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 PETITIONER

JESSICA L. DIAZ
Attorney
Counsel of Record for Petitioner

University of California, Berkeley
School of Law
Berkeley, CA 94720
jessica.diaz@berkeley.edu
(707) 321-1577

QUESTION PRESENTED

In interpreting the Computer Fraud and Abuse Act, 18 U.S.C. §1030 (2012), does the phrase "exceeds authorized access" include accessing information for unauthorized uses?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Legislative Materials

STATEMENT OF THE CASE

Nearly thirty years ago, Congress created the first cohesive framework to combat what was then a novel but rapidly mounting threat to businesses, government agencies, and individuals alike: computer crime. H.R. Rep. No. 98-894, at 6 (1984). In passing the Computer Fraud and Abuse Act (CFAA), Congress recognized that the existing patchwork of criminal laws failed to sufficiently address an emerging brand of criminal, one "who uses computers to steal, to defraud, and to abuse the property of others." S. Rep. No. 99-432, at 2 (1986). At issue in this case is the interpretation of the statute's three-word phrase, "exceeds authorized access." (R. at 3.) Hanging in the balance is whether these words will be read broadly enough to address the scope of theft, fraud and abuse that Congress placed squarely in the CFAA's crosshairs.

To address the growing threat of computer-related crime, the CFAA establishes a number of offenses. *See* 18 U.S.C. § 1030(a)(1)–(7) (2012). The penalties for these offenses range in severity from a fine and/or imprisonment for up to one year, to a fine and/or imprisonment for life. *See id.* § 1030(c)(2)(A), (c)(4)(F).

Among the CFAA's offenses is Section 1030(a)(4). This provision subjects someone to criminal sanction where he or she "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 . . . ".[1] *Id.* § 1030(a)(4). Provided the defendant has no prior conviction under the CFAA, this offense is punishable by fine, imprisonment not to exceed five years, or both. *Id.* § 1030(c)(3)(A).

This case arose out of precisely such an offense: respondent David Nosal's scheme to acquire confidential information from his former employer for the purpose of founding his own, competing firm. (R. at 13–14.) After leaving his job at the executive search firm, Korn/Ferry, Nosal recruited some of his former co-workers to assist in his scheme. (R. at 13.)

As Korn/Ferry employees, Nosal's alleged co-conspirators had access to Korn/Ferry's confidential database through their log-in credentials. (*Id.*) The opening screen of this database included the express warning that "[t]his product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." (*Id.*) In spite of both this warning and a company policy forbidding the disclosure of confidential information, these Korn/Ferry employees downloaded source lists, names, and contact information, and then transferred this data to Nosal. (*Id.*)

Nosal was indicted on twenty counts, one of which was aiding and abetting his former co-workers in violating Section 1030(a)(4). (R. at 14.) Specifically, the government alleged that under the CFAA, Nosal's co-conspirators "exceeded authorized access" by accessing Korn/Ferry's confidential database in order to

[1] This provision further specifies that someone is not subject to liability where the only item obtained was computer usage valued at less than $5,000 in a year-long period. 18 U.S.C. § 1030(a)(4) (2012).

acquire information for a competitor—a purpose that fell indisputably outside the scope of these employees' authorization. (*Id.*)

Nosal argued before the trial court that the CFAA did not extend to his co-conspirators' conduct, based on his interpretation of the phrase "exceeds authorized access." (*Id.*) He contended that because his former co-workers accessed the Korn/Ferry computer with authorization and merely *misused* the information they obtained "by means of such access," they did not "exceed[] authorized access" under the meaning of the statute. (*Id.*)

The interpretation of the phrase "exceeds authorized access" has been the topic of divergent opinions amongst the federal courts of appeals. (*See* R. at 27.) Under 18 U.S.C. § 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." (R. at 10.) The question is therefore whether the CFAA extends to a situation such as the one at bar, where someone is entitled to obtain information for *business* reasons, but obtains it instead for other, *un*authorized purposes. (*See* R. at 14.)

