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

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

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

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE *AMICUS CURIAE* 1

INTRODUCTION AND SUMMARY OF THE ARGUMENT 2

ARGUMENT 4

I. The Eleventh Circuit's Interpretation Of The CFAA Is Contrary To The Statute's Text And Congress' Intent, And Violates The Rule Of Lenity 4

- A. It Is Crucial That The Court Continue To Construe The Text Of Criminal Statutes Narrowly 5
- B. Congress Could Not Have Intended An Expansive Reading Of The CFAA 10

II. Expansively Construing The CFAA Raises Constitutional Concerns 13

- A. Expansively Construing The CFAA Raises Vagueness Concerns 14
- B. Expansively Construing The CFAA Invites Arbitrary Enforcement 16

III. Expansively Interpreting The CFAA Would Further Overcriminalization 18

CONCLUSION 23

TABLE OF AUTHORITIES

CASES PAGES

Blodgett v. Holden,
275 U.S. 142 (1927)...18

Bond v. United States,
572 U.S. 844 (2014)...22

Bryan v. United States,
524 U.S. 184 (1998)...8

City of Chicago v. Morales,
527 U.S. 41 (1999)..14, 16, 17

Clark v. Martinez,
543 U.S. 371 (2005)...18

Coates v. City of Cincinnati,
402 U.S. 611 (1971)...15

Crandon v. United States,
494 U.S. 152 (1990)...7

Dean v. United States,
556 U.S. 568 (2009)...7

Green v. Bock Laundry Machine Co.,
490 U.S. 504 (1989)...4

Holloway v. United States,
526 U.S. 1 (1999)...8

Johnson v. United States,
135 S. Ct. 2551 (2015) 13

Kimble v. Marvel Entertainment, LLC,
576 U.S. 446 (2015)... 13

Kolender v. Lawson,
461 U.S. 352 (1983)... 14

Liparota v. United States,
471 U.S. 419 (1985)..4-5, 8, 9

National Federation of Independent Business v. Sebelius,
567 U.S. 519 (2012)... 9

Scheidler v. National Organization for Women, Inc.,
537 U.S. 393 (2003)... 7

Skilling v. United States,
561 U.S. 358 (2010)... 13

United States Civil Service Commission v. National Ass'n of Letter Carriers, AFL-CIO,
413 U.S. 548 (1973)... 17

United States v. American Trucking Ass'ns,
310 U.S. 534 (1940)... 10

United States v. Bass,
404 U.S. 336 (1971)... 6, 8, 9

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

United States v. Granderson,
511 U.S. 39 (1994)..7

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

United States v. Kozminski,
487 U.S. 931 (1988)..8

United States v. Lanier,
520 U.S. 259 (1997)..14

United States v. Nosal,
676 F.3d 854 (9th Cir. 2012)............................16, 20, 21

United States v. Santos,
553 U.S. 507 (2008)...6, 8, 9

United States v. Valle,
807 F.3d 508 (2d Cir. 2015) 5, 6, 11

United States v. Wiltberger,
18 U.S. 76 (1820)..7

CONSTITUTIONAL PROVISIONS AND STATUTES

U.S. Const. amend. V..13

U.S. Const. art. I, § 7..13

18 U.S.C. § 32 12

18 U.S.C. § 1030(a)(2) 2, 4, 6, 20

18 U.S.C. § 1030(c)(2)(A) 22

18 U.S.C. § 1030(c)(2)(B)..22

18 U.S.C. § 1030(e)(2)(B) 20

18 U.S.C. § 1030(e)(6) 4, 6

OTHER AUTHORITIES

ABA Task Force on Federalization of Criminal Law, The Federalization of Criminal Law (1998).............19

1 William Blackstone, Commentaries...............................7

Defining the Problem and Scope of Over-Criminalization and Over-Federalization: Hearing Before the Over-Criminalization Task Force of 2013 of the H. Comm. on the Judiciary, 113th Cong. 65 (2013) 19

William N. Eskridge, Jr., Dynamic Statutory Interpretation 58 (1994)...12-13

William N. Eskridge, Jr., *Norms, Empiricism, and Canons in Statutory Interpretation*, 66 U. Chi. L. Rev. 671 (1999)..9

Eric. S. Fish, *Constitutional Avoidance as Interpretation and as Remedy*, 114 Mich. L. Rev. 1275 (2016) 18

Forecast on Connected Devices Per Person Worldwide 2003-2020, Statista, https://www.statista.com/statistics/678739/forecast-on-connected-devices-per-person..............................10

