No. 10-10038

# In the Supreme Court of the United States

UNITED STATES OF AMERICA,
PETITIONER

*v.*

DAVID NOSAL,
RESPONDENT

*ON WRIT OF CERTIORARI*
*TO THE UNITED STATES COURT OF APPEALS*
*FOR THE NINTH CIRCUIT*

## BRIEF FOR RESPONDENT

ANURADHA SIVARAM
*Attorney*
*Counsel of Record for Respondent*

University of California, Berkeley
School of Law
Berkeley, CA 94720
asivaram@berkeley.edu
(408) 921-4836

## QUESTION PRESENTED

Does the term "exceeds authorized access" as used in 18 U.S.C. § 1030(a)(4) and as defined in 18 U.S.C. § 1030(e)(6) extend to computer use restrictions, or is it limited to computer access restrictions?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND REGULATIONS



OTHER AUTHORITIES

## STATEMENT OF THE CASE

For the past thirty years, the federal government has continuously expanded the reach of the Computer Fraud and Abuse Act. Prosecutors now exploit its provisions to punish innocuous activities like downloading academic articles, creating profiles through social media, and disseminating publicly available user information to journalists reporting about website security. This case finally presents the Court with an opportunity to clarify the limits of this statute.

### I. Legislative Context and Factual Background

The Computer Fraud and Abuse Act ("CFAA") originally aimed to punish "hackers" who trespassed into computers owned by the federal government or large financial institutions. See H.R. Rep. No. 98-894, at 10-11, 20 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3695-97, 3706. Congress, however, dramatically expanded its scope through subsequent enactments.

Two years after enacting the CFAA, Congress extended its terms to cover those who, "with intent to defraud," access computers "without authorization," who "exceed authorized access" to computers, and who traffic in computer passwords. See Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified at 18 U.S.C. § 1030). Congress again broadened the law to create a private civil cause of action under the CFAA. See 18 U.S.C. § 1030(g) (1994).

The next set of amendments transformed the statute by extending its reach to criminalize improper access of any "protected computer" that is "used in

interstate or foreign commerce or communications." See Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (1996) (codified in scattered sections of 18 U.S.C.). Most recently, Congress provided for the CFAA to apply extraterritorially to unauthorized computer access that affects the interstate or foreign commerce of the United States. See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56 § 814, 115 Stat. 272, 382 (2001) (codified as amended at 18 U.S.C. § 1030).

Despite passing multiple sweeping expansions of the CFAA, Congress failed to address fundamental questions about exactly what actions fall under its terms. Crucially, the CFAA does not define what constitutes "authorized" or "unauthorized" access to a computer.

CFAA § 1030(e)(6) defines the phrase "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." See Record ("R") at 10. However, this circular definition does not explain how to establish authorization in the first instance, or how the phrase "exceeds authorized access" differs from "without authorization." This omission is particularly troubling because both criminal liability under § 1030(a)(2) and § 1030(a)(4) and civil liability under § 1030(g) turn on the same definition of "authorized access." See R. at 4.

Due to this vacuum in the statutory language, it is unclear whether respondent David Nosal "exceeded authorized access" under CFAA § 1030(a)(4) as the Government alleges. Nosal convinced several ex-colleagues to obtain client contact information from a database operated by Korn/Ferry, his former employer, in order to start a competing business. See R. at 13. Although Nosal's former coworkers could ordinarily log in to the database, Korn/Ferry company policy forbade disclosing confidential information. Id. The policy appeared on the opening screen of the database and warned users that the database contents were "intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." Id. There is no evidence in the record to indicate that Nosal and his co-workers "hacked" into the company database or stole login credentials.

## II. Legal Background

The Government indicted Nosal for trade secret theft, mail fraud, conspiracy, and violating the CFAA. Id. The district court initially adopted the Government's broad reading of CFAA § 1030(a)(4). R. at 14. It concluded that an individual "exceeds authorized access" by simply disregarding conditions attached to computer use established by a private policy or contract. Id. The court therefore found that the CFAA does not merely punish entrance into a portion of a computer to which one does not have electronic permission to access. Id.

After the district court issued its opinion, the Ninth Circuit decided that an employee using a computer in a manner contrary to his employer's interest does not "exceed" authorized access. LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir.

2009). The district court subsequently reconsidered its decision and adopted the Ninth Circuit's narrow construction of the CFAA. Id. The court found that any other interpretation necessarily treats the word "alter" in § 1030(e)(6) to mean "misappropriate," contrary to its plain meaning. Id. In its new opinion, the district court concluded that Nosal did not "exceed authorized access" by breaching conditions governing the use of information obtained from the Korn/Ferry computer. Id. The court then dismissed the CFAA counts from the case. Id.

The Government appealed this ruling to the Ninth Circuit. The court determined that it could interpret the term "exceeds authorized access" in two ways—either to describe the transgression of an electronic barrier shielding portions of a computer or to describe the misuse of information to which one has unrestricted access. R. at 15. However, the court held that punishing users for disobeying contractual limits on computer use will improperly "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." R. at 16.

In formulating its opinion, the Ninth Circuit relied on established textual canons of statutory construction. R. at 20. The Ninth Circuit also reasoned that Congress would have used clearer language if it truly meant to expand criminal liability under the CFAA to reach everyone who disregards a computer use restriction. R. at 16. Additionally, the majority rejected the Government's argument that the phrase "exceeds authorized access" could be read broadly in § 1030(a)(4) but could be construed narrowly for the purposes of prosecuting misdemeanor

violations under § 1030(a)(2), insisting, "[i]dentical words and phrases within the same statute should normally be given the same meaning." R. at 20.

The Ninth Circuit also employed the rule of lenity to construe what it found to be an ambiguous criminal statue narrowly, to "avoid making criminal law in Congress's stead." Id. Finally, the court expressed unease at the prospect of unbridled prosecution for a host of minor violations of computer use policies and accordingly justified its break with its sister circuits in interpreting the CFAA. R. at 27, 29.

The dissenting judges found the CFAA to be "plainly written." R. at 31. They concluded that one can "exceed authorized access" by ignoring "employer-placed limits on accessing information stored on the computer." R. at 32. The dissent distinguished Brekka as governing cases where employees only breach duties of loyalty and found that an employee "exceeds authorized access" by violating a specific agreement prohibiting misuse of computer data. R. at 32-33.

Upon exhausting all avenues of appeal, the Government sought a writ of certiorari. This Court granted the writ to decide whether the phrase "exceeds authorized access" as used in the CFAA extends to violations of express or implied contractual computer use restrictions, or whether it is limited to violations of code-based access restrictions. This Court does not defer to any entity's interpretation of criminal laws. Crandon v. United States, 494 U.S. 152, 177 (1990). Accordingly, it must decide these questions under a de novo standard.

## SUMMARY OF ARGUMENTS

No matter which statutory interpretation technique this Court utilizes, the result will be the same: the term "exceeds authorized access" does not include breaches of private contracts or duties that restrict the use of data obtained from a computer.

