No. 19-783

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES,

Respondent.

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

BRIEF FOR *AMICUS CURIAE* AMERICANS FOR PROSPERITY FOUNDATION IN SUPPORT OF PETITIONER

R. James Valvo, III
Counsel of Record
Michael Pepson
AMERICANS FOR PROSPERITY FOUNDATION
1310 N. Courthouse Road, Ste. 700
Arlington, VA 22201
(571) 329-4420
jvalvo@afphq.org

Counsel for Amicus Curiae

July 8, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Constitution

Statutes

Other Authorities

BRIEF OF *AMICUS CURIAE* IN SUPPORT OF PETITIONER

Under Supreme Court Rule 37.3(a), Americans for Prosperity Foundation ("AFPF") respectfully submits this *amicus curiae* brief in support of Petitioner.[1]

INTEREST OF *AMICUS CURIAE*

AFPF is a 501(c)(3) nonprofit organization committed to educating and training Americans to be courageous advocates for the ideas, principles, and policies of a free and open society. Some of those key ideas are the separation of powers, constitutionally limited government, due process, and the rule of law. As part of this mission, it appears as *amicus curiae* before federal and state courts.

AFPF believes that the real-world stakes here are high and radiate far beyond the specific facts of this case. If allowed to stand, the Eleventh Circuit's erroneous interpretation of the Computer Fraud and Abuse Act's ("CFAA") proscription against exceeding authorized computer access could extend to violations of the fine print in website terms of service, company computer-use policies, and other breaches of contract. That would wrongly criminalize a wide swath of innocent, innocuous conduct turning millions of honest, hardworking Americans into federal criminals

---

[1] All parties have consented to the filing of this brief. *Amicus* states that no counsel for a party authored this brief in whole or in part and that no person other than *amicus* or its counsel made any monetary contributions intended to fund the preparation or submission of this brief.

left to the mercy of the federal government. Worse, it turns private individuals and companies into super-legislatures with the power to create new federal crimes in the fine print of private contracts. This, in turn, jeopardizes the exercise of fundamental First Amendment rights by journalists and others, thereby wrongly threatening the marketplace of ideas vital to our system of self-governance.

Particularly in today's environment, with many Americans working remotely and regularly using computers, it is critical for this Court to foreclose the possibility that private companies could use website terms of service as a mechanism to criminalize speech and thereby chill the exercise of core First Amendment rights. This is particularly true with respect to online newspapers and search engines that may exercise control over the flow of core political speech and may silence or remove dissenting voices.

SUMMARY OF ARGUMENT

It is a safe assumption that many ordinary people do not read the fine print legalese in dense, lengthy website terms-of-service documents posted on popular social media websites like Facebook, YouTube, LinkedIn, and Twitter, or on subscription-based services like Netflix, all of which have tens of millions of users. Unsurprisingly, then, many users unknowingly violate those terms of service by, for example, sharing a log-in password, shading the details about their age, or fudging the details about their past employment history. Journalists, too, may create fictious profiles as part of an investigation about matters of public concern, in violation of website terms of service.

It is also reasonable to surmise that millions of Americans may, from time to time, use their work computers to check a sports score, check the local news, make a reservation at a restaurant, or perhaps check their personal email account. For those who work for companies that have a computer-use policy prohibiting use for non-business purposes, this is a technical violation of company policy.

Are these people federal criminals? The answer should be "no." It should be safe to assume that private companies cannot expand the reach of federal criminal law in the fine print of terms of use or company policies. And common sense suggests that this sort of innocuous conduct should not give rise to federal criminal liability. But under the Government's reading of the CFAA—a statute originally enacted decades ago to target computer hackers who break into government computers—the answer would be "yes."

That cannot be the law. This is so for the reasons Petitioner explains, *see* Pet. Br. 17–41, as the CFAA's plain language, structure, and history squarely foreclose such an absurd, overbroad construction. If it were otherwise, Section 1030(a)(2) of the CFAA would be:

- Void for vagueness under the First and Fifth Amendments;

- Violate due process for failure to give fair notice of prohibited or required conduct, and by creating fertile grounds for arbitrary and seriously discriminatory enforcement; and

- Violate Article I's Vesting Clause and the separation of powers by delegating to private businesses and individuals the power to "create" new federal crimes through the fine print in website terms of service and employment contracts.

In addition to the obvious constitutional problems, the practical consequences of adopting the Government's proposed interpretation would be sweeping. Trivial everyday activities of millions of ordinary Americans would become federal crimes, leaving them at the mercy of the *noblesse oblige* and whim of federal prosecutors.

To avoid these serious and far reaching constitutional and practical problems, this Court should construe the CFAA narrowly, consistent with its text, structure, and history, and the U.S. Constitution. The CFAA's proscription against intentionally exceeding authorized access to computers solely targets hackers; that is, individuals who use computers to break into government and business networks to steal data for nefarious purposes such as sensitive personal information used to facilitate identity theft, sensitive corporate documents, or classified information. It does not criminalize breaches of private contracts, garden-variety website terms-of-service violations, or other broad swaths of innocuous behavior. Nor does it criminalize the actions of a person who is authorized to access information on a computer for certain purposes but who accesses the same information for an improper purpose, as allegedly happened here.