John Goglia, *FAA Confirms Shooting A Drone Is A Federal Crime. So When Will U.S. Prosecute?*, Forbes, (Apr. 13, 2016), https://www.forbes.com/sites/johngoglia/2016/04/13/faa-confirms-shooting-drone-federal-crime-so-when-will-us-prosecute/#7ded37222a25 12

The History Of Drones (Drone History Timeline From 1849 To 2019), DroneEthusiast, https://www.dronethusiast.com/history-of-drones/ 12

Internet History 1962 to 1992, Comput. History Museum, https://www.computerhistory.org/internethistory 10

Charles G. Koch and Mark V. Holden, *The Overcriminalization of America*, Politico (Jan. 7, 2015) 20

Tim Lynch, *Overcriminalization, Cato Handbook for Policymakers* 17 (8th ed. 2017), https://www.cato.org/cato-handbook-policymakers/cato-handbook-policy-makers-8th-edition-2017/overcriminalization 19, 20

Note, *The New Rule of Lenity*, 119 Harv. L. Rev. 2420 (2006) 8

Richard A. Posner, *Foreword: A Political Court*, 119 Harv. L. Rev. 31 (2005) 9

S. Rep. No. 99-432, *reprinted in* 1986 U.S.C.C.A.N. 2479 11

Antonin Scalia, *Common-Law Courts in a Civil-Law System: The Role of United States Federal Courts in Interpreting the Constitution and Laws*, *in* A Matter Of Interpretation: Federal Courts And The Law (Amy Gutmann ed., 1997) 13

Sup. Ct. R. 37.1 2

Sup. Ct. R. 37.3(a) 1

Sup. Ct. R. 37.6 1

Indictment, *United States v. Yakubets*, No. 19-CR-342 (W.D. Pa. Nov. 12, 2019), https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens 22

Brian W. Walsh and Tiffany M. Joslyn, *Without Intent: How Congress is Eroding the Criminal Intent Requirement in Federal Law*, The Heritage Found. & NACDL, Apr. 2010 18-19

INTEREST OF THE *AMICUS CURIAE* [1]

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

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

In furtherance of NACDL's mission to safeguard fundamental constitutional rights, NACDL often

---

[1] In accordance with Supreme Court Rule 37.6, *amicus curiae* states that no counsel for a party authored this brief, "in whole or in part," and no counsel or party made a monetary contribution to fund the preparation or submission of this brief. No person other than the *amicus curiae*, its members, and its counsel made any monetary contribution to its preparation and submission. Pursuant to Supreme Court Rule 37.3(a), counsel of record for all parties received notice of *amicus curiae*'s intent to file and both parties have consented to the filing of this brief.

appears as *amicus curiae* in cases involving the proper construction of criminal laws, prosecutorial abuse, overcriminalization, and over-federalization. Because these issues are squarely presented by this case, NACDL urges the Court to define the scope of Section 1030(a)(2) of the Computer Fraud and Abuse Act ("CFAA") such that ordinary computer misuse cannot be prosecuted as a federal crime. Given NACDL's expertise in matters of criminal law, NACDL submits that its views will be of "considerable help" to the Court. Sup. Ct. R. 37.1.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

In this case, the Eleventh Circuit reaffirmed that a person violates the CFAA by using a computer to access information for an improper purpose, even if that person is otherwise authorized to access that information. As Petitioner explains, this holding was wrong on the merits, and Petitioner was wrongfully convicted. Pet. Br. at 16–26. *Amicus* writes separately here to further contextualize how the decision below undermines bedrock principles of criminal law and needlessly furthers the lamentable trend of overcriminalization.

The decision below interpreted the CFAA in a manner that deviates from settled practices for construing federal criminal statutes. It not only embraced a strained reading of the CFAA that goes well beyond the statute's text, but one that fails to account for Congress' intent in enacting it. The CFAA is most naturally read as an anti-hacking statute, a reading that is perfectly consistent with Congress' stated reasons for adopting it.

But perhaps the most egregious aspect of the decision below is its slipshod treatment of the rule of lenity. The rule of lenity is as longstanding a principle of criminal law as is known in Anglo-American law. It exists to ensure that people have fair notice of what is a crime, to minimize the threat of selective or arbitrary enforcement, and to maintain the proper balance between Congress, prosecutors, and courts. Failure to give the rule real and meaningful weight undermines each of these fundamental goals.

The decision below also interpreted the CFAA in a manner that raises obvious due process concerns, both because it is an unconstitutionally vague reading of the statute and because it invites arbitrary and discriminatory enforcement. These manifest constitutional concerns can be avoided only by adopting Petitioner's reading of the statute.