The trial court initially rejected Nosal's position, instead siding with the government's interpretation that Nosal's co-conspirators "exceed[ed] authorized access." (R. at 14.) The court reversed its prior judgment, however, after the Ninth Circuit Court of Appeals adopted a narrow interpretation of "exceeds authorized access" in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). (R. at 14.) Following *Brekka*, the district court applied this narrow interpretation to conclude

that "exceeds authorized access" did not extend to a situation where someone has authorization as a general matter to access information but accesses it for unauthorized purposes. (*Id.*) The district court accordingly dismissed the CFAA counts at issue. (*Id.*)

The Ninth Circuit Court of Appeals, sitting en banc, affirmed the lower court's ruling in a split opinion. (R. at 30.) Writing for the majority, Chief Judge Kozinski recognized other circuits' contrary positions, but "declined to follow" their interpretation of the CFAA and "urged[d] them to reconsider instead." (R. at 27.) In rejecting the government's argument that "exceeds authorized access" includes use restrictions, Judge Kozinski expressed concern that such an interpretation would criminalize harmless conduct, such as inadvertently violating the terms of use for a social media or dating website. (R. at 24–25.) The majority concluded that the phrase "exceeds authorized access" "is limited to violations of restrictions on *access* to information, and not restrictions on its *use*." (R. at 29.)

Judges Silverman and Tallman dissented, critiquing the majority's interpretation of the statute as "parse[d] . . . in a hyper-complicated way that distorts the obvious intent of Congress." (R. at 31.) The dissent noted that this case had "nothing to do with playing sudoku, checking email, fibbing on dating cites, or any of the other activities that the majority rightly values." (*Id.*) Rather, citing cases from the First, Fifth, and Eleventh Circuits applying the government's proposed interpretation, (R. 34–35), the dissent concluded that the phrase "exceeds

authorized access" applied to the case here, where Nosal's co-conspirators accessed information for clearly unauthorized purposes, (R. at 35–36).

The government petitioned for certiorari, and this Court granted certiorari on the question of whether the phrase "exceeds authorized access" is limited to "access restrictions, or includes use restrictions." (R. at 3.)

SUMMARY OF THE ARGUMENT

In enacting a comprehensive legal regime to counter the economic and security threats posed by computer-related crime, Congress intended to address not only unauthorized access but also the unauthorized use of information. The CFAA was not just a surgical strike on one pernicious new *means* of coopting private information. Rather, the CFAA reflected a broader effort to combat the *impacts* of such illicit behavior. Among these impacts were the widespread use of individuals' financial account information, theft of intangible assets from businesses and public agencies, and even the acquisition of sensitive medical records. *See* S. Rep. No. 99-432, at 2–3 (1986); *see also Task Force on Computer Crime Section of Criminal Justice, American Bar Association, Report on Computer Crime* 38 (1984). The Ninth Circuit's myopic focus on "hacking" thwarts Congress' intent to comprehensively address the myriad impacts of computer crime.

The statutory text itself illustrates Congress' intent to include unauthorized purposes within the CFAA's ambit. Because the statute provides a definition of "exceeds authorized access" in 18 U.S.C. § 1030(e)(6), the plain language of that provision is controlling. *See Burgess v. U.S.*, 553 U.S. 124, 129 (2008). Under Section 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." (R. at 10.)

As a threshold matter, the government's interpretation is consistent with the ordinary usage of the phrase "entitled so." Unlike the Ninth Circuit's narrowing

construction, moreover, the broader interpretation of "exceeds authorized access" gives meaning to the word "so" in Section 1030(e)(6), rendering no word superfluous. The canon of surplusage thus favors the broader construction. *See Marx v. Gen. Revenue Corp.*, 133 S. Ct. 1166, 1177 (2013) (competing statutory interpretations are resolved in favor of the one that gives meaning to each word and clause).

While the statute's plain language alone may be sufficient to foreclose any ambiguity, the CFAA's legislative history further bolsters the broader interpretation of "exceeds authorized access." *See* 73 *Am. Jur. 2d Statutes* § 83 (2014) (legislative history may serve a "confirmatory" role even where statutory language is unambiguous). An earlier version of the CFAA, enacted in 1984, explicitly proscribed "knowingly access[ing] a computer without authorization, or having accessed a computer with authorization, us[ing] the opportunity such access provides *for purposes to which such authorization does not extend*." S. Rep. No. 99-432, at 3 (1986) (emphasis added). Committee reports from both chambers indicate that when Congress later substituted this language with the phrase "exceeds authorized access," the change was intended merely to clarify the prior, "cumbersome" wording. *Id.* at 9; *see also* H.R. Rep. No. 99-612, at 11 (1986). Congress' stated policy goals in enacting the CFAA, moreover, demonstrate that that legislators fully contemplated the broader interpretation of "exceeds authorized access."