ARGUMENT

I. CONSTRUING THE CFAA TO EXTEND BEYOND COMPUTER HACKING CREATES A MAJOR OVERCRIMINALIZATION PROBLEM.

A. Section 1030(a)(2) of the CFAA: A Recipe for Overcriminalization

"The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking," and it "is best understood as an anti-intrusion statute." *HiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1000 (9th Cir. 2019). It is intended to target intrusions by hackers who use the Internet to break into government and corporate computers to steal sensitive data like classified information, trade secrets and other valuable intellectual property, and sensitive personal information used to facilitate identity theft.

Consistent with this overarching focus, this anti-hacking statute traces its genesis to the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190-92; *see also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130–31 (9th Cir. 2009). As originally enacted, the CFAA was "a narrow statute designed to criminalize unauthorized access to computers." Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1561 (2010). "The CFAA is concerned with the *unauthorized access* of protected computers." *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (emphasis added). It was "originally designed to criminalize only important federal interest computer

crimes," like "certain computer misuse relating to natural security, financial records, and government property." Kerr, 94 Minn. L. Rev. at 1561 & n.5.

Unfortunately, however, Congress has amended the statute to remove statutory guardrails and culpability requirements strictly cabining its reach to the mine run of hacking activities. *See id*. at 1563–1571 (discussing in detail how Congress has expanded the scope of the CFAA over time). Concordant with Congress's expansion of the CFAA's scope over the years, our society has become increasingly interconnected and reliant on technology in our personal and professional lives.

These parallel expansions create a toxic mixture of the key ingredients for the problem of overcriminalization, framing what is at stake here:

> Computers have become an indispensable part of our daily lives. We use them for work; we use them for play. Sometimes we use them for play at work. Many employers have adopted policies prohibiting the use of work computers for nonbusiness purposes. Does an employee who violates such a policy commit a federal crime? How about someone who violates the terms of service of a social networking website? This depends on how broadly we read the Computer Fraud and Abuse Act[.]

United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc) (Kozinski, C.J.). Judge Kozinski's prescient observations hold particularly true now, as

tens of millions of Americans work remotely from home, conduct meetings and business virtually online, meet with their healthcare providers remotely, and order food and supplies over the Internet. This case thus "brings to the surface the real issue: overcriminalization and excessive punishment in the U.S. Code."[2] *Yates v. United States*, 574 U.S. 528, 569 (2015) (Kagan, J., dissenting).

The root of the problem is Subsection 1030(a)(2)(C) of the CFAA, which makes it a crime to obtain "information from any protected computer" by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer."[3] 18 U.S.C. § 1030(a)(2)(C); *see also id*. § 1030(e)(6) ("the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter").

---

[2] "The main problem with overcriminalization is that it results in crimes that are often . . . poorly defined in ways that exacerbate their already considerable breadth and punitiveness, maximize prosecutorial power, and undermine the goal of providing fair warning of the acts that can lead to criminal liability." Stephen F. Smith, *Overcoming Overcriminalization*, 102 J. Crim. L. & Criminology 537, 565 (2012).

[3] "Protected computers" are computers "used in or affecting interstate or foreign commerce or communication," 18 U.S.C. § 1030(e)(2)(B), *i.e.*, every computer with an Internet connection. Likewise, the term "computer" is broadly defined to extend to basically any Internet-accessible device (*e.g.*, smart phone, tablet). *See id.* § 1030(e)(1) (defining "computer").

As the broadest provision of the CFAA, "subsection 1030(a)(2)(C) . . . makes it a crime to exceed authorized access of a computer connected to the Internet without any culpable intent." *Nosal*, 676 F.3d at 859. *But cf. Rehaif v. United States*, 139 S. Ct. 2191, 2195 (2019). Violations are punishable by a fine or imprisonment for up to one year, or both. *See* 18 U.S.C. § 1030(c)(2)(A).[4]

B. The Government's Interpretation of the CFAA Wrongly Criminalizes a Broad Swath of Innocent Conduct.

In the Government's view, under the CFAA, "exceeds-authorized-access violations may occur where the actor had authorization to access the computer for one purpose but accessed the computer for a prohibited purpose."[5] This appears to logically include violations of company computer-use policies and website terms of service; that is, any garden-variety breach of contract involving a computer.[6]

Now consider the implications of the broad reading of Subsection 1030(a)(2)(C)'s proscription against

---

[4] The misdemeanor becomes a felony, punishable by imprisonment for up to five years, if "the offense was committed for purposes of commercial advantage or private financial gain." 18 U.S.C. § 1030(c)(2)(B)(i).

[5] Intake and Charging Policy for Computer Crime Matters, Memorandum from U.S. Att'y Gen. to U.S. Att'ys and Asst. Att'y Gens. for the Crim. and Nat'l Sec., at 4 (Sept. 11, 2014) [hereinafter "Charging Policy"], *available at* https://bit.ly/3cJenCh.

[6] *See id.* at 4–5; *see also* J.A. 38–39.

exceeding unauthorized access urged by the Government:

- **Workplace "Crimes":** "Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes."[7] *Nosal*, 676 F.3d at 860.