Lastly, the approach embraced by the decision below, if adopted by the Court, stands to drastically expand the CFAA's reach, contributing to the widespread trend of overcriminalization. This is of particular concern to NACDL because overcriminalization both burdens the criminal justice system and wrongfully expands government power at the expense of ordinary liberties. These dangers are only heightened in the context of the CFAA, both due to the ubiquity of computers in daily life and the fact that ordinary computer use is governed by a web of businesses' and websites' access and use policies, meaning the CFAA, if interpreted consistent with the decision below, would subject millions to possible criminal penalties for commonplace computer misuse.

For these reasons, *amicus* respectfully submits that the Eleventh Circuit's ruling should be reversed, and a narrower reading of the CFAA adopted.

ARGUMENT

I. The Eleventh Circuit's Interpretation Of The CFAA Is Contrary To The Statute's Text And Congress' Intent, And Violates The Rule Of Lenity.

Section 1030(a)(2) of the CFAA makes it a federal crime to "intentionally access[] a computer without authorization" or to "exceed[] authorized access." 18 U.S.C. § 1030(a)(2). Congress did not define the term "without authorization," but did define "exceeds authorized access" as "access[ing] a computer with authorization" and "us[ing] 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 question of whether Petitioner has violated the statute Congress wrote hinges on the meaning of "exceed[ing] authorized access" by "obtain[ing] or alter[ing] information" a person is "not entitled so to obtain or alter." In giving meaning to this provision, the Court looks first to the text, while accounting for Congress' intent to the extent the text is ambiguous, with all doubts resolved in favor of a narrower construction pursuant to the rule of lenity. *Green v. Bock Laundry Mach. Co.*, 490 U.S. 504, 508–09 (1989) ("We begin by considering the extent to which the text of [the disputed provision] answers the question before us. Concluding that the text is ambiguous with respect to [that question], we then seek guidance from legislative history"); *Liparota v. United States*, 471 U.S. 419, 427–

28 (1985) (explaining that the rule of lenity "provides a time-honored interpretive guideline when the congressional purpose is unclear" and requires that "'ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity'") (citation omitted). The decision below broke with this approach at every turn.

A. It Is Crucial That The Court Continue To Construe The Text Of Criminal Statutes Narrowly.

Courts construing the meaning of Section 1030(a)(2) have reached differing conclusions, with some courts taking the view espoused by Petitioner that the statute is violated only if a person accesses computer data without permission to do so in any circumstance, and others adopting a more expansive view, in which it *also* is a crime for a person to access computer data with permission if done for an improper purpose. *Compare, e.g.*, *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015) (discussing the narrower view), *with United States v. John*, 597 F.3d 263, 272–73 (5th Cir. 2010) (discussing the more expansive view). As Petitioner explains, the narrower view is the one that is most true to the CFAA's text and purpose. But it also is jurisprudentially important that the narrower view be the one that prevails in this case.

Initially, as Petitioner explains in detail, from a purely textual perspective, this should be an easy case. Pet. Br. at 17–23. The CFAA defines "exceed[ing] authorized access" as being limited to situations where a person accesses a computer "with authorization," but nevertheless "obtain[s] or alter[s] information" in the

computer that they are "not entitled" to obtain or alter. 18 U.S.C. § 1030(e)(6). The reference to "obtaining or altering" information makes clear that this portion of the CFAA is essentially an anti-*internal*-hacking statute that criminalizes accessing information "only when a person has no right at all to access the information." Pet. Br. at 17. This conclusion is bolstered by the remainder of Section 1030(a)(2)'s text, which contains two clauses, one covering those who "intentionally access[] a computer without authorization" and another for those who "exceed[] authorized access" by "obtain[ing] or alter[ing] information" that they are "not entitled so to obtain or alter." 18 U.S.C. §§ 1030(a)(2), (e)(6). The first clause would naturally apply to external hackers, and the second, as explained above, to internal hackers. *See Valle*, 807 F.3d at 524 (citing *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012)). Such internal hacking would, for example, cover situations where an employee only is allowed to access certain files or databases, but nevertheless accesses prohibited areas, such as an accountant accessing confidential human resources files. *See* Pet. Br. at 23–24.

But more broadly, even if there were some arguable textual merit to the expansive reading of the CFAA that the government has promoted, per the rule of lenity it is axiomatic that "the tie must go to the defendant." *United States v. Santos*, 553 U.S. 507, 514 (2008) (concluding that two statutory readings were plausible, and therefore adopting the "more defendant-friendly" one); *see also United States v. Bass*, 404 U.S. 336, 348–49 (1971) (recognizing that Congress had not "'plainly and unmistakably'" criminalized the charged conduct, and

thus adopting the narrower statutory reading) (citation omitted).