In light of the statute's plain language and legislative history, the CFAA cases adopting the broader interpretation of "exceeds authorized access" have

exemplified the more persuasive approach. Courts have employed two approaches to determining what constitutes an "unauthorized" purpose. Under the "contracts" approach, courts look to tangible indications of whether obtaining information for a given purpose was proscribed. *See, e.g.*, *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001) (confidentiality agreement barred any disclosure that would be adverse to the company). Other courts have employed an "agency" approach, looking to whether an employee severed the agency relationship with an employer, thus extinguishing any "authorized" access. *See, e.g. Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 421–22 (7th Cir. 2006) (authorization to access company laptop ceased when employee decided to start his own competing business). These approaches have proven both administrable and consistent with the statute's plain language.

The CFAA caselaw also demonstrates that the broader interpretation of "exceeds authorized access" is necessary to address serious threats to economic and personal security. "Hacking," or overcoming technological barriers to gain access, (*see* R. at 29), is merely one means of stealing proprietary or other sensitive information. An equal danger inheres to those who have authorization to access information for certain purposes but choose to coopt it for other, destructive ends. The respondent's narrowing construction of "exceeds authorized access" would insulate such conduct from CFAA liability.

Finally, the interpretive question in this case did not yield such a "grievous ambiguity" that a court should resort to "guess[ing] as to what Congress intended."

See Barber v. Thomas, 560 U.S. 474, 488 (2010). The Ninth Circuit's invocation of the rule of lenity was accordingly unwarranted, (*see* R. at 28–29), and fails to tip the scales towards the respondent's narrowing construction. Nor do the "void for vagueness" doctrine or other due process considerations require the court to abandon Congress' clear intent in enacting the CFAA. Despite the Ninth Circuit's fears to the contrary, even the government's broader interpretation of "exceeds authorized access" would not implicate innocuous workplace diversions or inadvertent violations of websites' terms of use.

In light of the statute's plain language, legislative history, purpose and context, the government's broader reading of "exceeds authorized access" more accurately reflects the magnitude of the issue at which Congress took aim. The petitioner accordingly urges this Court to reverse the Court of Appeals decision below.

ARGUMENT

I. BASED ON THE CFAA'S PLAIN LANGUAGE, THE PHRASE "EXCEEDS AUTHORIZED ACCESS" INCLUDES OBTAINING INFORMATION FOR UNAUTHORIZED PURPOSES.

The CFAA defines the term "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (2006).

In resolving issues of statutory interpretation, courts begin with the statute's plain language. *See BP Am. Prod. Co. v. Burton*, 549 U.S. 84, 91 (2006) ("We start, of course, with the statutory text."). Where Congress expressly provides for a statutory definition, as it did here, the language of that definition is controlling. *See Burgess v. U.S.*, 553 U.S. 124, 129 (2008). The task of interpreting the phrase "exceeds authorized access" thus begins with analyzing the plain language of Section 1030(e)(6). This provision's plain language evinces an unambiguous legislative intent to include not only access but also use restrictions within the scope of the phrase "exceeds authorized access."

A. Ordinary Usage of the Words in the Statutory Definition of "Exceeds Authorize Access" Demonstrate an Intent to Include Unauthorized Purposes.

It is undisputed that the phrase "exceeds authorized access" covers conduct where initial access to a computer was duly authorized. (*See* R. at 15.) The controversy, accordingly, is what it means for someone, having accessed a computer, to then "obtain or alter information in the computer that the accesser is not *entitled*

so to obtain or alter." *See* § 1030(e)(6) (emphasis added). The nugget of this dispute lies in the interpretation of the italicized language.