- **Criminalization of Password Sharing and High-School Students' Educational Research:** With respect to a search engine that "forbade minors from using its services. Adopting the government's interpretation would turn vast numbers of teens and pre-teens into juvenile delinquents—and their parents and teachers into delinquency contributors. Similarly, . . . [a social media platform] makes it a violation of the terms of service to let anyone log into

---

[7] "Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars." *Nosal*, 676 F.3d at 860.

your account. Yet it's very common for people to let close friends and relatives check their email or access their online accounts. Some may be aware that, if discovered, they may suffer a rebuke from the ISP or a loss of access, but few imagine they might be marched off to federal prison for doing so." *Id.* at 861 (citations omitted).

- **Website Terms-of-Service "Crimes"**: "[N]umerous dating websites whose terms of use prohibit inaccurate or misleading information. Or . . . [consider online sales platforms], where it's a violation of the terms of use to post items in an inappropriate category. Under the government's proposed interpretation of the CFAA, posting for sale an item prohibited by . . . [a platform's] policy, or describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit." *Id.* at 861–62 (citation omitted).[8]

Additional examples abound.[9] Put simply, the consequences of accepting the Government's liability theory will radiate far beyond this case. *See Nosal*, 676 F.3d at 862 (criticizing courts that, in interpreting

---

[8] By contrast, this Court struck down as inconsistent with the First Amendment the Stolen Valor Act, which criminalized lying about military decorations and medals. *See United States v. Alvarez*, 567 U.S. 709 (2012).

[9] *See* Statement of Orin S. Kerr, U.S. House of Representatives Subcommittee on Crime, Terrorism, Homeland Security and Investigations, "Investigating and Prosecuting 21st Century Cyber Threats," at 9 (Mar. 13, 2013) [hereinafter "Statement of Orin S. Kerr"], *available at* https://bit.ly/37eMDnG.

the CFAA, "looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of 'exceeds authorized access.'"); *Miller*, 687 F.3d at 206 (rejecting CFAA liability theory with "far-reaching effects unintended by Congress."). If this Court adopts the Government's proposed construction, "millions of unsuspecting individuals would find that they are engaging in criminal conduct." *Nosal*, 676 F.3d at 859. This is particularly true because Section 1030(a)(2) does not contain any meaningful *mens rea* (*i.e.*, culpable criminal intent) requirement, thereby potentially criminalizing a broad array of innocent, innocuous conduct that most people would not dream would be unlawful, let alone a federal crime.

After all, "subsection 1030(a)(2)(C) . . . makes it a crime to exceed authorized access of a computer connected to the Internet *without any culpable intent*." *Nosal*, 676 F.3d at 859. This is so because, as Professor Orin Kerr, a preeminent legal scholar who has written extensively about (and represented clients charged with violating) the CFAA has testified:

> It is true that the statute requires that the exceeding of authorized access be "intentional," but this is a very modest requirement because the element itself is so easily satisfied. Presumably, any user *who knows that the Terms of Use* ***exist***, and who intends to do the conduct that violated the Term of Use, will have "intentionally" exceeded authorized access.

Statement of Orin S. Kerr at 9 (emphasis added). Put differently, even though "most people are only dimly aware of and virtually no one reads or understands" these private agreements and website policies, *see Nosal*, 676 F.3d at 861, ignorance as to the specific terms and conditions of use would presumably not be a defense to criminal liability under the Government's overbroad interpretation of Section 1030(a)(2). *Cf. Bryan v. United States,* 524 U.S. 184, 193–95 (1998).

Therefore, Section 1030(a)(2)'s "exceeds authorized access" language necessarily plays a key gatekeeping function in establishing the limits of the CFAA's reach and screening out innocent, innocuous Internet-related conduct from the hacking-related intrusions Congress intended to target and criminalize. *Cf. Kelly v. United States*, 140 S. Ct. 1565 (2020) (money-or-property requirement in federal property fraud statutes "prevents these statutes from criminalizing all acts of dishonesty by state and local officials"). And as Professor Kerr has explained elsewhere: "If we interpret the phrase 'exceeds authorized access' to include breaches of contract, we create a remarkably broad criminal prohibition that has no connection to the rationales of criminal punishment." Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U.L. Rev. 1596, 1663 (2003). Blithely dispensing with any meaningful culpability inquiry by criminalizing mere breaches of contract without any clear indication that Congress intended such an absurd result would also appear to be "inconsistent with our philosophy of criminal law." *Morissette v. United States*, 342 U.S. 246, 250 (1952). And as other legal scholars have noted, "as long as

courts fail to make proof of a culpable mental state an unyielding prerequisite to punishment, federal prosecutors will continue to water down mens rea requirements in ways that allow conviction without blameworthiness." Smith, 102 J. Crim. L. & Criminology at 574.

C. A Case Study in "Exceeding Authorized Access" Overcriminalization

This concern is not speculative. Consider, for example, *United States v. Drew* where a jury found the defendant guilty of violating the CFAA because she violated MySpace's terms of service by creating a fake profile and posting a fake picture for the purpose of communicating with a teenager. 259 F.R.D. 449, 461 (C.D. Cal. 2009).[10] *See generally* Trent England, Andrew M. Grossman, and Erica A. Little, *The MySpace Suicide Case*, pp. 79–95, *in* One Nation Under Arrest: How Crazy Laws, Rogue Prosecutors, and Activist Judges Threaten Your Liberty (2010). In the so-called MySpace suicide case, the defendant, Lori Drew, was far from sympathetic, and her "cyberbullying" actions may have had some impact on the tragic suicide of the teenager she communicated with using the fake MySpace profile.[11] But using the

---

[10] This is not the only example of CFAA prosecutions based at least in part on terms-of-service violations. *See* Pet. Br. 32–33; *see also* Victor Manolache, *Computer Fraud and Abuse or Prosecutorial Fraud and Abuse: Time for Change*, 5 J. of Law, Tech. & the Internet 67 (2015).