The rule of lenity is a common law doctrine which traces its lineage in the United States' jurisprudence to an 1820 opinion of this Court by Chief Justice Marshall, in which the Court rejected the government's expansive reading of a criminal statute and instead construed the statute strictly. *United States v. Wiltberger*, 18 U.S. 76, 95, 105–06 (1820); *see also* 1 William Blackstone, Commentaries on the Laws of England 88 (describing the rule as one of strict construction). In doing so, the Court observed that "[t]he rule that penal laws are to be construed strictly .... is founded on the tenderness of the law for the rights of individuals; and on the plain principle that the power of punishment is vested in the legislative, not in the judicial department." *Wiltberger*, 18 U.S. at 95. Since then, the rule of lenity has remained a "'time-honored interpretive guideline'" in interpreting the nation's criminal laws. *Crandon v. United States*, 494 U.S. 152, 158 (1990) (citation omitted).[2]

[2] In applying the rule of lenity, the Court has in some instances required "'grievous ambiguity or uncertainty in the statute,'" but in numerous other cases has applied the rule of lenity where a statute is simply "ambiguous." *Compare Dean v. United States*, 556 U.S. 568, 577 (2009) ("'To invoke the rule, we must conclude that there is a grievous ambiguity or uncertainty in the statute'") (citations omitted) *with Scheidler v. Nat'l Org. for Women, Inc.*, 537 U.S. 393, 408–09 (2003) (explaining that the rule of lenity should be applied when there is "'any ambiguity'" or if there are "'two rational readings'" of a criminal statute) (citation omitted); *United States v. Granderson*, 511 U.S. 39, 54 (1994) ("[W]here text, structure, and history fail to establish that the Government's position is unambiguously correct—we apply the rule of lenity and resolve the

The rule of lenity compels that Petitioner's view of the CFAA prevail for three reasons.

For one, favoring Petitioner's view over an expansive one "ensures that criminal statutes will provide fair warning concerning conduct rendered illegal." *Liparota*, 471 U.S. at 427; *Bass*, 404 U.S. at 348 ("'[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.'") (citation omitted). It certainly cannot be said that anyone familiar with the text of Section 1030(a)(2) would have fair warning that the authorized access of computer data, for an inappropriate purpose, is a crime.

For another, the rule of lenity helps to "minimize the risk of selective or arbitrary enforcement" of criminal statutes, *United States v. Kozminski*, 487 U.S. 931, 952 (1988), and "foster[s] uniformity in the interpretation of criminal statutes," *Bryan v. United States*, 524 U.S. 184, 205 (1998) (Scalia, J., dissenting). In so doing, it also

---

ambiguity in [defendant]'s favor."); *Santos*, 553 U.S. at 514 (applying the rule without noting that the criminal statute satisfied any heightened degree of ambiguity). Of these, the ambiguity standard is most consistent with the rule's origins and purpose. *See Holloway v. United States*, 526 U.S. 1, 21 (1999) (Scalia, J., dissenting) (explaining that the "grievous ambiguity" standard threatened to "reduce" the rule of lenity from a "presupposition of our law" to "a historical curiosity"); Note, *The New Rule of Lenity*, 119 Harv. L. Rev. 2420, 2424–25 (2006) (noting the "grievous ambiguity" standard is "much weaker than the version of the rule [of lenity] articulated in earlier cases" and its use "adds credibility to critics' claims that [the rule of lenity] is no longer being faithfully applied").

generates "greater objectivity and predictability" in the construction and application of criminal laws. William N. Eskridge, Jr., *Norms, Empiricism, and Canons in Statutory Interpretation*, 66 U. Chi. L. Rev. 671, 678–79 (1999).

Equally important, applying the rule of lenity and adopting the narrower view of criminal statutes "strikes the appropriate balance between the legislature, the prosecutor, and the court in defining criminal liability." *Liparota*, 471 U.S. at 427; *see also Bass*, 404 U.S. at 348 (recognizing that, "because of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity"). The rule of lenity thus "places the weight of inertia upon the party that can best induce Congress to speak more clearly and keeps courts from making criminal law in Congress's stead." *Santos*, 553 U.S. at 514.

Similarly, but beyond the rule of lenity, adopting Petitioner's view of the CFAA also respects the fundamental principle of judicial modesty. As the Court has recognized, its members "are vested with the authority to interpret the law[,]" but "possess neither the expertise nor the prerogative to make policy judgments," as those are "entrusted to our Nation's elected leaders." *Nat'l Fed'n of Indep. Bus. v. Sebelius*, 567 U.S. 519, 538 (2012); *see also* Richard A. Posner, *Foreword: A Political Court*, 119 Harv. L. Rev. 31, 55–56 (2005) (explaining that, "in the modest role," the Justice is "a timid politician"). Such judicial modesty is particularly important when criminal statutes are

involved, as it ensures the judiciary does not create a crime that the legislature did not intend.