The plain meaning of the phrase "entitled so" unambiguously demonstrates an intent to include the use of information for unauthorized *purposes* within the CFAA's scope. While "entitled so" is not itself defined in the CFAA, undefined terms are assumed to take on their usual and ordinary meaning. *Roberts v. Sea-Land Services, Inc.*, 132 S. Ct. 1350, 1364 (2012). Looking to ordinary usage, Black's Law Dictionary defines "entitle" as "[t]o grant a legal right to or qualify for." *Entitle Definition, Black's Law Dictionary* (9th ed. 2010)*, available at* WestLawNext. In context, the most ordinary definition of the word "so" is "[i]n the way or manner described, indicated, or suggested; in that style or fashion." *So Definition, Oxford-English Dictionary Online*, www.oed.com (last visited Feb. 21, 2014).

Applying these words' ordinary usage supports the broader interpretation of the phrase "exceeds authorized access." For example, a sales employee may be authorized to access his employer's customer database for the purpose of processing new orders. This employee is legally authorized and qualified—he is *entitled*—to obtain customer information for business purposes. Yet this employee likely *lacks* comparable entitlement to obtain customer phone numbers and birthdays for personal use. In this sense, he is entitled to access the customer database, but only in "the way of manner described, indicated or suggested." *See id.* By acquiring customer phone numbers for patently unauthorized purposes, this employee thus obtains information that he is not entitled *so* to acquire.

B. The Canon Against Surplusage Favors the Broader Interpretation of "Exceeds Authorized Access."

Because the narrowing construction of "exceeds authorized access" urged by the respondent fails to imbue the word "so" with any meaning, it runs afoul of the canon against surplusage. Under this canon, the Court must give effect to "every word of a statute wherever possible." *Ransom v. FIA Card Servs., N.A.*, 131 S. Ct. 716, 724 (2011). While this canon has been characterized as an interpretive aid rather than a strict rule, it is particularly helpful "where a competing interpretation gives effect to every clause and word of a statute." *Marx v. Gen. Revenue Corp.*, 133 S. Ct. 1166, 1177 (2013).

Here, the government's interpretation serves to "give[] effect to every clause and word" by giving meaning to the word "so." Under the government's interpretation of Section 1030(e)(6), someone can "exceed[] authorized access" by obtaining or altering information that he or she is not entitled to obtain or alter in that "way or manner." *See So Definition*, *Oxford-English Dictionary Online*, *supra*. The word "so" adds this final clause. Returning to the example of the customer database, the sales employee may be entitled to access customer information to process sales orders, but not in a way or manner that entails mining the database for personal or competitive purposes.

Under the narrowing construction, in contrast, the word "so" is mere surplus verbiage. In addressing the canon against surplusage, the Ninth Circuit surmised that the word "so" in the definition of "exceeds authorized access" could simply be a conjunction. (R. at 16.) Yet no such conjunction was required. To proscribe someone

from accessing information that he or she is not "entitled to obtain or alter" would be perfectly grammatically correct. If anything, this would have been the more elegant choice of phrasing, making the phrase "entitled *so* to obtain or alter" all the more conspicuous. *See* § 1030(e)(6) (emphasis added).

Given the ordinary usage of the words Congress used in Section 1030(e)(6), coupled with the application of the canon against surplusage, the plain language of the CFAA favors the broader interpretation of "exceeds authorized access" as including restrictions on the *use* of information.

II. JUST AS THE CFAA'S PLAIN LANGUAGE SUPPORTS A BROAD STATUTORY CONSTRUCTION, SO TOO DOES ITS LEGISLATIVE HISTORY.

Because the plain language of the statute forecloses any ambiguity, the Court is not *required* to rely on extrinsic interpretative aids such as legislative history. *See United States v. Gonzales*, 520 U.S. 1, 6, (1997) ("Given the straightforward statutory command, there is no reason to resort to legislative history."). While unambiguous statutory language may be determinative as a general matter, the legislative history here may nonetheless provide instructive context for the Court and serve a "confirmatory" role. *See* 73 *Am. Jur. 2d Statutes* § 83 (2014). If the CFAA's language *were* deemed ambiguous, moreover, the legislative history strongly supports the broader interpretation of "exceeds authorized access."