The CFAA's terms must be interpreted narrowly to conform to elementary textual and substantive canons of statutory construction. The technical meaning of "authorization" indicates that Congress intended to punish hackers who circumvent electronic barriers to computer access. The ordinary meanings of other words in the statute, read together, show that the drafters also wanted to punish password theft.

Any alternate interpretation of "exceeds authorized access" improperly punishes more than computer trespass and password theft. Indeed, the Government's stance pinning liability to violations of private contracts widens the reach of the CFAA, as does an "agency" paradigm that pegs CFAA liability to breaches of common-law fiduciary duties.

Interpreting the CFAA broadly to cover such use restrictions, however, flouts multiple textual canons of construction and is thus improper. First, a broad interpretation eliminates the distinction between "unauthorized access" and action

that "exceeds authorized access," contravening the rule that this Court must give effect "to every word of a statute wherever possible." Leocal v. Ashcroft, 543 U.S. 1 (2004). Secondly, it reads the word "so" entirely out of CFAA § 1030(e)(6), defying the canon that courts must give meaning to each word in a statute. Duncan v. Walker, 533 U.S. 167, 174 (2001). Additionally, such an interpretation finds scant support in the CFAA's legislative history. Finally, an expansive interpretation of "exceeds authorized access" creates discord with a cognate statute and thereby disregards the in pari materia canon advising courts to construe terms in similar statutes in a parallel fashion.

Even if this Court finds the phrase "exceeds authorized access" ambiguous, it must interpret § 1030(a)(4) narrowly to exclude breaches of contract from its scope, pursuant to established substantive canons of statutory construction.

First, the canon of lenity cautions against punishing crimes not enumerated in a statute simply because they seem to be "of a kindred character" with those crimes that are so enumerated. United States v. Wiltberger, 5 Wheat. 76, 96, 18 U.S. 76, 96 (1820). Per this principle, terms of use violations may not fall into the sweeping reach of the CFAA. Doing so unfairly criminalizes an entirely new category of sundry activities without express legislative authorization.

This Court must also construe the words of an ambiguous statute in a manner that avoids "serious constitutional doubts." FCC v. Fox Television Stations, 566 U.S. 502, 516 (2009). Accordingly, it should restrict the scope of activities that "exceed authorized access" to hacking and password theft in order to avoid two

weighty constitutional questions. The first is whether a statute that incorporates dense, potentially ill-defined terms from a boilerplate agreement is "void for vagueness" under the Due Process Clause. Bouie v. City of Columbia, 378 U.S. 347, 351 (1964). The second is whether Congress may, under the CFAA delegate the power to define criminal acts to private parties who draft the terms and conditions of computer use. A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935).

Finally, federalism canons also favor a narrow reading of the CFAA. The Court should respect the rights of state governments by preventing the CFAA from creeping into a field traditionally left to state governance. Rice v. Santa Fe Elevator Corp., 331 U.S. 218 (1947). It should also preserve common-law rules prohibiting punitive remedies for breaches of contract.

## ARGUMENT

### I. THE TEXT OF THE CFAA PRECLUDES PUNISHING THOSE WHO FLOUT CONTRACT-BASED COMPUTER USE RESTRICTIONS

The interpretation of § 1030(a)(4) must commence "where all such inquiries must begin: with the language of the statute itself." United States v. Ron Pair Enters., Inc., 489 U.S. 235, 241 (1989). However, CFAA § 1030(a)(4) and related provisions do not actually specify which computer interactions fall under the terms "without authorization" or "exceeds authorized access." R. at 4, 10 (displaying the text of CFAA § 1030(a)(4) and CFAA § 1030(e)(6)). Nevertheless, the meanings of technical and ordinary words used in the CFAA, taken together, indicate that Congress intended to punish only two types of criminals. The first is the computer hacker, and the second steals others' credentials to interface with a computer.

The Government's alternative reading allows the CFAA to expand to punish individuals who simply operate a computer after breaching an express or implied contract or condition of agreement restricting use of computer data. This not only battles with the intended meanings of words and phrases used in the CFAA but also violates multiple longstanding textual canons of construction. Regardless of whether the Court finds the CFAA ambiguous, it cannot accept any broader interpretation that the Government proposes.

### A. The Term "Exceeds Authorized Access" Does Not Extend So Broadly as to Punish Those Who Misuse Computer Data

The most flexible words in the § 1030(e)(6) definition of "exceeds authorized access" are "authorization" and "entitled." The Court should adopt the narrowest interpretations of these terms premised on the idea that "unauthorized" access requires transgressing code-based computer access barriers—colloquially, hacking. See Orin Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1599-1600 (2003) (distinguishing the "code-based" paradigm of unauthorized computer access from the "contract-based" paradigm restricting authorization based on contract terms).

Under a code-based paradigm, anybody who interfaces with a computer after submitting proper passwords to surmount electronic barriers—that is, anybody who successfully logs in—is an "authorized" user. This is because "authorization," as used in the CFAA, is a technical term related to the internal electronic barriers in a computer. As a corollary, no contract-based use restriction can make computer access "unauthorized." However, other words in the statute show that not all authorized access is permissible. Those who interface with computers after stealing login information "exceed authorized access" and are liable under the CFAA.

#### 1. The Court Must Read the Word "Authorized" in the CFAA as a Technical Term of Art

In order to determine which actions "exceed authorized access" under the definition in § 1030(e)(6), the Court should first determine what that provision means when it refers to accessing computers "with authorization." R. at 10.

This Court customarily endows words in a statute with their ordinary meanings. Moskal v. United States, 498 U.S. 103, 108 (1990). However, it also gives "technical words in . . . statutes their usual technical meaning." Barber v. Gonzales, 347 U.S. 637, 643 (1954). Whether a statute adopts a word's technical or ordinary meaning depends on evidence of how it is used by "[professionals], regulators, courts, and commentators." Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 371-72 (1986). Where Congress has used "technical words or terms of art" in a statute, it is proper to interpret them "by reference to the art or science to which they [are] appropriate." Corning Glass Works v. Brennan, 417 U.S. 188, 201 (1974).

"Authorization" is a classic example of a technical term of art. Computer experts, lawmakers, and academics regularly use the term to describe code-based electronic access permission. This Court consulted these same types of sources to hold that certain words in the Communications Act of 1934 were, in fact, technical accounting terms. Louisiana Pub. Serv. Comm'n, 476 U.S. at 355. Accordingly, it should find that "authorization" carries a specialized meaning in the CFAA.

The Oxford Dictionary of Computing defines "authorization" as a "process by which users, having completed an authentication stage, gain or are denied access to particular resources." Oxford Dictionary of Computing 30 (6th Ed. 2008). The dictionary defines "authentication" as a "process by which subjects . . . establish their identity to a system. This may be effected by the use of a password or . . . a physical device, e.g. a coded token." Id. at 29. Furthermore, experts generally only consider "hackers" to access computers without "authorization." See Dictionary of

Computer and Internet Terms 211 (7th ed. 2000). These sources demonstrate how experts perceive the technical word "authorization" to represent a successful, conventional navigation of a code-based barrier to computer use.

