. 37-38, the Government offers no good reason why that would be so. Nor can we think of any. Such login credentials, in ordinary English, plainly authorize the user to access information on the website. Furthermore, people are often authorized to set up accounts in the first place only if they satisfy certain restrictions, such as minimum age requirements.

significant barrier against wide-ranging applications of the CFAA.

c. *Mens rea.* Lastly, the Government opines that the mens rea requirements in the CFAA protect against criminal liability for routine online conduct. According to the Government, violating a stated restriction on computer use of which the user is "only dimly aware" would not satisfy the requirement of "knowingly" or "intentionally" exceeding authorized access. U.S. Br. 39 (citations omitted). Again, the Government's contention suffers from several defects.

For one thing, the Government has taken the exact opposite view in the past. It has maintained that a "defendant need *not* have read the [terms of service of a publicly available website] in order for her conduct to be in violation of the [CFAA]." Govt's Opp. to Defendant's Motion for Acquittal at 6, *United States v. Drew*, No. 2:08-cr-00582-GW (C.D. Cal. 2008), ECF No. 97 (emphasis added).

Furthermore, it is unclear, at best, whether the Government's current contention regarding the CFAA's mens rea requirement is correct. Website operators typically procure consent to their terms of use through "clickwrap" in which users check "I agree" in boxes attached to recitations of those terms. *See generally* Mark A. Lemley, *Terms of Use*, 91 Minn. L. Rev. 459, 465-67 (2006). Courts in contract cases regularly hold that such action establishes knowledge of the terms, even when consumers have not read them. *Hancock v. AT&T*, 701 F.3d 1248, 1255-58 (10th Cir. 2012); *accord Meyer v. Uber Techs., Inc.*, 868 F.3d 66, 79–80 (2d Cir. 2017); *Melo v. Zumper, Inc.*, 439 F. Supp. 3d 683, 698 (E.D. Va. 2020); *Davis v. USA Nutra Labs*, 303 F. Supp. 3d 1183, 1192–93 (D.N.M. 2018).

Consequently, if the Government wins this case, courts might well hold in future CFAA cases that violating terms in clickwrap constitutes an intentional or knowing act, regardless of whether defendants were subjectively aware of the terms.

In any event, many of the forms of everyday computer use that the Government's interpretation of the CFAA would ensnare are unquestionably *intentional* violations of use restrictions. Start with the prosecutor's own example in the closing argument in this case: using one's work computer to "access personal information." J.A. 39. Courts "should be hesitant to impose federal sanctions for conduct as pedestrian as checking one's private social media account on a work phone." *Royal Truck & Tractor Sales Servs. Inc. v. Kraft*, ___ F.3d ___, 2020 WL 5406118, at *5 (6th Cir. 2020) (joining other courts rejecting Eleventh Circuit's construction of "exceeds authorized access"). Yet it is common knowledge that employer-issued devices are supposed to be used only for business purposes. So the CFAA's mens rea element would offer no refuge in that context. Nor would it offer protection in any of the scenarios described above, where people disobey an explicit directive from a supervisor, parent, or professor. *See supra* at 4.

The same goes for any number of other everyday online practices. It is well known, for example, that users may not post inaccurate statements about themselves on dating apps. But more than 80 percent of the over 30 million users of such apps "misrepresent

their height, weight, or age in their profiles."[6] Fantasy football websites prohibit using their content "in connection with any form of gambling or wagering." Yet almost three-quarters of the 75 million Americans who play such fantasy sports report wagering in their fantasy leagues.[7] And popular ridesharing apps like Uber and Lyft forbid people under 18 from using the services alone. But those rules are "routinely ignored" by teenagers, parents, and drivers alike.[8]

The inescapable reality is that if the CFAA covers violations of stated use restrictions, then a substantial portion—if not a majority—of Americans violate the statute every single day. No part of the statute besides the definition of "exceeds authorized access" is capable of placing serious limits on the Government's (or private parties') discretion to invoke it.

---

[6] Stephanie Rosenbloom, *Love, Lies, and What They Learned*, N.Y. Times, Nov. 12, 2011; *see also* Match.com, *Terms of Use Agreement* § 3a (Nov. 12, 2019), https://perma.cc/N7BJ-JPL6; J. Clement, *Online Dating in the United States - Statistics & Facts*, statista (Mar. 24, 2020), https://perma.cc/G4CG-RXVD.

[7] Verizon Media, *Yahoo Sports Fantasy Football Additional Terms of Service*, https://perma.cc/SG5A-77RB; Gregory Bresiger, *Nearly 75M People Will Play Fantasy Football this Year*, N.Y. Post (Sept. 25, 2015), https://perma.cc/38XK-JGL4.

[8] Uber, *U.S. Terms of Use*, https://perma.cc/K8RP-BL75 (July 15, 2020); Phil Rogers & Courtney Copenhagen, *Underage Rideshare: Too Young to Ride—But Doing it Anyway*, NBC 5 Chicago (May 21, 2018), https://perma.cc/9F4R-9UTB; *see also* Terry Nguyen, *Ride-sharing services refuse to serve underage kids. Teens still use them*, Vox (Sept. 9, 2019), https://perma.cc/8SXG-QQPW.

IV. The Government's interpretation of the CFAA contravenes the constitutional avoidance canon and the rule of lenity.

If ambiguity remained, two final canons of judicial restraint would preclude the Government's all-embracing construction of the "exceeds authorized access" prong.