A. The CFAA's Original Language, Coupled With Committee Reports on the 1986 Amendments, Demonstrate that Congress Intended to Effectuate the Broader Reading of "Exceeds Authorized Access."

In 1984, Congress enacted its first statute focused on computer crime. S. Rep. No. 99-432, at 3 (1986). Under this initial enactment ("the 1984 CFAA"), an element of each offense was to "knowingly access[] a computer without authorization, or having accessed a computer with authorization, use[] the opportunity such access provides *for purposes to which such authorization does not extend*." *Id.* (emphasis added). This earlier enactment thus *explicitly* addressed the type of situation at issue here, where the defendant had authorization to Korn/Ferry's database for business purposes, but accessed it instead "for purposes to which such authorization [did] not extend." (*See* R. at 13.) A pivotal question thus arises: whether Congress intended to narrow the CFAA's reach or merely simplify the statute's language when it enacted amendments two years later, in 1986 ("the 1986 Amendments").

"A statutory amendment may clarify rather than change the law. . . . When determining whether an amendment clarifies or changes a statute, the courts look to the amendment's plain language and legislative history, and the time and circumstances of an amendment may indicate that the legislature merely intended to clarify the intent of the original enactment." 73 *Am. Jur. 2d Statutes* § 63 (2014). As described below, House and Senate committee reports on the 1986 Amendments forcefully support the government's position that the phrase "exceeds authorized access" was meant merely to clarify rather than narrow the CFAA's prior reference to unauthorized "purposes."

1. The 1986 Amendments on the Whole Were Intended to Expand, and Not Narrow, the CFAA's Reach.

The CFAA's legislative history soundly rebuts the view that Congress intended the phrase "exceeds authorize access" to narrow the language in the 1984 CFAA. This is first because the overarching purpose of the 1986 Amendments was to expand, and not contract, the statute's reach. *See* H.R. Rep. No. 99-612, at 3–4 (1986).

When enacted in 1984, the CFAA established three offenses under 18 U.S.C. §1030(a), addressing only government-classified information (§ 1030(a)(1)), financial records (§ 1030(a)(2)), and the use, destruction, modification or disclosure of information on government computers (§ 1030(a)(3)). *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, ch. 21, sec. 2102, Pub. L. No. 98-473, 98 Stat.1837. Upon passage of the 1984 CFAA, legislators were already anticipating legislation that would further expand the federal government's role in policing computer crime. *See* H.R Rep. No. 99-612, at 3–4. As a House Judiciary Committee report explains, House leaders had agreed to delete provisions in the 1984 bill addressing "private sector computers and felony theft," in exchange for the Senate Judiciary Committee's commitment to address those issues in later legislation. *Id.* at 4.

Accordingly, the 1986 Amendments were intended to "readdress[] these gaps," and thus represented a more expansive scope of Congressional action. *Id.* To achieve this, the 1986 Amendments added three new offenses to the CFAA. *Id.* at 11. Among these three offenses was the provision under which Nosal was charged,

Section 1030(a)(4). *See id.*; (R. at 14). A Senate Judiciary Committee report on the 1986 Amendments similarly reflects Congress' intent to *expand* rather than contract the CFAA's prior scope. *See* S. Rep. No. 99-432, at 3 (1986) (referring to the 1986 Amendments as "[l]egislation to *expand* and to amend 18 U.S.C. § 1030") (emphasis added).

Given Congress' overall intent in enacting the 1986 Amendments, it seems unlikely that legislators would have made a concurrent revision to so drastically *narrow* the CFAA's application: namely, by excluding situations where someone is authorized to access information, but only for certain purposes. The Ninth Circuit opinion points to no evidence in the legislative history signaling such intent.

2. Congress' Intent Merely to Clarify the Prior 1984 Language Was Evidenced by the House and Senate Judiciary Committees' Clear Explanation of the 1986 Amendments.

If the *overall* legislative history of the 1986 Amendments is problematic for the Ninth Circuit's position, Congress' *specific* explanations of the phrase "exceeds authorized access" prove fatal.