Moreover, even before enacting the CFAA, lawmakers understood the term "authorized" to carry a specialized, code-based meaning in the context of secured electronic systems. In Sable Communications of California, Inc. v. FCC, 492 U.S. 115 (1989), this Court acknowledged that authorization for "dial-a-porn" telephone services turns on entering a proper identification code. Id. at 121 (citing to 50 Fed. Reg. 42,699, 42,705 (Oct. 22, 1985)). The regulations at issue in that case specify that authorization for the adult phone-messaging systems depended on the program providing a functioning access code. 50 Fed. Reg. 42,669, 42,704-05 (Oct. 22, 1985) (codified at 47 C.F.R. § 64.201).

Academics, too, recognize that "authorization" represents a technical process by which an individual successfully responds to computer code to initiate computer use. See Orin Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1599-1600 (2003); David J. Rosen, Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access," 27 Berkeley Tech. L.J. 737 (2012).

Based on the evidence of how "[professionals], regulators, courts, and commentators" define the term "authorization," this Court should find that it is a technical term. Louisiana Pub. Serv. Comm'n, 476 U.S. at 371-72. Allowing the meaning of "authorization" to turn on the nuances of private agreements, as the

Government suggests, conflicts with the duty to interpret "authorized" by reference "to the art or science" of computer programs in which it is situated. Corning Glass Works, 417 U.S. at 201. It is "incumbent" upon this Court to give words their technical meanings if those intimate with the subject of the legislation deem them to have a peculiar connotation. NLRB v. Coca-Cola Bottling Co., 350 U.S. 264, 269 (1956). As evidence shows that experts consider "authorized" to have a "peculiar" connotation, this Court should adopt the technical meaning of "authorization" when it interprets the CFAA. Accordingly, it should find that an authorized user interfaces with computers by supplying valid credentials, whereas an unauthorized user hacks into systems by exploiting loopholes in code.

2. CFAA § 1030(e)(6) Defines "Exceeds Authorized Access" Using Plain Terms That Indicate That the Provision Targets Password Thieves

Reading the phrase "exceeds authorized access" on its own in CFAA § 1030(a)(4) hints that the statute does not punish computer data misuse. After all, "by its plain terms, ['exceeds authorized access'] speaks to access, not use." JBC Holdings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 523 (S.D.N.Y. 2013). However, since statutes may only be given their ordinary meaning "unless otherwise defined," and because another CFAA § 1030(e)(6) defines this term, the Court must interpret "exceeds authorized access" according to that provision. Sebelius v. Cloer, 133 S. Ct. 1886, 1893 (2013).

Even analyzing the precise terms in CFAA § 1030(e)(6) that define "exceeds authorized access" yields the same result. The provision defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain

or alter information in the computer that the accesser is not entitled so to obtain or alter". R. at 10; 18 U.S.C. § 1030(e)(6).

"Obtain" generally means to "hold on to or possess." The American Heritage Dictionary 857 (4th ed. 2006). It therefore does not encompass a subsequent misuse of information once obtained. Furthermore, the term "alter" means simply "to make different"; this definition does not carry the negative connotations that the word "misuse" does. See The American Heritage Dictionary 53 (4th ed. 2006); Merriam Webster's Collegiate Dictionary 35 (11th ed. 2003). The phrase "in the computer" circumscribes both "obtain" and "alter" and limits violations to activity that occurs within the computer upon authorized access. CFAA § 1030(e)(6); R. at 10. These terms imply that one cannot "exceed authorized access" by subsequently misappropriating data.

The preposition "so" means "in the way or manner indicated." Merriam-Webster's Collegiate Dictionary 605 (11th ed. 2003). Read as part of the phrase "entitled so to obtain," this two-letter word restricts information the one may not be entitled to retrieve from a computer to data acquired upon achieving authorized access. However, this presents a paradox: how can an individual at once be authorized to use a computer, yet not entitled to obtain or alter any information therein?

The only logical solution to this puzzle is that CFAA § 1030(e)(6) punishes people who successfully log in to computers through stolen passwords that they are not "entitled" to possess. This definition incorporates the technical meaning of

"authorized" as a successful navigation of computer code and allows the word "so" to define the manner of authorized access that may itself be improper. Under this narrow definition, individuals like Nosal who interface with computers using their own passwords, no matter how deplorable the use to which they put computer data, do not "exceed authorized access."

Stretching the definition of "exceeds authorized access" to encompass subsequent misuse of information obtained from a computer is akin to fitting a square peg in a round hole. The plain meanings of terms in the phrase clearly indicate that the CFAA only punishes hacking and password theft—not the improper disclosure at issue here. Interpreting "exceeds authorized access" using contractual provisions or disregarding the definition in § 1030(e)(6) will contravene the rule that courts eschew plain meaning analyses if the statute pre-defines select terms. Cloer, 133 S. Ct. at 1893.

B. Textual Canons of Construction, Legislative History, and Similar Statutes Counsel the Court to Reject the Government's Broad Interpretation of "Exceeds Authorized Access"

The inquiry in a statutory construction case ceases "if the statutory language is unambiguous." Sebelius v. Cloer, 133 S. Ct. 1886 (2013). Accordingly, only if this Court finds the language of the CFAA unclear should it evaluate the Government's alternate interpretation using textual canons of construction, legislative history, and constructions of comparable statutes.

1. Interpreting "Exceeds Authorized Access" as Broadly as the Government Urges Violates Multiple Textual Canons of Construction

The Government argues that the phrase "exceeds authorized access" means that an individual initially interfaces with a computer with permission but then—like Nosal—obtains or alters information that they are not supposed to possess or use, pursuant to the terms of a contract restricting data use. Although this interpretation of the CFAA has the trappings of a complete definition, longstanding textual canons of construction foreclose this reading. This Court "must give effect to every word of a statute wherever possible," Leocal v. Ashcroft, 543 U.S. 1 (2004). Furthermore, "a reviewing court normally cannot add to the words of a statute." Dean v. United States, 556 U.S. 568 (2009). Additionally, this Court cannot read the same phrase in a statute two different ways. Clark v. Martinez, 543 U.S. 371, 378 (2005). Finally, an interpretation of a statute cannot yield absurd results. Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 575 (1982). Reading "exceeds authorized access" to encompass contract-based use restrictions, however, violates each of the preceding rules.

a. The Government's Interpretation Reads the Word "So" out of the Statute

The Government interprets the word "entitled" in CFAA § 1030(e)(6) as if entitlement to computer data can flow from any agreement or policy governing access to computers. In this contract-based paradigm, an individual with authorized access to a computer might disobey a use restriction provision, and consequently lose entitlement to their computer privileges. The individual will thus "exceed" authorized access by obtaining information from the computer, since they are no longer entitled to do so by the terms of the use restriction policy.