So while an expansive reading of the CFAA's statutory text fails at the outset as a purely textual matter, whatever arguable ambiguity exists in the text gets the government nowhere. Its expansive textual view *still* fails because it is contrary to these basic protections. Thus, the approach of the decision below should be rejected.

B. Congress Could Not Have Intended An Expansive Reading Of The CFAA.

When a court interprets a federal statute, it seeks "to construe the language so as to give effect to the intent of Congress." *United States v. American Trucking Ass'ns*, 310 U.S. 534, 542 (1940). When Congress passed the CFAA, it did not—and could not—have taken into account the ubiquity of computer use today. At the start of 1986, the year Congress enacted the CFAA, there were 2,000 total networks connected via the Internet. *Internet History 1962 to 1992*, Comput. History Museum, https://www.computerhistory.org/internethistory. For 2020, "forecasts suggest that there will be around 6.58 network connected devices *per person* around the globe," meaning that "there could be nearly 50 billion network connected devices." *Forecast on Connected Devices Per Person Worldwide 2003-2020*, Statista, https://www.statista.com/statistics/678739/forecast-on-connected-devices-per-person. (emphasis added). Nor was Congress in any position to account for the myriad ways computer use today is regulated by employers and others.

It thus represents a massive expansion of the CFAA's anticipated reach to apply it as broadly as the government's theory of liability would require. Congress enacted the CFAA "to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data." *Valle*, 807 F.3d at 525 (citing H.R. Rep. No. 98–894, *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691–92, 3695–97 (1984); S. Rep. No. 99–432, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2480 (1986)). The House Committee Report written in conjunction with the original 1984 bill confirms this, as it identifies "'hackers' who have been able to access (trespass into) both private and public computer systems.'" *Id.* (citing H.R. Rep. No. 98–894, at 3695). Likewise, the Senate Committee Report, written in conjunction with the CFAA's 1986 amendment, provided examples of the type of activity it intended the CFAA to address. One such example concerned "a group of adolescents" who "broke into the computer system at Memorial Sloan-Kettering Cancer Center in New York" and thereby "gained access to the radiation treatment records of 6,000 past and present cancer patients and had at their fingertips the ability to alter the radiation treatment levels that each patient received." S. Rep. No. 99-432, at 2–3, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2480. Another example concerned "pirate bulletin boards" created "for the sole purpose of exchanging passwords to other people's computer systems." *Id.*

The immediate concern that animated the legislation thus was the potential harm caused by a "trespass"—unauthorized access to computer data. Accordingly, expanding the CFAA's reach beyond this, without any

indication Congress so intended, risks defying Congress' intent.

More broadly, interpreting the CFAA expansively here, absent any such indication from Congress, would have ramifications far beyond this case. It would give courts leave to disregard the meaning of all sorts of criminal statutes, as understood at the time of their passage, whenever a technological change, common of this era, breathes new life into a statute. It also would give prosecutors and courts a backdoor means of updating the criminal laws, laws Congress is tasked with writing, in response to changed technological—or potentially cultural, economic, or political—realities. This could, for example, mean that the traditional understanding of "aircraft" is disregarded, such that someone who shoots down a neighbor's toy drone faces the same weighty criminal charge as someone who shoots down a commercial airliner, despite that the relevant statute Congress enacted, 18 U.S.C. § 32, has not been amended by Congress since early 2006, the same year the FAA issued its very first commercial drone permits. *See* John Goglia, *FAA Confirms Shooting A Drone Is A Federal Crime. So When Will U.S. Prosecute?*, Forbes, (Apr. 13, 2016), https://www.forbes.com/sites/johngoglia/2016/04/13/faa-confirms-shooting-drone-federal-crime-so-when-will-us-prosecute/#7ded37222a25; *The History Of Drones (Drone History Timeline From 1849 To 2019)*, DroneEthusiast, https://www.dronethusiast.com/history-of-drones/ (last visited July 7, 2020).

Although some have advocated for such a dynamic approach to statutory interpretation, *see e.g.*, William N.

Eskridge, Jr., Dynamic Statutory Interpretation 58 (1994), "[i]t is simply not compatible with democratic theory that laws mean whatever they ought to mean, and that unelected judges decide what that is," Antonin Scalia, *Common-Law Courts in a Civil-Law System: The Role of United States Federal Courts in Interpreting the Constitution and Laws*, *in* A Matter Of Interpretation: Federal Courts And The Law 22 (Amy Gutmann ed., 1997); *see also Kimble v. Marvel Entm't, LLC*, 576 U.S. 446, 463 (2015) (explaining that "Congress, not this Court, is [the] proper audience" for these kinds of arguments). Our constitutional structure requires that Congress, not courts, amend statutes to account for such changes. *See* U.S. Const. art. I, § 7. Maintaining this critical distinction is even more important when criminal statutes are involved.