This is because in addition to creating the three new offenses under the CFAA, the 1986 Amendments also made a few changes intended to "clarify[] the existing law." H.R Rep. No. 99-612, at 4. Committee reports from both chambers illustrate that the incorporation of the phrase "exceeds authorized access" was among these clarifications. *See id.*; S. Rep. No. 99-432, at 9. Accordingly, the legislative history rebuts any presumption that adding the phrase "exceeds

authorized access" was intended as a substantive change meant to narrow the scope of the unauthorized "purposes" language in the 1984 CFAA.

This is demonstrated first in the House Judiciary Committee's section-by-section description of the changes made by the 1986 Amendments. *See* H.R. Rep. No. 99-612, at 11. The Committee's report notes that:

> *Section (2)(c)* deletes the phrase 'or having accessed a computer with authorization, uses the opportunity such access provides *for purposes to which such authorization does not extend*,' and substitutes 'or exceeds authorized access' in 18 U.S.C. 1030 (a)(1) (a)2. . . . *The purpose of this change is merely to clarify the language in existing law.*

Id. (emphasis added). Such unequivocal statements in Congressional committee reports are considered controlling in interpreting legislative intent. *See C.I.R. v. Bilder*, 369 U.S. 499, 503 (1962) (describing "authoritative pronouncements" in committee reports as "controlling"). Here, the House Judiciary Committee could scarcely have attested to Congress' intent more clearly.

Nor do statements emerging from the other chamber add ambiguity in any way. Like its House counterpart, the Senate Judiciary Committee's report on the 1986 Amendments explains the "exceeds authorized access" language in its section-by-section analysis. *See* S. Rep. NO. 99-432, at 9. As the report explains:

> Section 2(c) substitutes the phrase "exceeds authorized access" for the more cumbersome phrase in present 18 U.S.C. 1030 (a)(1) and (a)(2), "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend". The Committee intends this change to simplify the language in 18 U.S.C. 1030(a) (1) and (2), and the phrase "exceeds authorized access" is defined separately in Section (2)(g) of the bill.

Id. The Committee's explicit mention of the "cumbersome phrase" in the 1984 enactment illuminates not a focus on changing the substance of the CFAA, but merely its linguistic elegance. *See id.* Nor does an intention to "simplify the *language*" suggest an effort to drastically narrow a statute's substantive scope. *See id.* Had Congress intended not merely to clarify but instead to *change* the meaning of the 1984 language addressing unauthorized "purposes," it is doubtful that legislators would have been so coy about such a seemingly significant objective.

3. The Oft-Cited Statements from Senators Mathias and Leahy Are Irrelevant to Interpreting the Phrase "Exceeds Authorized Access."

Despite the seeming clarity of the statements above, a handful of courts have myopically focused their legislative history analysis on the "Additional Views of Messrs. Mathias and Leahy" ("the Mathias/Leahy Statement") included in the 1986 Senate Judiciary Committee report. *See, e.g.*, (R. at 19 n.5); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005); *United States v. Aleynikov*, 737 F. Supp. 2d 173, 192 n.23 (S.D.N.Y. 2010). The Ninth Circuit, for instance, cited a painstakingly edited excerpt of the Mathias/Leahy Statement, *purportedly* explaining how replacing the prior language with "exceeding authorized access" was intended to "remove[ ] from the sweep of the statute one of the murkier grounds of liability, under which a[n] . . . employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances." (*See* R. at 19 n.5.)

In relying on this passage, courts adopting the narrow view of "exceeds authorized access" have neglected the critical context in which this oft-quoted portion is situated. This has distorted the Senators' statement in three critical ways.

First, the Mathias/Leahy Statement—including the portion quoted above—was devoted to a very specific issue that had concerned the two Senators since the adoption of the 1984 CFAA: the potential chilling effect of Section 1030(a)(3) on government employees' willingness to comply with public records requests under the Freedom of Information Act. *See* S. Rep. No. 99-432, at 20–22. This concern arose because Section 1030(a)(3) made it a crime to "'knowingly use . . . or disclose information in [any] computer . . . operated for or on behalf of the Government of the United States,' when the defendant gains access to the computer without authorization or his conduct exceeds the scope of his authorization." *Id.* at 20 (quoting the former version of Section 1030(a)(3)). The Senators worried that a government employee might be reticent to comply with a public records request absent "assurance of the precise contours of his authorization." *Id.* Senators Mathias and Leahy said nothing, however, about the consequences of forbidding access for unauthorized purposes *outside* the context of government computers, *see id.* at 20–22, thus limiting their statement's relevance to the CFAA offenses involving *private* sector computers, such as Section 1030(a)(2) and (a)(4).