The precise text of the CFAA, however, prohibits obtaining or altering information that the accesser is not "entitled *so* to obtain or alter." R. at 10 (emphasis added). The word "so" in that phrase refers to the manner in which the accesser acquires information—that is, the authorized access by way of a computer password. Thus, reading the phrase "not entitled so to obtain or alter" to mean something like "not contractually entitled to obtain or alter" as the Government suggests eliminates the significance of the word "so" from the statute. This interpretation thereby contravenes the canon of construction that requires courts to give effect to "every word" of a statute. Duncan v. Walker, 533 U.S. 167, 174 (2001).

b. A Broad Interpretation of the CFAA Renders the Phrase "Without Authorized Access" Useless

Tethering computer authorization to the particularities of use restriction contracts blurs the distinction between "unauthorized" access and access that "exceeds authorization." Demolishing the distinction between these two phrases renders at least one of the terms meaningless. Thus, adopting the Government's broad contract-based interpretation of "exceeds authorized access" disobeys the canon of statutory construction that cautions against superfluity. Corley v. United States, 556 U.S. 303, 314 (2009).

Any interpretation of "authorization" that does not depend on computer codes risks defining the same conduct as both unauthorized and as "exceeding authorized access." For example, in Southwest Airlines Co. v. Fairchase, 318 F. Supp. 2d 435 (N.D. Tex. 2004), the court found that that after breaching a website's use agreement, the defendant engaged in "unauthorized" access of the site and its

computer servers. However, another court determined that a defendant who committed the same conduct "exceeded" authorized access. Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001).

The following hypothetical illustrates this inconsistency. A minor views a website for individuals eighteen and older. Under the plain terms of the website's use agreement, the minor is "unauthorized" because he has not reached majority. However, he also "exceeds authorized access" by disobeying a condition that technically restricts the manner in which he can use the website and its servers.

This difficulty also arises when courts define "authorization" based on violations of fiduciary duties. The Seventh Circuit held that a former employee was "unauthorized" to use information obtained from a computer after he breached a duty of loyalty to his employer. Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006). However, another circuit found the use of a former employer's information to "exceed authorized access," where the information was publicly available. EF Cultural Travel, BV v. Explorica, Inc., 274 F.3d 577, 583-84 (1st Cir. 2005). Even Judge Posner, author of the Citrin opinion, admitted that the distinction between "unauthorized" access and action that "exceeds authorized access" is "paper thin." 440 F.3d at 420.

Interpreting the term "authorized" and the phrase "exceeds authorized access" in the context of computer access codes avoids these problems. Under that paradigm, only hacking constitutes "unauthorized" access and only password theft "exceeds authorized access." The Government's broad interpretation of the statute

should not govern, as it reads key terms out of the CFAA and thus violates the canon against superfluity.

c. It is Improper to Adopt Two Interpretations of "Exceeds Authorized Access" in the Same Statute

A broad interpretation of "exceeds authorized access" technically allows the Government to prosecute violations of web site terms of use as a felony. The Government argues that the heightened state-of-mind provisions in CFAA § 1030(a)(4) requiring fraudulent intent ensure that the law only applies to serious theft and hacking incidents. This theory, however, ignores the fact that the broad interpretation will still apply to CFAA § 1030(a)(2). Accordingly, adopting the Government's loose construction of this term will criminalize actions besides hacking and password theft in another provision of the CFAA.

The Government previously suggested reading the phrase "exceeds authorized access" differently when it applies to different provisions of the CFAA. R. at 20. This "solution" disobeys an elementary precept that words in a statute should maintain consistent meanings. Clark v. Martinez, 543 U.S. 371, 378 (2005). Accordingly, the Government's position that "exceeds authorized access" be interpreted differently to cover contract-based use restrictions is untenable.

d. The Government's Interpretation Violates the Canon Against Absurdity

This Court must eschew interpretations of a statute that yield absurd results where there exist "alternative interpretations consistent with the legislative purpose." Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 575 (1982). This Court

finds interpretations to be absurd where "it is unreasonable to believe that the legislator intended to include [a] particular act" in the scope of the statute. Holy Trinity Church v. United States, 143 U.S. 457, 459 (1892).

Statutory interpretations are "absurd" when they require applying a statute to a class of persons or offenses clearly not within the contemplated scope of the law. In United States v. Jin Fuey Moy, 241 U.S. 394 (1916), this Court analyzed a statute punishing individuals who carried opium without registration. The Court concluded that the statute could only punish those required to register for opium possession and not individuals who could not participate in the registration scheme at all. Id. at 402. In United States v. Katz, 271 U.S. 354 (1926), this Court interpreted a law that required licensed liquor vendors to keep records of sales. It concluded that interpreting its terms literally to punish "all persons" would be absurd, as that would extend a statute intended to monitor licensed liquor distributors to bootleggers. Id. at 363.

The Government's contract-centric interpretation of "exceeds authorized access" is one such interpretation that yields absurd results, while Nosal's narrower approach provides the proper alternative.

Reading "exceeds authorized access" to mean "violating terms and conditions of use" transforms the CFAA—originally an anti-hacking statute—into an omnibus Internet patrol bill. See H.R. Rep. No. 98-894, at 21 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3707 (specifying that the legislation imposes criminal punishment on "hackers"). This will criminalize not only hacking, but also phishing,

email harvesting, page scraping, domain spoofing, and similar activities. This generates an absurd result, because performing many of these activities would have been technically impossible at the time legislators enacted the CFAA. It is therefore "unreasonable to believe" that the legislators intended to allow punishment for these acts using the CFAA. Holy Trinity Church, 143 U.S. at 459. Extending the CFAA to cover those acts is as improper as extending the statutes in Katz and Jin Fuey Moy to punish acts that the laws did not quite reach. Although such conduct may warrant prosecution, the responsibility lies with Congress to amend the CFAA or enact additional laws punishing harmful computer behavior.

2. The Legislative History of the CFAA Indicates that the Drafters Were Not Concerned with Those Who Misuse Computer Use Restrictions

Where the words of a statute are ambiguous, "the judiciary may properly use the legislative history to reach a conclusion" as to their meaning. United States v. Pub. Utilities Comm'n of Cal., 345 U.S. 295, 315 (1953). Therefore, this Court can look to documents that shaped the CFAA if it does not find that the plain language is clear.

a. The CFAA Drafters Aimed to Punish Hackers and Password Thieves

The code-based paradigm of interpreting "exceeds authorized access" best reflects the original "trespass" rationale of the CFAA. According to this analogy, an individual who breaks into a computer by exploiting weaknesses in computer code—otherwise known as a hacker—is an unauthorized entrant. This entrant is analogous to a trespasser who exploits weaknesses in barriers protecting a home.