[11] *See generally* Emily Bazelon, *Lori Drew Is a Meanie: The Problem with Prosecuting Cyber-bullying*, SLATE (Dec. 3, 2008), https://bit.ly/30m31Sc.

Internet as a vehicle to be a jerk to others and to say mean and senseless things to other people for irrational, and even cruel, reasons—however immoral it may be—is not a federal crime under the CFAA.

Accordingly, the Government's overreaching, wayward prosecution of Drew for violating the CFAA drew widespread criticism for bearing all of the hallmarks of the overcriminalization problem in the United States:

- The decline of *mens rea* requirements as a protection against unfair criminal liability;
- The arbitrary nature of modern criminal offenses that provide citizens with no notice that their conduct may be illegal;
- Extremely broad liability that threatens to make millions of citizens criminals;
- Politics and public opinion trumping ordinary prosecutorial discretion and traditional notions of justice; and
- The threat to liberty, the rule of law, and our civil society.

England *et al.*, *supra*, at 79–80. And taken to its logical conclusion, if the Government's liability theory had been upheld as a matter of law in *United States v. Drew*, it would be yet another example of bad facts making bad law—with far reaching consequences.

"The amount of conduct that would have been criminalized if Lori Drew had been convicted on the prosecution's theory of the law is enormous, as is the number of Americans who would be in violation of the law." England *et al.*, *supra*, at 91. While far from laudable, "[l]ying on social media websites is common: People shave years off their age, add inches to their height and drop pounds from their weight. The difference between puffery and prosecution may depend on whether you happen to be someone an AUSA has reason to go after." *Nosal*, 676 F.3d at 862.

D. "Exceeding Authorized Access" Should Not Be Construed to Criminalize the Innocuous Everyday Actions of Millions of Unsuspecting Americans.

This Court has consistently rejected statutory interpretations that "would appear to criminalize a broad range of day-to-day activity[.]"[12] *United States v. Kozminski*, 487 U.S. 931, 932 (1988). For example, this Court recently—and unanimously—rejected the Government's efforts to bulldoze statutory guardrails constraining federal prosecutors' use of property fraud statutes, as it has done before. *See Kelly*, 140 S. Ct. 1565. If it were otherwise, "even a practical joke could be a federal felony." *Id.* at 1573 n.2.

---

[12] In other contexts involving *malum prohibitum* offenses, this Court has found heightened *mens rea* requirements must apply. *See, e.g.*, *Ratzlaff v. United States*, 510 U.S. 135, 136–37 (1994) (holding money-laundering statute requires proof defendant acted with knowledge the conduct was unlawful), *superseded by statute* (codified as amended at 31 U.S.C. §§ 5322, 5324).

This Court should follow the same approach here and reject the Government's proposal to broadly construe the vaguely worded CFAA to criminalize (and federalize) a vast array of conduct, including everyday innocent conduct by ordinary people. *See also Yates,* 574 U.S. at 536 ("reject[ing] the Government's unrestrained reading" of 18 U.S.C. § 1519—a felony offense with a statutory maximum of 20 years imprisonment—to criminalize throwing a few fish overboard); *Bond v. United States*, 572 U.S. 844, 862 (2014) ("We are reluctant to ignore the ordinary meaning of 'chemical weapon' when doing so would transform a statute passed to implement the international Convention on Chemical Weapons into one that also makes it a federal offense to poison goldfish."). "Whatever the apparent merits of imposing criminal liability may seem to be in this case," this Court should "construe the statute knowing that . . . [its] interpretation of 'exceeds authorized access' will govern many other situations." *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015).

Section 1030(a)(2)'s reach should be narrowly cabined to intentional, culpable hacking-related computer crimes, as Congress intended. Specifically, as Professor Kerr has explained: "The CFAA should only apply to those who circumvent technological access barriers. The law should apply only to those who break in to computers—to use the common term, it should apply only to 'hackers.'"[13] At the least, Section 1030(a)(2) should be construed so as "to separate wrongful conduct from otherwise innocent

---

[13] Statement of Orin S. Kerr at 9.

conduct."[14] *Elonis v. United States*, 135 S. Ct. 2001, 2010 (2015). To be sure, under our system of government, Congress may pass stupid laws that are nonetheless constitutional. "Justice Scalia once said that he wished all federal judges were given a stamp that read 'stupid but constitutional.'" *Brown v. Chi. Bd. of Educ.*, 824 F.3d 713, 714 (7th Cir. 2016). But if Congress wants to criminalize innocent conduct like sharing a Netflix password or using a work computer to check personal email, at the very least it should be required to speak clearly by statute. *See United States v. Gradwell*, 243 U.S. 476, 485 (1917). It did not do so here.

II. BROADLY CONSTRUING SECTION 1030(A)(2) OF CFAA TO CRIMINALIZE BREACHES OF PRIVATE CONTRACTS VIOLATES DUE PROCESS.

A. Extending "Exceeding Authorized Access" Liability to Breaches of Contracts Violates Due Process for Failure to Give Fair Notice.