II. Expansively Construing The CFAA Raises Constitutional Concerns.

The Fifth Amendment provides that "[n]o person shall … be deprived of life, liberty, or property, without due process of law." U.S. Const. amend. V. The government violates this guarantee by "taking away someone's life, liberty, or property under a criminal law so vague that it fails to give ordinary people fair notice of the conduct it punishes, or so standardless that it invites arbitrary enforcement." *Johnson v. United States*, 135 S. Ct. 2551, 2556–57 (2015) (citing *Kolender v. Lawson*, 461 U.S. 352, 357–58 (1983)); *see also Skilling v. United States*, 561 U.S. 358, 402–03 (2010) (explaining that, to satisfy due process, "'a penal statute [must] define the criminal offense [1] with sufficient definiteness that ordinary people can understand what

conduct is prohibited and [2] in a manner that does not encourage arbitrary and discriminatory enforcement'") (citation omitted). Although there is no such danger under the narrower view, the decision below's expansive approach to the CFAA invites both results.

A. Expansively Construing The CFAA Raises Vagueness Concerns.

It is axiomatic that criminal statutes must make "reasonably clear at the relevant time that the defendant's conduct was criminal." *United States v. Lanier*, 520 U.S. 259, 267 (1997). Thus, statutes must "describe with sufficient particularity what a suspect must do in order to satisfy the statute," *Kolender v. Lawson*, 461 U.S. 352, 361 (1983), such that "the ordinary citizen" can conform their conduct to the law and not "'speculate as to the meaning of penal statutes,'" *City of Chicago v. Morales*, 527 U.S. 41, 58 (1999) (citation omitted). When a statute fails to provide such guidance, it will be invalidated.

For example, in *Morales*, the Court invalidated a criminal statute that prohibited "loitering" where that had been defined as "remain[ing] in any one place with no apparent purpose." 527 U.S. at 47, 56. In so doing, the Court observed it would be "difficult to imagine how any citizen … standing in a public place … would know if he or she had an 'apparent purpose,'" including when simply engaging in commonplace activities such as "talking to another person" or "frequently checking [their] watch and looking expectantly down the street." *Id.* at 56–57. Similarly, the Court in *Coates* invalidated a statute prohibiting persons from assembling in an "annoying" manner because the statute's sweep depended entirely

on others' determinations of what was "annoying." *Coates v. City of Cincinnati*, 402 U.S. 611, 611–16 (1971).

Here, the decision below reaffirmed an interpretation of the CFAA so expansive that it would capture every instance where a person "misuses" a computer they are otherwise authorized to use by accessing information for an "inappropriate reason," including for a "nonbusiness" purpose. Pet. App. 26a–28a. The limits of this, however, are undefined, and raise issues akin to those in *Morales* and in *Coates*.

As in *Morales* where the "loitering" definition failed to specify when persons lacked an "apparent" purpose, expansively interpreting the CFAA would leave people guessing regarding when, exactly, they had accessed something for an inappropriate reason. Would they, for example, be deemed to have done so merely because they opened a photo of a colleague's recent vacation attached to an otherwise work-related email? What if they perhaps accessed their personal email from a work computer, even simply to verify information they needed to provide to human resources? Or what if they instead accessed the internet for no other reason than to locate a joke or inspirational quote to send to a colleague, or to buy a gift to congratulate their colleague regarding a new job or the birth of a baby? Each of these commonplace situations could run afoul of the CFAA, simply because they involved accessing information on a work computer for an inappropriate reason in violation of an employer's computer access policy—one simply could not know from the CFAA's text alone.

Similarly, as in *Coates*, where criminality depended on what third-parties deemed to be "annoying," under

the decision below's theory of CFAA liability, criminality would be entirely dependent on third-parties'—including employers', internet providers', websites', and others'—ever-changing determinations of what was improper. Thus, as in *Morales* and in *Coates*, an expansive reading of the CFAA would fail to provide fair notice of illegal conduct or allow persons to conform their activities accordingly.

B. Expansively Construing The CFAA Invites Arbitrary Enforcement.

The reach of a criminal statute also must not be so broad as to invite arbitrary and discriminatory enforcement. A legislature thus must "'establish minimal guidelines to govern law enforcement.'" *Morales*, 527 U.S. at 60 (citation omitted). Without such guidance, a law will be invalidated on constitutional grounds. *Id.* at 60–64. By way of example, in invalidating the loitering statute in *Morales*, the Court noted that the statute "'provide[d] absolute discretion to police officers to decide what activities constitute loitering.'" *Id.* at 61 (citation omitted). Likewise, adopting an expansive interpretation of the CFAA here would also "invite arbitrary and discriminatory enforcement." *See United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012). That is, it would provide law enforcement with no meaningful guidance to determine when persons had accessed information for an unauthorized purpose.