The drafters of the CFAA explicitly relied on the trespass metaphor in defining "unauthorized" users. See H.R. Rep. No. 98-894, at 20 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3706 ("Thus, the conduct prohibited is analogous to that of 'breaking and entering' . . . ."); Computer Crime and Computer Security, Hearing on H.R. 1001 and H.R. 930 Before the Subcomm. On Crime of the H. Comm. on the Judiciary, 99th Cong., 213 (1985) (statement of Representative William Hughes, Chairman of the Subcommittee on Crime) (drawing an explicit analogy to unauthorized computer access and trespassing or breaking into a house); H.R. Rep. No. 99-612, at 6 (1986) (discussing the problem of computer "hackers" who trespass into computers).

As the Government's contract-based definition of "authorization" does not fit the "trespass" metaphor, Nosal's code-based interpretation of the CFAA demonstrates more fidelity to Congressional intent.

Extending the trespass analogy, an individual authorized to enter a computer must possess a proper password, much like an individual authorized to enter a home will possess a key. The legislative history illustrates how the CFAA drafters intended to punish individuals who use passwords to which they are not entitled as criminals who "exceed authorized access." See Computer Crime and Computer Security, Hearing on H.R. 1001 and H.R. 930 Before the Subcomm. On Crime of the H. Comm. on the Judiciary, 99th Cong., 213 (1985) (statement of Representative William Hughes, Chairman of the Subcommittee on Crime) (describing a hypothetical scenario punishable under the CFAA involving an employee who

obtains an access subcode to which he has no right and uses that to access data); see also S. Rep. No. 99-432, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2480 (expressing concern about the proliferation of "pirate bulletin boards" used to exchange passwords for accessing computers).

Nowhere does the statutory history indicate that the individual who uses his own password to obtain data that he later improperly discloses under the terms of an agreement restricting data use is also a trespasser. Accordingly, adopting the Government's "contract-based" paradigm for defining authorization and entitlement will contravene Congressional intent.

b. Congress Consciously Excluded Misuse of Computer Data from the Scope of the CFAA

In initially enacting the CFAA, the drafters expressed their intent to "exclude from these sections coverage of a person authorized to access a computer who merely exceeds such authorization by . . . use of the computer (e.g., if a government employee does homework or plays computer games on a government computer)." H.R. Rep. No. 98-894, at 15, reprinted in 1984 U.S.C.C.A.N. 3689, 3701; see also S. Rep. No. 99-432, at 7 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2486 (stating that the Committee considered comments from the Department of Justice and others and wanted to clarify that the statute was not so broad as to create a risk that authorized users would face prosecution for acts of computer access that "while technically wrong, should not rise to the level of criminal conduct").

Moreover, Congress consciously removed terms that punish the disclosure of information obtained from a computer from earlier versions of the CFAA. Compare

H.R. Rep. No. 98-894, at 3, 15 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3689, 3701 (punishing a person who, "having accessed a computer with authorization . . . knowingly uses, modifies, destroys, or discloses information in . . . such computer . . . .") with S. Rep. No. 99-432, at 7 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2486 (eliminating this provision).

Reasoning that a punishment for improperly disclosing computer data will penalize whistleblowers, Congress consciously narrowed the law to target computer trespassers—what it thought to be of paramount concern. See Computer Crime and Computer Security, Hearing on H.R. 1001 and H.R. 930 Before the Subcomm. On Crime of the H. Comm. On the Judiciary, 99th Cong., 142 (1985) (recording statements of ACLU attorneys arguing that the CFAA punishes even those who have proper access to computers); S. Rep. No. 99-432, at 7 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2484-85 (noting that the amended statute will punish "simple trespass offense[s]").

The legislative history indicates that Congress did not want to criminalize the type of misuse that this Court will punish if it adopts the Government's reading of the CFAA. Accordingly, contorting the meaning of the phrase "exceed authorized access" to include violations of use restrictions imposed by contract defies the wishes of Congress.

3. To Conform to the In Pari Materia Canon, This Court Should Interpret the CFAA Consistently with Its Sister Statute

The in pari materia canon advises this Court to construe statutes addressing the same subject matter "as if they were one law." Erlenbaugh v. United States, 409

U.S. 239, 243 (1976). The CFAA addresses unauthorized employee access to private computer information. Similarly, the Stored Electronic Communications Act ("SCA") contains the phrase "exceeds authorized access" and aims to prohibit improper access of electronic communications. See Electronic Communications Privacy Act, Pub. L. No. 99-508 § 2701, 100 Stat. 1860 (1986) (codified at 18 U.S.C. § 2701). Accordingly, the in pari materia canon of construction applies. The canon "makes the most sense when the statutes were enacted by the same legislative body at the same time." Erlenbaugh, 409 U.S. at 244. It is thus particularly apt to use it here, given that Congress enacted both the relevant version of the CFAA and the SCA in 1986.

Under the SCA, "[a] member of the general public authorized to access the public portion of a computer facility would violate the statute by exceeding this authorization and accessing the private portions of the facility." S. Rep. No. 99-541, at 36, reprinted in 1986 U.S.C.C.A.N. 3555, 3590. The legislators thus seemed to adopt a trespass-based definition of "exceeds authorized access" like the framers of the CFAA did. The authors of the SCA also noted their concern about those unauthorized users who gain access to and tamper with electronic communications. See H.R. Rep. No. 99-647, at 62 (1986). The SCA thus seems to interpret "authorization" in the context of electronic or code-based access permission. Accordingly, the SCA does not seem to embrace a reading of "exceeds authorized access" that turns on terms of use restriction contracts. Giving effect to the canon of in pari materia, then, the Court should read the CFAA to punish

hackers as "unauthorized" computer users, as this is the only way to honor the code-based trespass framework that animates the SCA, a related statute.

## II. ESTABLISHED PRINCIPLES OF STATUTORY INTERPRETATION ALSO COMPEL A NARROW READING OF THE CFAA

When faced with ambiguous language in a criminal statute, this Court must construe the law to fit with several "wise principles" that it "has long followed." United States v. Bass, 404 U.S. 336, 347 (1971). One such principle is the "venerable rule of lenity." United States v. R.L.C., 503 U.S. 291, 305 (1992). This rule favors the "more lenient interpretation of a criminal statute." Kasten v. Saint-Gobain Performance Plastics Corp., 131 S. Ct. 1325, 1336 (2011).

Additionally, there is a "long-established practice" of refraining from deciding the constitutionality of a statute, Ashwander v. Tennessee Valley Auth., 297 U.S. 288, 341 (1936) (Brandeis, J., concurring), when "ambiguous statutory language [can] be construed to avoid serious constitutional doubts." FCC v. Fox Television Stations, Inc., 129 S. Ct. 1577 (2010).