The scope of exceeds-authorized-access liability under the CFAA must be narrowly cabined for

---

[14] As Professor Kerr has explained:

> [T]he CFAA should not be a catch-all statute that always gives the federal government another ground on which to charge a wrongdoer who violated some other crime that happened to involve a computer. The problem with a broader approach is that it inevitably ends up covering a great deal of innocent activity.

Statement of Orin S. Kerr at 9.

another reason: extending the statute to criminalize violations of private computer-related contractual agreements fails the Fifth Amendment's test for constitutionally adequate notice.

To be sure, the Eleventh Circuit panel below believed itself bound by *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010).[15] *See* Pet. App. 26a–28a. And as applied in *Rodriguez*, construing the CFAA to criminalize accessing information for nonbusiness reasons from a government work computer did not create any fair notice problems under the bizarre facts of that case. 628 F.3d at 1260. There, the defendant worked for the Social Security Administration and was told literally every day for years that it was a federal crime for him to access others' personal information for nonbusiness reasons; he did it anyway, even after he knew he was under criminal investigation for doing that. *Id.* But *Rodriguez* is a perfect example of the old cliché that bad facts make bad laws.

---

[15] Elsewhere, the Eleventh Circuit itself has questioned the validity of *Rodriguez*, explaining:

> We decided Rodriguez in 2010 without the benefit of a national discourse on the CFAA. Since then, several of our sister circuits have roundly criticized decisions like *Rodriguez* because, in their view, simply defining "authorized access" according to the terms of use of a software or program risks criminalizing everyday behavior. . . . We are, of course, bound by *Rodriguez*, but note its lack of acceptance.

EarthCam, Inc. v. OxBlue Corp., 703 F. App'x 803, 808 n.2 (11th Cir. 2017) (citations omitted).

And if the CFAA is construed to criminalize innocuous conduct technically violating the fine print in website terms of service and company policies, it would violate due process for failure to give fair notice.

"In our constitutional order, a vague law is no law at all. Only the people's elected representatives in Congress have the power to write new federal criminal laws. And when Congress exercises that power, it has to write statutes that give ordinary people fair warning about what the law demands of them." *United States v. Davis*, 139 S. Ct. 2319, 2323 (2019). As Justice Holmes has explained:

> Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable 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. To make the warning fair, so far as possible the line should be clear.

McBoyle v. United States, 283 U.S. 25, 27 (1931). "[A] statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application, violates the first essential of due process of law." *Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926).

These basic propositions hold true *a fortiori* here if the Government's proposed construction is accepted, thereby allowing private parties to surreptitiously

create crimes through dense, confusingly worded fine print legalese contained in documents people—including those trained in the law—will not think to consult, let alone carefully read and understand.[16] "[W]ebsites' terms of service provide inadequate notice for purposes of criminal liability." *Sandvig v. Barr*, No. 16-1368, 2020 U.S. Dist. LEXIS 53631, *31 (D.D.C. Mar. 27, 2020). "Not only are the terms of service vague and generally unknown—unless you look real hard at the small print at the bottom of a webpage—but website owners retain the right to change the terms at any time and without notice. Accordingly, behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever." *Nosal*, 676 F.3d at 862; *see also Sandvig*, 2020 U.S. Dist. LEXIS 53631, at *31 ("These protean contractual agreements are often long, dense, and subject to change."). Reading Section 1030(a)(2) to authorize federal criminal prosecutions for breaches of private contracts, website terms of service, and company policies would plainly contravene bedrock fair-notice due-process

---

[16] As one court put it:

> It's a dangerous business, reading the fine print. Nearly every website we visit features Terms of Service ("ToS"), those endless lists of dos and don'ts conjured up by lawyers to govern our conduct in cyberspace. They normally remain a perpetual click away at the bottom of every web page, or quickly scrolled past as we check the box stating that we agree to them. But to knowingly violate some of those terms, the Department of Justice tells us, could get one thrown in jail.

Sandvig v. Sessions, 315 F. Supp. 3d 1, 7–8 (D.D.C. 2018).

principles.[17] It blinks reality that the fine print in these rarely read, dense, and frequently vague materials provides notice of anything at all, let alone constitutionally adequate notice of potential criminal liability.

B. Danger of Arbitrary and Discriminatory Enforcement

There is another serious constitutional problem with expanding criminal liability under the CFAA to garden-variety breach of contract. If Section 1030(a)(2) is construed to extend beyond hacking-type offenses to criminalize everyday conduct, it would also violate due process by creating fertile grounds for seriously discriminatory enforcement.

Criminal laws that "authorize and even encourage arbitrary and discriminatory enforcement" may be invalidated for vagueness. *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999). Indeed, "[v]ague statutes threaten to hand responsibility for defining crimes to relatively unaccountable police, prosecutors, and judges, eroding the people's ability to oversee the creation of the laws they are expected to abide." *Davis*, 139 S. Ct. at 2325. Thus, "[a] conviction or punishment fails to comply with due process if the statute or regulation under which it is obtained . . . is so standardless that it authorizes or encourages seriously discriminatory enforcement." *FCC v. Fox TV*

---

[17] It would also be difficult to square with the "general maxim that a contract should be construed most strongly against the drafter" in a contract dispute. *United States v. Seckinger*, 397 U.S. 203, 210 (1970).