1. *Constitutional avoidance.* The Government offers no good answer to the serious constitutional concerns that its construction of the CFAA would raise.

a. The Government denies that its conception of the CFAA would render the statute invalid under the First Amendment's "overbreadth" doctrine. U.S. Br. 45. According to the Government, even assuming that "a small fraction" of the activity its interpretation would cover is protected by the First Amendment, that does not matter because that fraction is not a "substantial amount" of the overall activity the statute prohibits. *Id.* at 45-46 (citation omitted).

The Government is asking and answering the wrong question. The pertinent question with respect to the First Amendment—as it would be with any other constitutional provision—is whether the Government's interpretation of the CFAA would raise serious constitutional issues in *any* of "the statute's applications." *Clark v. Martinez*, 543 U.S. 371, 381-82 (2005) (due process); *see also FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 516 (2009) (free speech); *NLRB v. Catholic Bishop of Chicago*, 440 U.S. 490, 499-504 (1978) (religious liberty). If so, the Court should construe the statute to avoid such problems.

The Government also is wrong that the CFAA regulates "conduct, not speech." U.S. Br. 45. Many restrictions on using websites—which the Government's construction of the CFAA would incorporate into the statute—directly forbid certain kinds of speech. *See, e.g.*, Zoom, *Terms of Service* 3(d) (Apr. 13, 2020), https://perma.cc/AB8T-V5GZ (prohibiting "false or misleading" speech); Twitter, *Civic Integrity Policy* (Sept. 2020), https://perma.cc/Z3JN-KUZ3 (prohibiting "content that may suppress participation or mislead people" regarding electoral rules or procedures).

The Government's construction of the CFAA would also raise distinct First Amendment problems by inhibiting newsgathering and academic research. *See* Petr. Br. 36-37; Amicus Br. of Reporters Committee for Freedom of the Press 9-17; Amicus Br. of The Markup 21-27; Amicus Br. of Kyratso Karahalios et al. 14-17. The Government says the techniques amici discuss "may not" fall within the "with authorization" predicate in the definition of "exceeds authorized access." U.S. Br. 37, 46. But the Government's own hedging on that issue (*see supra* at 14) only enhances the chilling effects amici describe. And the Government provides no answer at all to the concern that its interpretation of the CFAA would cover a wide range of journalistic sources who provide vital information regarding governmental and commercial activities. Amicus Br. of Reporters Committee 11.

b. Nor is the Government able to deflect the serious due process concerns that would arise if the CFAA were violated whenever an individual was not authorized "under the circumstances" to obtain

computerized information. As with the First Amendment, the Government begins by mischaracterizing the issue. Petitioner is raising a constitutional argument in favor of *construing the statute* in a particular manner, so it does not matter whether the CFAA is unconstitutionally vague as applied to his conduct. *See* U.S. Br. 46-48. The question is whether the Government's interpretation of the statute would raise any due process problems.

On that score, the Government mostly repeats its suggestions that aspects of the CFAA other than the definition of "exceeds authorized access" limit the reach of the statute. U.S. Br. 47. For the reasons explained above, that is not so. *See supra* at 14-19. And any construction of the CFAA that makes tens of millions of individuals criminals for their daily use of websites like Facebook, OkCupid, and Gmail cannot be said to "limit[] prosecutorial discretion." U.S. Br. 47 (quotation marks omitted).

Nor does the CFAA's mens rea element ensure that individuals will have "fair notice of the conduct [the statute] punishes." U.S. Br. 47-48 (quoting *Beckles v. United States*, 137 S. Ct. 886, 892 (2017)). That element does not require a defendant to "know his conduct is illegal." *Elonis v. United States*, 135 S. Ct. 2001, 2009 (2015). It requires only that he know he is violating an access or use restriction. As explained above, that sort of knowledge is utterly commonplace. *See supra* at 18-19. What is *not* known—indeed, what would dumbfound most Americans—is that such everyday activity is a federal crime.

It is not necessary to "amend" the statute to avoid the startling and pernicious implications of the Government's interpretation of the CFAA. U.S. Br. 43.

All the Court needs to do is resolve any ambiguity in the CFAA's definition of "exceeds authorized access" to cover only "inside hackers." *See* Petr. Br. 24. If the statute should be updated somehow to account for certain other types of misconduct in the internet age, Congress can do so in clear and calibrated terms. *See* Petr. Br. 39-40 (describing legislation DOJ has proposed in recent years); Amicus Br. of Orin Kerr 23-27 (describing potential future legislation); Amicus Br. of Electronic Information Privacy Ctr. 21-26 (offering various ways to limit the CFAA's "exceedingly broad" coverage, none of which have any basis in the text of the current statute).

2. *Rule of Lenity.* The Government's conception of the CFAA also contravenes the rule of lenity. True, the Court has alternated in recent years between applying the rule where "ambiguities" exist and restricting its application to situations involving "grievous ambiguity." Amicus Br. of NACDL 7 n.2 (collecting cases). The former is the traditional—and correct—test. *See id.* at 6-10; Amicus Br. of Committee for Justice at 14-18. But petitioner would prevail under either verbal formulation.

The rule of lenity is particularly important where, as here, technological developments give rise to sweeping legal implications that Congress could never have envisioned. The rule is designed partly to ensure that the Legislative Branch has truly determined that certain conduct should be subject to the "moral condemnation" that a criminal sanction entails. *United States v. Bass*, 404 U.S. 336, 348 (1971). And here, there is no way to say that Congress—legislating before the advent of the internet—intended the CFAA to "transform whole categories of otherwise innocuous

behavior into federal crimes simply because a computer is involved." *Nosal*, 676 F.3d 860. That alone is enough to reject the Government's all-encompassing construction of the statute's "exceeds authorized access" prong. *Id.* at 863.

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

September 28, 2020