Finally, this Court strives to maintain a "healthy balance of power between the States and the Federal Government." Gregory v. Ashcroft, 501 U.S. 452, 458 (1991). To that end, it habitually construes "statutes which invade the common law" in a manner that avoids a "derogation of traditional legal principles." Pasquantino v. United States, 544 U.S. 349, 359 (2005). It also refrains from creating federal criminal law absent a clear statement from Congress. Jones v. United States, 529 U.S. 848, 858 (2000).

If this Court wishes to maintain fidelity to these cardinal interpretive rules, it has no choice but to construe the CFAA to exclude punishment for breaches of terms-of-use agreements. At most, it may read the CFAA narrowly to punish computer hackers and password thieves exclusively.

A. The Rule of Lenity Directs This Court to Read the CFAA Narrowly to Favor Potential Defendants and to Defer to Congress's Legislative Powers

Where there is ambiguity in a criminal statute, "doubts are resolved in favor of the defendant" as a matter of conventional statutory interpretation. United States v. Bass, 404 U.S. 336, 348 (1971). This principle, known as the "rule of lenity," compels courts to favor the "more lenient interpretation" of a criminal law when it construes an "ambiguous statute." Kasten v. Saint-Gobain Performance Plastics Corp., 131 S. Ct. 1325 (2011).

The rule of lenity is perhaps one of the oldest and best-established principles governing statutory interpretation. It is "founded on . . . the plain principle that the power of punishment is vested in the legislative, not in the judicial department." See United States v. Wiltberger, 5 Wheat. 76, 95, 18 U.S. 76, 95 (1820). Additionally, the rule of lenity safeguards the rights of potential defendants by warning them about what conduct a statute considers to be criminal. United States v. Lanier, 520 U.S. 259, 266 (1997).

Despite this Court's zeal to clarify the ambiguous text of the CFAA, the rule of lenity advises it to avoid "making criminal law in Congress's stead." R. at 27 (quoting United States v. Santos, 553 U.S. 507 (2008)). Criminalizing actions that

vaguely resemble conduct penalized by the plain terms of the law is thus a "dangerous" endeavor that the Court should avoid. See Wiltberger, 5 Wheat. at 96.

Construing the CFAA broadly will aggrandize judicial power. By allowing any private contract to set terms that define criminal behavior, this Court will pull into the scope of a CFAA many acts besides conventional "hacking" and password theft. The Government's proposed interpretation effectively allows the Court to enact criminal legislation sub silentio by interpreting federal statutes broadly. The rule of lenity will check such "dangerous" judicial encroachment on Congressional powers, by preventing this Court from interpreting the CFAA in a manner that punishes a wider array of conduct. Id. The rule thereby preserves the principle that "the power of punishment is vested in the legislative, not in the judicial department." Wiltberger, 5 Wheat. at 95.

Applying the rule of lenity to invalidate the Government's contract-centric interpretation of "authorization" will also give notice to potential defendants. The Government's interpretation will "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." R. at 22-23. Such a sea change in the scope and purpose of the CFAA will utterly fail to "ensure[] that citizens will have fair notice of the criminal laws" and will "unintentionally turn ordinary citizens into criminals." R. at 29. Restricting the CFAA to punish only hackers and password thieves will protect those who lack sufficient notice that their "otherwise innocuous behavior" will trigger federal criminal liability. R. at 22.

Accordingly, the Court should reaffirm the decisions of lower courts interpreting the CFAA[1] by yielding to the rule of lenity and construing the law to exclude violations of contracts restricting computer use.

B. This Court Must Interpret the CFAA Strictly to Avoid Deciding Constitutional Questions Absent a Clear Statement from Congress

If interpreting a statute in a particular manner raises a "serious doubt of constitutionality," it is a "cardinal principle" that this Court will try to construe it in a manner that avoids the question. Crowell v. Benson, 285 U.S. 22, 62 (1932); see also Ashwander v. Tennessee Valley Auth., 297 U.S. 288, 341 (1936) (Brandeis, J., concurring). However, as a corollary to this "canon of constitutional avoidance," this Court will confront the "serious constitutional questions" if it identifies an "affirmative intention" of Congress to do so. NLRB v. Catholic Bishops of Chicago, 440 U.S. 490, 501 (1979).

The constitutional avoidance cannon manifests the "fundamental and longstanding principle of judicial restraint" that directs courts to "avoid reaching constitutional questions in advance of the necessity of deciding them." Lyng v. Nw. Indian Cemetery Protective Ass'n, 485 U.S. 439, 445 (1988). Accordingly, the canon

[1] See WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 204-06 (4th Cir. 2012); LVRC v. Brekka, 581 F.3d 1127, 1134-35 (9th Cir. 2009) (construing the CFAA narrowly in accordance with the rule of lenity in a case brought under the private action provision of the statute); Orbit One Commc'ns, Inc., v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010) (emphasizing that the rule of lenity imposes a "fair warning requirement" on criminal statutes); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966-67 (D. Ariz. 2008) (finding that the rule of lenity guides interpretations of the CFAA because it has "both criminal and noncriminal applications"); Int'l Ass'n of Machinists v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005) (reasoning that because the CFAA is primarily a criminal statute, it should be construed narrowly).

encourages cautious behavior that preserves the "heavy presumption of constitutionality" to which a "carefully considered decision of a coequal and representative branch of our government is entitled." United States Dep't of Labor v. Triplett, 494 U.S. 715, 721 (1990) (internal citations omitted).

Interpreting the CFAA broadly to allow criminal liability to attach to breaches of computer use agreements triggers at least two serious constitutional issues not clearly flagged by Congress. First, it is likely that vague, boilerplate terms-of-use contracts will "fail to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden" by the CFAA. Bouie v. City of Columbia, 378 U.S. 347 (1964). This will, at least in some cases, violate the due process protections inherent in the Fifth Amendment and thus implicate a "serious constitutional question." Catholic Bishops, 440 U.S. at 501. Additionally, interpreting the CFAA to allow private parties to define the contours of criminal liability raises a concern about the constitutionality of delegating legislative powers to politically unaccountable bodies. A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935).

1. Allowing Opaque Contracts to Restrict Computer Use Will Render the CFAA Unconstitutionally Void-for-Vagueness

Construing CFAA § 1030(e)(6) with reference to private terms-of-use agreements ties criminal liability to the vagaries of dense, extra-statutory contracts and law enforcement's interpretation of such policies. At least some of these boilerplate documents will undoubtedly "fail to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden by the

statute." Bouie v. City of Columbia, 378 U.S. 347 (1964). Incorporating expansive terms-of-use agreements into the CFAA by reference thus raises a serious related question about whether the statute is "void for vagueness." As vague statutes encourage discriminatory enforcement, a broad interpretation of the CFAA will inevitably raise concerns about unconstitutionally arbitrary prosecution. Kolender v. Lawson, 461 U.S. 352, 357 (1983).

The void-for-vagueness doctrine and its relatives originate from the Fifth Amendment's Due Process Clause. United States v. Williams, 553 U.S. 285, 304 (2008). Accordingly, the Court risks improperly wrestling with constitutional questions by interpreting the CFAA broadly in the absence of a clear statement from Congress to do so.