Stations, Inc., 567 U.S. 239, 253 (2012); *see also Giaccio v. Pennsylvania*, 382 U.S. 399, 402–03 (1966) (finding due process violated if "judges and jurors [are] free to decide, without any legally fixed standards, what is prohibited and what is not in each particular case"). That proposition holds true if unaccountable *private* companies are tasked with responsibility for defining the scope, terms, and conditions under which criminal liability under the CFAA may be imposed—without notice or any, let alone meaningful, public participation.

If the CFAA's proscription against "intentionally . . . exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer," 18 U.S.C. § 1030(a)(2)(C), is construed to criminalize website terms-of-service violations and the like, there is a serious danger of arbitrary and discriminatory enforcement. *But see* Kerr, 94 Minn. L. Rev. at 1562 ("The void-for-vagueness doctrine requires courts to adopt narrow and clear interpretations of unauthorized access to save the constitutionality of the [CFAA] statute."). "[I]f every such breach does qualify [as a CFAA violation], then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution." *Drew*, 259 F.R.D. at 467. "Given the standardless sweep that results, federal law enforcement entities would be improperly free to pursue their personal predilections." *Id.* (cleaned up).

It should go without saying that "we shouldn't have to live at the mercy of our local prosecutor." *Nosal*, 676 F.3d at 862. But that is the practical effect of the Government's proposed construction of Section 1030(a)(2), which would, quite

literally, make tens of millions of unsuspecting Americans federal criminals. In so doing, it would allow federal prosecutors to bring charges—or use the threat of criminal liability as leverage—for arbitrary and seriously discriminatory reasons in circumstances where, for example, an individual expresses unpopular political views or engages in conduct the prosecutor feels *should* be a crime deserving of punishment, but which isn't. *See, e.g.*, *Drew*, 259 F.R.D. 449.

To be sure, the Government has said that ""if the Defendant exceeded authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website, federal prosecution *may not* be warranted."[18] But "[w]hile the Government might promise that it would not prosecute an individual for checking Facebook at work, . . . [courts] are not at liberty to take prosecutors at their word in such matters. A court should not uphold a highly problematic interpretation of a statute merely because the Government promises to use it responsibly."[19] *Valle*, 807 F.3d at 528; *see also Nosal,* 676 F.3d at 862 ("The government assures us that . . . it won't prosecute minor [CFAA] violations. But . . . it's not clear we can trust the government when a tempting target comes along.").

---

[18] Charging Policy at 5 (emphasis added).

[19] The Government appears to have deployed this "trust us, we're the government" line of argument here. *See* Pet. Br. 32–34.

The broad interpretation of Section 1030(a)(2) urged by the Government "would delegate to prosecutors and juries [or, in this case, even private individuals and companies] the inherently legislative task of determining what type of coercive activities are so morally reprehensible that they should be punished as crimes" and "subject individuals to the risk of arbitrary or discriminatory prosecution and conviction." *Kozminski*, 487 U.S. at 949. That is patently unconstitutional.

This Court should therefore reject any invitation to broadly construe Section 1030(a)(2) based on putative assurances of the exercise of prosecutorial restraint, as it has done before. *See, e.g.*, *United States v. Stevens*, 559 U.S. 460, 480 (2010). Section 1030(a)(2), broadly construed, would "leave us at the mercy of noblesse oblige." *Id.*

III. ALLOWING PRIVATE PARTIES TO CREATE FEDERAL CRIMES BY CONTRACT VIOLATES THE PRIVATE NONDELEGATION DOCTRINE.

The Government's expansive view of liability under the CFAA not only violates principles of due process protected by the Fifth Amendment but also runs afoul of separation-of-powers principles. In our system of checks and balances, only the legislature may create federal crimes through duly enacted legislation. *See Gradwell,* 243 U.S. at 485 ("[B]efore a man can be punished as a criminal under the federal law his case must be plainly and unmistakably within the provisions of some statute[.]") (cleaned up). Thus, Article III Courts may not create federal crimes; "[i]t is well settled that there are no common law offences against the United States." *United States v. Eaton*,

144 U.S. 677, 687 (1892). Nor may the Executive branch unilaterally promulgate new federal law restricting liberty on pains of criminal punishment—at least in theory. *But see Gundy v. United States*, 139 S. Ct. 2116, 2131 (2019) (Gorsuch, J., dissenting) (describing statute that "purports to endow the nation's chief prosecutor with the power to write his own criminal code governing the lives of a half-million citizens" as an "extraconstitutional arrangement" and suggesting the state of affairs should be revisited).

It would seem to necessarily follow—as a matter of logic and common sense—that surely private parties cannot create new federal crimes. Not so, under the Government's reading of the CFAA. If this Court accepts the Government's invitation to obliterate all meaningful textual and constitutional barriers to prosecution under the CFAA, once Pandora's box is open there would be no limiting principle. Overzealous prosecutors could bring charges against innocent actors for a "crime" created by a private party whose lawyers created the elements of the offense in the fine print of some purported contract. This Court should not allow this to happen.

To be sure, liberty of contract is a cornerstone of free and prosperous societies. Indeed, the Contract Clause of the U.S. Constitution specifically prohibits the government from interfering with these voluntary private agreements: "No State shall . . . pass any . . . Law impairing the Obligation of Contracts[.]" U.S. Const. Art. I, § 10, Cl. 1. Accordingly, subject to principles of contract law, private companies have wide latitude to determine the terms and conditions on which they choose to offer their services, do business, offer employment, and to decide who they

will employ and do business with. Of course, private parties should have these economic freedoms.