The government has previously argued these concerns can be assuaged because the Attorney General issued a Charging Policy in 2014 setting forth factors that Department of Justice attorneys should consider when deciding whether to pursue a prosecution under

Section 1030 of the CFAA. *See* BIO at 16–18. As Petitioner has explained, however, this gets the government nowhere. Pet. Br. at 2–3, 32–33. That is particularly true with respect to concerns of arbitrary enforcement. The Court rejected a very similar argument in *Morales*, as the police department there had issued a general order intended to limit the discretion granted to the police in enforcing the loitering statute. The Court deemed such internal guidelines insufficient, because a person still could not "safely assume" that adverse action would not be taken against them pursuant to the loitering statute. *Morales*, 527 U.S. at 63–64. The Charging Policy here likewise can offer no such comfort. Indeed, far from denouncing prosecutions premised solely on situations where "'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,'" the Charging Policy counsels merely that such prosecutions "'may'" not be warranted. *See* Pet. Br. at 32–33 (citing 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)).

* * * *

The constitutional problems presented by the approach to the CFAA taken by the decision below are clear and undeniable. Yet the Court should endeavor to construe the CFAA so as to preserve it, rather than invalidate it. *See United States Civil Serv. Comm'n v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 413 U.S. 548, 571 (1973) ("[O]ur task is not to destroy the Act if we can,

but to construe it, if consistent with the will of Congress, so as to comport with constitutional limitations.").

This is so per the doctrine of constitutional avoidance, in which courts "faced with two plausible constructions of a statute"—one constitutional and another unconstitutional—are "commanded" to choose the constitutional reading. *See Clark v. Martinez*, 543 U.S. 371, 395 (2005) (Thomas, J., dissenting); *see also Blodgett v. Holden*, 275 U.S. 142, 148 (1927) (Holmes, J., concurring) (explaining that, "as between two possible interpretations of a statute, by one of which it would be unconstitutional and by the other valid, our plain duty is to adopt that which will save the Act"). This principle should apply in full even if the Court has mere doubts regarding the constitutionality of one possible statutory interpretation. Thus, the Court still should "adopt the interpretation free from constitutional doubt." *See Clark*, 543 U.S. at 391; Eric. S. Fish, *Constitutional Avoidance as Interpretation and as Remedy*, 114 Mich. L. Rev. 1275, 1283 (2016) (explaining how modern avoidance "prevents a court from issuing advisory opinions").

The due process failings of the CFAA, as read in the decision below, are unavoidable. Because Petitioner's narrower construction of the CFAA evades these flaws, it should be the one the Court adopts.

III. Expansively Interpreting The CFAA Would Further Overcriminalization.

According to a 1998 report published by the American Bar Association's Task Force on the Federalization of Crime, 40% of all federal criminal provisions passed into law during the 132-year period from the end of the Civil

War to 1996 were enacted in the twenty-six years from 1970 to 1996. Brian W. Walsh and Tiffany M. Joslyn, *Without Intent: How Congress is Eroding the Criminal Intent Requirement in Federal Law*, The Heritage Found. & NACDL, Apr. 2010, at 6. Since then, federal crimes have proliferated to such an extent that the American Bar Association's Task Force on the Federalization of Criminal Law stated that "the present body of federal criminal law" had grown "[s]o large" that there was "no conveniently accessible, complete list of federal crimes." ABA Task Force on Federalization of Criminal Law, The Federalization of Criminal Law (1998), at 9.

Not even the federal government can determine the exact number of federal crimes in existence. Evidencing this, when the Congressional Research Service ("CRS") was asked to provide a list of all federal crimes, CRS' initial response, according to Congressman John Sensenbrenner, Chairman of the Over-criminalization Task Force of 2013, was that CRS "lack[ed] the manpower and resources to accomplish this task." As noted by the Congressman, CRS's response alone "demonstrates the breadth of over-criminalization." *See Defining the Problem and Scope of Over-Criminalization and Over-Federalization: Hearing Before the Over-Criminalization Task Force of 2013 of the H. Comm. on the Judiciary*, 113th Cong. 65 (2013).