If the phrase "exceeds authorized access" incorporates noncompliance with any of the myriad terms and conditions typical of private use agreements, punishment will rest on at least some vague provisions. If the terms use normative language that fails to specify any "standard of conduct at all," there may be a "serious" question about whether the CFAA is unconstitutionally vague. Coates v. City of Cincinnati, 402 U.S. 611, 614 (1971). In Coates, this Court invalidated an ordinance prohibiting conduct "annoying to persons passing by" because the statute failed to specify any "standard of conduct" to which individuals could adhere. 402 U.S. at 614.

The user policy the Ninth Circuit cited prohibits submitting "misleading" information to websites. R. at 25. What is misleading to some may not be so to

others, just like what is "annoying" to some may not be so to others. Coates, 402 U.S. at 614. Accordingly, individuals of "common intelligence must necessarily guess" whether a breach of such terms will render them criminally culpable, in violation of the void-for-vagueness doctrine. Coates, 402 U.S. 614.

Just as this Court invalidated the standardless ordinance in Coates, it may have to declare the CFAA unconstitutionally vague, at least cases where the terms-of-use agreement is hopelessly broad.

Furthermore, allowing vague standards to define culpable conduct will effectively vest "virtually complete discretion in the hands of the police" to prosecute perceived unlawful conduct. Kolender, 461 U.S. at 358. Complete discretion encourages "arbitrary and discriminatory enforcement," which in turn violates the Due Process Clause of the Fifth Amendment. Id. at 357. See also United States v. Drew, 259 F.R.D. 449, 465-66 (C.D. Cal. 2009) (finding that an expansive interpretation of "exceeds authorized access" will encourage discriminatory enforcement by allowing prosecutors to "pursue their personal predilections" in the absence of clear language indicating what conduct should be punished).

In the absence of a clear statement from Congress, this Court must not adopt an interpretation of the CFAA that triggers constitutional questions. A construction that defines "exceeds authorized access" narrowly avoids generating a "serious doubt" about the constitutionality of the law. Crowell v. Benson, 285 U.S. 22, 62 (1932). Accordingly, the Court should disregard the Government's contract-based

theory of authorization and exclude breaches of terms-of-use agreements from the ambit of the statute.

2. A Serious Constitutional Question Will Arise if Unaccountable Entities Define Criminal Behavior

Although this Court has long permitted Congress to delegate lawmaking authority to non-legislative bodies, there exist implied limits to that power that have remained untested for decades. Mistretta v. United States, 488 U.S. 361, 371 (1989). Allowing contract-based computer use restrictions to create criminal liability pushes the boundaries of this doctrine. Because the Government's position raises a constitutional question concerning the delegation of lawmaking power, the Court should avoid construing the statute as it requests.

This Court ordinarily acquiesces to delegations of lawmaking powers to coordinate branches of the federal government. However, Congress must establish "an intelligible principle to which the person or body authorized to [exercise the delegated authority] is directed to conform." J.W. Hampton, Jr. & Co. v. United States, 276 U.S. 394, 409 (1928). The Court has however, invalidated delegations of legislative power when it has determined that such grant gives too much lawmaking authority to an unaccountable body. Specifically, this Court struck down the legislative delegation to agencies under the National Industrial Recovery Act in Panama Refining Co. v. Ryan, 239 U.S. 388 (1935), and in A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935).

This Court justified its decisions in part because the statute created new federal crimes of conduct that previously did not constitute criminal

behavior. See Fahey v. Mallonee, 322 U.S. 245, 249 (1947) (interpreting the decisions in Panama Refining and Schechter Poultry). Furthermore, this Court in Schechter Poultry expressed concern about Congress delegating lawmaking power to private individuals. See 295 U.S. at 537 (questioning whether Congress could delegate its legislative authority to groups enacting laws they deem to be wise and beneficent for "the rehabilitation and expansion of their trade or industries").

The Court has since "upheld . . . without deviation, Congress' ability to delegate power under broad standards." Mistretta, 488 U.S. at 73. However, no subsequent case has triggered its main concerns about delegating power to private parties or delegating power to create novel federal criminal law.

A broad reading of the CFAA unearths exactly those twin fears about the limits of the nondelegation principle that have remained buried for decades. It will criminalize violations of terms-of-use agreements, necessarily creating "federal crimes of acts that never had been such before." Fahey, 332 U.S. at 249. It will also allow private employers and website owners to set the terms of criminal conduct through rarely-examined, one-sided, and frequently changed contracts of adhesion that will only benefit their interests. This is tantamount to empowering industry associations to "enact the laws they deem to be wise and beneficent" for their own expansion. Schechter Poultry, 295 U.S. at 537; see also Note, The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation, 127 Harv. L. Rev. 751 (2013).

An expansive reading of § 1030(e)(6) that includes express or implied terms of use violations and thus outsources the task of selecting and defining criminal conduct to unaccountable private parties will open a Pandora's box of constitutional issues. This is because questions about the proper delegation of Congressional lawmaking power are constitutional questions. The nondelegation doctrine may, however, be sidestepped through the canon of constitutional avoidance. See John F. Manning, The Nondelegation Doctrine as a Canon of Avoidance, 2000 Sup. Ct. Rev. 223 (2000). Unless this Court believes that Congress intended to disturb the precarious corpus of non-delegation law by its use of the phrase "exceeds authorized access," it should not read into § 1030(e)(6) an ability to punish simple violations of computer user agreements created through private contracts.

If this Court interprets § 1030(e)(6) to encompass violations of private computer terms-of-use agreements, it will necessarily revive the slumbering giant that is the nondelegation doctrine by triggering serious constitutional questions about whether Congress may grant individuals power to define conduct that generates criminal liability. Because Congress could not have signaled its desire for this Court to address weighty constitutional issues simply through its use of the term "exceeds authorized access," the Court should construe the CFAA narrowly to give it the "heavy presumption of constitutionality" it deserves. United States Dep't of Labor v. Triplett, 494 U.S. 715, 721 (1990).

C. Federalism Concerns Require the CFAA to Preserve Centuries of Contract Law in a Field Reserved for State Legislation

Prosecuting individuals who ignore the terms of computer use agreements will wreak unprecedented havoc on "literally centuries of the common law." Complete Auto Transit, Inc. v. Reis, 451 U.S. 401, 425 (1981). This is because the law has never allowed imprisonment for what is essentially a breach of contract. It is well-established that "statutes that invade the common law" presumably favor retaining "long-established and familiar principles." Pasquantino v. United States, 544 U.S. 349 (2005). Therefore, the only sensible reading of the CFAA is one that does not destroy settled precepts of common law resolving breaches of private agreements exclusively as civil wrongs under state law.