But that is not what is at issue here if the rationale undergirding the decision below is allowed to stand. Instead, the question is whether the CFAA somehow empowers private parties to unilaterally adjust the ambit of the federal criminal law, with or without procedural niceties like providing the public advance notice of what is forbidden or required, through dense legalese in the fine print of their contracts, policies, and terms of service. Our Constitution directs the answer is no. "Criminalizing terms-of-service violations risks turning each website into its own criminal jurisdiction and each webmaster into his own legislature." *Sandvig*, 2020 U.S. Dist. LEXIS 53631, at *33. Under "[s]uch an arrangement . . . each website's terms of service 'is a law unto itself[.]'" *Id.* (quoting *Emp't Div., Dep't of Human Res. of Or. v. Smith*, 494 U.S. 872, 890 (1990)). That is unconstitutional.[20] *See The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 Harv. L. Rev. 751, 768–71 (2013).

That cannot be right. "The Constitution promises that only the people's elected representatives may adopt new federal laws restricting liberty." *Gundy*, 139 S. Ct. at 2131 (Gorsuch, J., dissenting). Not private companies. This is because "Article I, § 1, of the Constitution vests 'all legislative Powers herein

---

[20] "[A]lthough not a paradigmatic example of a 'nondelegation' problem, enabling private website owners to define the scope of criminal liability does raise concerns[.]" *Sandvig*, 2020 U.S. Dist. LEXIS 53631, at *31.

granted . . . in a Congress of the United States.' This text permits no delegation of those powers[.]" *Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 472 (2001). "Not content to rely merely on the implication from the principle of delegation, the Constitution emphasizes that *all* legislative powers granted to the United States shall be in Congress. It thereby expressly bars the subdelegation of such powers." Philip Hamburger, *Is Administrative Law Unlawful?*, 386 (2014).[21]

As Professor Philip Hamburger has suggested, this basic principle is deeply rooted in the structure of our system of government, which has only those powers that We the People have granted to it: "As [John] Locke explained, 'The legislature cannot transfer the power of making laws to any other hands. For it being but a delegated power from the people, they, who have it, cannot pass it over to others.' This followed not simply from their constitution, but from the nature of constitutions[.]" *Id.* at 382 (quoting John Locke, *Two Treatises of Government*, 362–63 (II.xi.141–42), ed. Peter Laslett (1988)); *see also Gutierrez-Brizuela v. Lynch*, 834 F.3d 1142, 1149 (10th Cir. 2016) (Gorsuch, J., concurring) ("[T]he founders considered the

---

[21] As Professor Hamburger has explained, at the time of the Founding, "Americans clearly understood how to write constitutions that expressly permitted the subdelegation of legislative power to the executive, and they did not do this in the federal constitution. On the contrary, as apparent from the word *all* [in Article I, § 1], they expressly barred any such subdelegation." *Id.* at 388. This proposition holds true with respect to subdelegation of legislative powers (particularly criminal lawmaking powers) to private parties.

separation of powers a vital guard against governmental encroachment on the people's liberties, including all those later enumerated in the Bill of Rights.").

"The principle that Congress cannot delegate away its vested powers exists to protect liberty. Our Constitution, by careful design, prescribes a process for making law, and within that process there are many accountability checkpoints. It would dash the whole scheme if Congress could give its power away to an entity that is not constrained by those checkpoints." *DOT v. Ass'n of Am. R.R.*, 575 U.S. 43, 61 (2015) (Alito, J., concurring); *see also Perez v. Mortg. Bankers Ass'n*, 575 U.S. 92, 118 (2015) (Thomas, J., concurring in the judgment) ("To the Framers, the separation of powers and checks and balances were more than just theories. They were practical and real protections for individual liberty in the new Constitution.") (cleaned up).

Accordingly, Congress may not delegate lawmaking powers to private entities.[22] Period. "This is legislative delegation in its most obnoxious form; for it is not even delegation to an official or an official body, presumptively disinterested, but to private

---

[22] *See also A.L.A. Schechter Poultry Corp. v. United States*, 295 U.S. 495, 537 (1935) (Is it "seriously contended that Congress could delegate its legislative authority to [private] groups so as to empower them to enact the laws they deem to be wise and beneficent for the rehabilitation and expansion of their trade or industries? . . . The answer is obvious. Such a delegation of legislative power is unknown to our law and is utterly inconsistent with the constitutional . . . duties of Congress.").

persons whose interests may be and often are adverse to the interests of others in the same business." *Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936); *see also* Hamburger, *supra*, at 398 ("Perhaps the most extraordinary sort of subdelegation is the transfer of legislative and judicial powers . . . to private bodies."). And private entities certainly cannot create new criminal law through the fine print in their contracts. *Cf. Ass'n of Am. R.R.*, 575 U.S. at 61 (Alito, J., concurring) ("Even the United States accepts that Congress cannot delegate regulatory authority to a private entity.") (cleaned up).

But that unconstitutional result is a necessary consequence of construing the CFAA broadly to criminalize violations of private contractual agreements—particularly with respect to the fine print in form contracts, website terms of service, and company policies that the vast majority of people do not actually read. For instance, "by utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime, that approach makes the website owner—in essence—the party who ultimately defines the criminal conduct." *Drew*, 259 F.R.D. at 465.