What's more, the Senators' concern about discouraging transparency in government agencies had nothing to do with the distinction between restrictions on

access and restrictions on *use*. Rather, the Senators explained that "the existence" of a government employee's authority to access a particular database "is not always free from doubt." *Id.* at 20. Using the phrase "exceeds authorized access" would therefore do nothing to remedy this problem.

For this reason, Section 1030(a)(3) was revised to "eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend.'" *Id.* at 21 (quoting the 1984 CFAA). Significantly, Congress did *not* replace this language with the purportedly narrower phrase, "exceeds authorized access." *See id.* at 7. Rather, the Committee explicitly "*declined* to criminalize acts in which the offending employee merely 'exceeds authorized access,'" for purposes of a Section 1030(a)(3) offense. *Id.*

Despite the Ninth Circuit's somewhat incredible insinuation to the contrary, Senator Mathias and Leahy's views on deleting the unauthorized "purposes" language from Section 1030(a)(3) are thus entirely irrelevant to interpreting the phrase "exceeds unauthorized access"—which Congress wrote only into other, separate subdivisions: (a)(1), (a)(2) and (a)(4). *See* Computer Fraud and Abuse Act of 1986, PL 99–474 § 2(c), (d)(4), 100 Stat 1213. Courts' reliance on a misleadingly excerpted portion of the Mathias/Leahy Statement has unfortunately obscured Congress' otherwise clear explanation of the 1986 Amendments.

B. The Government's Interpretation of "Exceeds Authorized Access" Better Comports With Congress' Goals in Enacting the CFAA.

Like the legislative evolution of the specific language at issue, Congress' broader policy objectives similarly support the government's reading of "exceeds authorized access." A Court may take into account legislators' policy goals in interpreting statutory language. *See* 73 *Am. Jur. 2d Statutes* § 68 (" . . . the policy which induced its enactment, or which was designed to be promoted thereby, is a proper subject for consideration . . . "). Though some courts have painted Congress' objectives in passing the CFAA as narrowly addressing "hacking," *see, e.g.*, (R. at 18); *United States v. Aleynikov*, 737 F. Supp. 2d 173, 192 (S.D.N.Y. 2010), the CFAA's legislative history reveals Congress' broader goal: to prevent the kinds of fraud and theft to which computers rendered people increasingly vulnerable.

This broader objective is evident in committee reports on both the initial 1984 CFAA and the subsequent 1986 Amendments. For instance, the House Judiciary Committee report on the 1984 CFAA outlined the substantial financial losses resulting from "credit and computer fraud," an emerging type of "white collar crime" that "silently robs" millions in taxpayer dollars. H.R. Rep. No. 98-894, at 4–5 (1984). As experts explained to the Judiciary Committee, the ubiquity of computers required a shift in focus from "'tangible property' and credit and debit instruments to 'information' and 'access to information.'" *Id.* at 4. Congress' efforts to prevent computer crime, accordingly, were aimed not merely at the act of trespass itself, but rather at the substantial *losses* that result and the underlying threat to important

"information." *See id.* In fact, it was only after describing the problem for several pages that the Committee noted that "*[c]ompounding* this is the advent of the activities of so-called 'hackers' . . . ." *Id.* at 10.

The legislative history of the 1986 Amendments reflects a similar intention to address a broader range of computer crime than "hacking" alone. As a House Judiciary Committee Report explains, legislation was needed in the area of computer crime not only due to computers' growing ubiquity, but also because the *property* at risk did "not fit well into traditional categories of property targeted by abuse or theft," in part because "the information stolen almost always remains in the possession of the original owner." H.R. Rep. No. 99-612, at 5. Here again, the Committee noted that the increasing number of "so called hackers" presented "*[o]ne* somewhat unique aspect of computer crime." *Id.* (emphasis added). While high-profile hacking incidents indisputably "dramatize[d] the need for Federal computer crime protection," *id.* at 6, these reports on the whole suggest that it was the broader computer-related threat to *property*, and not the mere act of hacking alone, that animated Congressional action.