Additionally, the CFAA must not usurp the established roles of Congress and state governments. Gregory v. Ashcroft, 501 U.S. 452, 459 (1991). Both contract law and criminal law are within the domain of state courts and legislatures. Accordingly, this Court should strive not to encroach on the "the historic police powers of the states" absent a "clear and manifest purpose of Congress." Rice v. Santa Fe Elevator Corp., 331 U.S. 218 (1947).

1. Authorizing Imprisonment for Simple Breaches of Contract Flies in the Face of Centuries of Common Law

Reading the CFAA broadly penalizes those who disobey computer terms of use agreements. See R. at 6; CFAA § 1030(c)(2)(A) (setting the penalty for violations of CFAA § 1030(a)(2) as "a fine . . . or imprisonment for not more than one year, or both . . . ."); CFAA § 1030(c)(3)(A) (setting the penalty for violations of CFAA § 1030(a)(4) as "a fine . . . or imprisonment for not more than five years, or both . . .

."). This is tantamount to punishing mere breaches of contract as crimes, which is unheard of and foreign to the common law. Since "[s]tatutes which invade the common law . . . are to be read with a presumption favoring . . . long-established and familiar principles," such a radical construction of the CFAA is wholly inappropriate. Pasquantino v. United States, 544 U.S. 349 (2005).

It is well-established that punitive damages and criminal sentences, "unlike compensatory damages and injunction, are generally not available for breach of contract." Barnes v. Gorman, 536 U.S. 181, 187 (2002). See also Douglas Laycock, Modern American Remedies 262 (4th Ed. 2010) (arguing that at least formally, no cases allow imprisonment as a civil penalty for a breach of contract). Although academics may discuss whether courts should award punitive sanctions for breaches of contract, the governing rule prohibits criminal penalties for ordinary breaches of private agreements. William S. Dodge, The Case for Punitive Damages in Contracts, 48 Duke L.J. 629 (1999).

This elementary principle also exists in numerous opinions emanating from the highest state courts.[2] Any interpretation of the CFAA questioning this principle

[2] See, e.g., Freeman & Mills, Inc. v. Belcher Oil Co., 900 P.2d 669 (Cal. 1995) (refusing to award punitive damages for an action for denial of contract); Mortg. Fin. Inc. v. Podleski, 742 P.2d 900 (Colo. 1987); Goins v. W. R.R. of Ala., 68 Ga. 190 (1881); Miller Brewing Co. v. Best Beers of Bloomington, Inc., 608 N.E.2d 975, 984 (Ind. 1993) (determining that punitive damages are available in a contract action only if there exists an independent tort); Higgins v. Blue Cross of W. Iowa & S. Dakota, 319 N.W.2d 232 (Iowa 1982); Louisville & Nashville R.R. Co. v. Wilkerson, 8 Ky. Op. 671 (1876); McGinnis v. Honeywell, Inc., 791 P.2d 452 (N.M. 1990); Pioneer Fuels, Inc. v. Montana-Dakota Utilis. Co., 474 N.W.2d 706, 709 (N.D. 1991); W. Union Tel. Co. v. Reeves, 126 P. 216 (Okla. 1912); Welborn v. Dixon, 49 S.E. 232, 236 (S.C. 1904); Wangen v. Ford Motor Co., 294 N.W.2d 437, 443 (Wis. 1980).

violates the rule that "Congress . . . acts in the context of existing common-law rules." Pierson v. Ray, 386 U.S. 547, 561 (1967).

Nowhere does the plain text of the CFAA seem to acknowledge that the statute imposes exemplary damages for breaches of private agreements ordinarily enforced through civil suits—let alone imprisonment. Congress has "failed to establish by the clearest proof" that it has provided "a sanction so punitive as to transfor[m] what was . . . intended as a civil [action] into a criminal penalty." United States v. Ursery, 518 U.S. 267, 278 (1996). A broad construction of the CFAA will therefore inappropriately upend centuries of established contract law principles.

2. A Presumption Against Federalizing Common Law Counsels That the CFAA Not Police Computer Misuse

Before Congress turns over a field traditionally reserved for state governments to the federal courts, it must make an "an unmistakably clear statement to that effect." Jones v. United States, 529 U.S. 848, 858 (2000); Pennhurst State Sch. & Hosp. v. Halderman, 465 U.S. 89, 99 (1984).

In Rewis v. United States, 401 U.S. 808 (1971), this Court declined to expand criminal liability under the Travel Act to punish a larger class of people than enumerated in the statute, particularly when the legislative history was silent on that point. Id. at 811-12 (noting that the Court was "struck by what Congress did not say").

Although the CFAA is a federal statute manifesting Congressional intent to shift litigation of some computer trespass-based crimes to the federal courts, "[i]t is

unlikely that Congress, given its concern about the appropriate scope of Federal jurisdiction in the area of computer crime" intended to "essentially to criminalize state-law breaches of contract." See Brett Senior & Assocs. v. Fitzgerald, No. 06-1412, 2007 WL 2043377 at *4, (E.D.Pa. July 13, 2007); see also S. Rep. No. 99-432, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2482 (stating that lawmakers desired to narrow the reach of the law because they were "especially concerned about the appropriate scope of Federal jurisdiction in this area").

Nowhere in the text of the CFAA does Congress indicate that it wishes this Court to create law broadly policing crimes stemming from misconduct due to improper trade secret disclosures, cyberbullying, or workplace policy violations. The term "exceeds authorized access" alone provides scant evidence of Congressional intent to enter into the province of state common law; reading the CFAA to allow such a result is improper. Like in Rewis, this Court should take note of an absence of Congressional intent to punish a wide range of crimes. 401 U.S. at 811-12. Construing the CFAA to occupy a broader space in criminal law will open the floodgates to federal criminal litigation that will disturb the balance of authority over these offenses between federal and state governments.

The Government argues that there is a need to use the CFAA as an all-purpose Internet patrol statute. However, expanding the reach of the CFAA to cover offenses traditionally resolved under state law will invariably disturb the "healthy balance of power between the States and the Federal Government." Gregory v. Ashcroft, 501 U.S. 452, 458 (1991). Therefore, absent a clearer statement from

Congress, the CFAA cannot federalize anything more than code-based computer crimes and password theft.

## CONCLUSION

The Court should adopt a narrow reading of the CFAA pursuant to established principles of statutory interpretation. Expanding the CFAA criminalizes not only the hacker and the cyberbully, but also the student, the whistleblower, the investigative journalist, the computer programmer, and the harmless prankster. Such an interpretation fails to provide sufficient notice to potential defendants about what constitutes criminal activity, threatens to raise the specter of serious constitutional challenges to the law, and usurps the role of state governments in policing crime. Accordingly, this Court should AFFIRM the decision of the Ninth Circuit and find that the phrase "exceeds authorized access" does not extend to computer use restrictions.

Dated: February 24, 2014

Respectfully submitted,

_____

ANURADHA SIVARAM
Counsel for Respondent

# APPENDIX

## SELECTED PROVISIONS OF THE COMPUTER FRAUD AND ABUSE ACT

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(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;