This is yet another reason why Section 1030(a)(2)'s proscription against "exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer," 18 U.S.C. § 1030(a)(2), must be construed to exclude violations of private contracts, as well as accessing information for an allegedly improper purpose.

IV. THE RULE OF LENITY AND THE CONSTITUTIONAL AVOIDANCE CANON COUNSEL IN FAVOR OF A LIMITING CONSTRUCTION.

To the extent there are any lingering doubts as to why the Government's interpretation of the CFAA should be rejected, and the decision below reversed, "both the rule of lenity and the [constitutional] avoidance canon weigh in favor of . . . narrow[ly] interpreti[ng]" the CFAA to exclude terms-of-service and other contractual violations. *Sandvig*, 2020 U.S. Dist. LEXIS 53631, at *33.

To begin with, to the extent Section 1030(a)(2) is sufficiently ambiguous to be plausibly interpreted to criminalize breach of private contracts and terms of service, that reading must be rejected under the rule of lenity. "[A]mbiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *Yates*, 574 U.S. at 547–48 (cleaned up). Under that rule, "ambiguities about the breadth of a criminal statute should be resolved in the defendant's favor. That rule is 'perhaps not much less old than' the task of statutory 'construction itself.'" *Davis*, 139 S. Ct. at 2333 (quoting *United States v. Wiltberger*, 18 U.S. 76, 5 Wheat. 76, 95 (1820) (Marshall, C. J.)). "The rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them." *United States v. Santos*, 553 U.S. 507, 514 (2008).

Thus, "when there are two rational readings of a criminal statute, one harsher than the other, [courts] are to choose the harsher only when Congress has spoken in clear and definite language." *McNally v.*

United States, 483 U.S. 350, 359–60 (1987). As Justice Scalia explained: "This venerable rule not only vindicates the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain or subjected to punishment that is not clearly prescribed. It also 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.

It is simply wrong for Mr. Van Buren to "languish[] in prison" without "the lawmaker ha[ving] clearly said [that he] should."[23] *United States v. Bass*, 404 U.S. 336, 348 (1971). "Congress has not [in the CFAA] clearly criminalized obtaining or altering information 'in a manner' that is not authorized. Rather, it has simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter." *Miller,* 687 F.3d at 206. "[T]he rule of lenity requires that Congress, not the courts or the prosecutors, must decide whether conduct is criminal. [Courts], on the other hand, are obligated to 'construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals.'" *Valle,* 807 F.3d at 528 (quoting *Nosal,* 676 F.3d at 863). "[I]t is appropriate, before . . . [the Court] choose[s] the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *Yates*, 574 U.S. at 548 (cleaned up). Congress did not do so here.

---

[23] This is particularly true because Mr. Van Buren's prosecution is a result of a government sting operation. *See* Pet. Br. 10–12.

Buttressing this conclusion is the doctrine of constitutional avoidance, which often works in a synergistic tandem with the rule of lenity to counsel a *narrow* (but constitutionally permissible) reading of a criminal statute. Under the avoidance canon, "when presented with two fair alternatives, this Court has sometimes adopted the *narrower* construction of a criminal statute to avoid having to hold it unconstitutional if it were construed more broadly." *Davis*, 139 S. Ct. at 2332 (cleaned up). "[W]hat Congress has written . . . must be construed with an eye to possible constitutional limitations so as to avoid doubts as to its validity." *United States v. Rumely*, 345 U.S. 41, 45 (1953) (cleaned up); *see, e.g., McDonnell v. United States,* 136 S. Ct. 2355, 2372–73 (2016) (rejecting expansive reading of criminal statute that "would raise significant constitutional concerns"); *Skilling v. United States*, 561 U.S. 358, 405 (2010) ("It has long been our practice . . . before striking a federal statute as impermissibly vague, to consider whether the prescription is amenable to a limiting construction."). "Applying constitutional avoidance to narrow a criminal statute . . . accords with the rule of lenity." *Davis*, 139 S. Ct. at 2333. So too here.

As Petitioner ably explains, *see* Pet. Br. 17–35, the plain language, context, structure, purpose, and history of Section 1030(a)(2) unambiguously bar prosecutions of individuals who are authorized to access information on a computer for certain purposes but who access the same information for improper purposes, as Petitioner is alleged to have done here. For those reasons, as a matter of statutory interpretation, CFAA liability may not be imposed

based on breach of contract, violations of website terms of service, or violations of company policies.

But even if it were otherwise, and Section 1030(a)(2) could plausibly be read to criminalize such conduct, this Court should nonetheless adopt an equally textually permissible narrowing construction, in line with the Constitution. Because if the CFAA applies as broadly as the Government seems to think, it would be unconstitutional under the Due Process Clause of the Fifth Amendment, violate Article I's Vesting Clause, and offend the separation of powers by delegating criminal lawmaking powers to private entities.

CONCLUSION

The judgment of the court of appeals should be reversed.

Respectfully submitted,

R. James Valvo, III
Counsel of Record
Michael Pepson
AMERICANS FOR PROSPERITY FOUNDATION
1310 N. Courthouse Road, Ste. 700
Arlington, VA 22201
(571) 329-4420
jvalvo@afphq.org

Counsel for Amicus Curiae July 8, 2020