Overcriminalization causes wide ranging detrimental effects. It undermines the bedrock American value of freedom, because "a society in which the criminal rules are so pervasive that no one is safe from arrest and prosecution cannot be described as free." Tim Lynch, *Overcriminalization, Cato Handbook for Policymakers*

17, 195–96 (8th ed. 2017), https://www.cato.org/cato-handbook-policymakers/cato-handbook-policy-makers-8th-edition-2017/overcriminalization. It also burdens the criminal justice system by spreading resources thinly across a broader range of enforcement priorities, often away from more serious crimes. *Id.* And it leads to more governmental errors, including wrongful arrests, prosecutions, and imprisonment. *Id.*

Overcriminalization also contributes to poverty and mass incarceration. Upon release, those incarcerated can expect decreased earnings and higher unemployment. *See* Charles G. Koch and Mark V. Holden, *The Overcriminalization of America*, Politico (Jan. 7, 2015). In fact, one study concluded that, absent mass incarceration, "poverty would have decreased by more than 20 percent" and "several million fewer people would have been in poverty." *Id.* Yet, as of 2015, the United States housed approximately twenty-five percent of the world's prisoners, despite representing just around five percent of the world's population. *Id.*

If the Court reads the CFAA consistent with the decision below, the Court would exacerbate this already concerning and growing trend. This is particularly true both because Section 1030(a)(2) of the CFAA applies to information obtained from every computer with an internet connection, 18 U.S.C. §§ 1030(a)(2), (e)(2)(B); *Nosal*, 676 F.3d at 859, and because an expansive theory of CFAA liability would criminalize every situation where a person accesses information for an improper purpose, including in violation of businesses' and websites' computer access and use policies, such as "the

typical corporate policy that computers can be used only for business purposes," *Nosal*, 676 F.3d at 860–61.

Thus, adopting an expansive reading of the CFAA would instantaneously transform common, seemingly innocuous instances of computer misuse—such as utilizing a work computer to "chat[] with friends," "shop[]," or "watch[] sports highlights"—into federal crimes throughout the entire nation. *See id*. "This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *Nosal*, 676 F.3d at 859.

To minimize this reality, the government previously asserted that Petitioner had not "identif[ied] any case in which *a court of appeals* has determined that the statute authorizes the prosecution of someone who engages in such 'commonplace activities' involving the violation of private computer-use policies." BIO at 16 (emphasis added). But the government has not waited for any court of appeals to bless these prosecutions and, unsurprisingly, prosecutors have already utilized the CFAA to do exactly what the government discounts—to bring serious federal criminal charges against defendants under the CFAA premised on ordinary terms-of-use violations. Thus, in *United States v. Drew*, the defendant was indicted for three counts of violating a felony portion of the CFAA, predicated entirely on a violation of the website MySpace's terms of service. *United States v. Drew*, 259 F.R.D. 449, 452–54 (C.D. Cal. 2009).

Indeed, if the Court were to interpret the CFAA consistent with the government's theory of liability, prosecutors would have discretion to treat any computer

use violation as a federal crime that would, nonsensically, be equated to computer hacking by foreign nationals. *Compare Drew*, 259 F.R.D. at 452 (explaining that "Drew was charged with … three counts of violating a felony portion of the CFAA, *i.e.*, 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii)") *with* Indictment at 13, *United States v. Yakubets,* No. 19-CR-342 (W.D. Pa. Nov. 12, 2019), https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens (indicting two foreign nationals for, among other things, computer hacking pursuant to 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)).

The danger of overcriminalization is even more acute in the context of the CFAA because of the substantial criminal penalties that CFAA violations carry. An initial conviction under 18 U.S.C. § 1030(a)(2)—the one at issue in this case—is punishable by fines and imprisonment of up to one year, or up to five years in certain situations, including where the offense was committed for "private financial gain." 18 U.S.C. § 1030(c)(2)(A), (B). Applying the framework under the decision below, this means someone who uses a work computer to make changes to a retirement savings account, in violation of their employer's computer use policy, could face up to five years in federal prison. Permitting such weighty penalties for such frequent, innocuous activity serves no legitimate purpose, and needlessly promotes overcriminalization.

The Court previously has rejected similar attempts by the government to exponentially expand the breadth of criminal statutes. *See generally e.g.*, *Bond v. United*

States, 572 U.S. 844, 863 (2014) (rejecting government's interpretation of statute which threatened to "transform the statute from one whose core concerns are acts of war, assassination, and terrorism into a massive federal anti-poisoning regime that reaches the simplest of assaults."). The Court's restraint in interpreting the CFAA is likewise warranted here.

CONCLUSION

For the foregoing reasons, *amicus curiae* the National Association of Criminal Defense Lawyers urge the Court to construe Section 1030(a)(2) of the CFAA more narrowly and reverse Petitioner's conviction.

July 8, 2020

Respectfully submitted,

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

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

Counsel for Amicus Curiae The National Association of Criminal Defense Lawyers