Finally, one of the problems mentioned expressly in the CFAA's legislative history could *only* be addressed by employing the broader explanation of "exceeds authorized access." In detailing the country's increasing financial fraud crisis, a House Judiciary Committee report on the 1984 CFAA described "[d]ishonest merchants and/or their employees" who "obtain valid numbers taken from authorized sales at the merchant's place of business, transcribe those numbers onto

blank sales slips, and either submit them to their banks for payment or sell them to other colluding merchants." H.R. Rep. No. 98-894, at 7. Because such merchants' employees would presumably be authorized to access customer credit card numbers for valid business purposes, the CFAA would only reach this kind of abuse under the government's broader interpretation of "exceeds authorized access."

The committee reports described above illustrate Congress' broader goal not only to combat "hacking" but also to better protect commercial and individual property from computer-facilitated theft and misuse. *See also* 132 Cong. Rec. H3275 (daily ed. June 3, 1986) (statement of Rep. Nelson) ("Computer-*assisted* crime is the way we should refer to this particular type of wrong-doing.") (emphasis added). Read on the whole, the legislative history therefore counters the Ninth Circuit's conclusion that the CFAA was aimed narrowly at addressing "access" rather than "misappropriation." (*See* R. at 27 (citing *Shamrock Foods Co. v. Gast,* 535 F.Supp.2d 962, 965 (D.Ariz. 2008).)

III. THE JUDICIAL DECISIONS ADOPTING THE BROADER INTERPRETATION OF "EXCEEDS AUTHORIZED ACCESS" OFFER THE MORE PERSUASIVE APPROACH.

As recognized by the Ninth Circuit's decision below, the federal circuits are split on the proper interpretation of "exceeds authorized access." (R. at 27.) The Fourth and Ninth Circuit Courts of Appeals, as well as district courts in the Second Circuit, have adopted the narrower construction. *See* (R. at 27); *WEC Carolina Energy Solutions LLC v. Miller,* 687 F.3d 199, 201 (4th Cir. 2012); *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010).

The First, Fifth, Seventh, and Eleventh Circuit Courts of Appeals have adopted the government's interpretation. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001); *United States v. John*, 597 F.3d 263, 273 (5th Cir. 2010); *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010).

Academics have identified three approaches courts have employed in defining the contours of CFAA liability: "code," "contracts," and "agency." *See, e.g.*, Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 Wm. & Mary L. Rev. 1369, 1372 (2011). Employing a code-based approach, courts adopting the narrow construction of "exceeds authorized access" have looked only to whether the defendant bypassed some sort of technological barrier (i.e. "coding") in order to "exceed authorized access." *See id.* at 1380. Yet as discussed above, the statute's plain language and legislative history are at odds with such a narrow reading of the statute.

Courts adopting the broader meaning of "exceeds authorized access," in contrast, have done so under either a contracts- or an agency-based approach. *Id.* at 1372. These CFAA cases demonstrate how both of these latter approaches provide readily administrable frameworks for determining what constitutes an unauthorized purpose.

Finally, the CFAA caselaw supports the government's interpretation of "exceeds authorized access" in another key regard: by demonstrating the

importance of the broader interpretation to addressing serious computer-related threats to economic and personal security. The Ninth Circuit's rule, in contrast, would exculpate a range of such activities from the scope of CFAA liability without any regard for such conduct's harm-causing potential.

A. The Government's Interpretation of "Exceeds Authorized Access" Can be Effectively Applied Through Either a Contracts- or an Agency-Based Approach.

1. The Contracts-Based Approach Provides an Administrable Means of Distinguishing Authorized from Unauthorized Purposes.

Under the "contracts"-based approach, courts look to employment contracts, agreements, or posted information to determine whether someone exceeded his or her scope of authorized access. Urban, *Causing Damage Without Authorization*, *supra*, at 1378–79. This approach has a number of merits. First, it provides for an administrable standard by looking to express indications that access for certain purposes was in fact unauthorized. Second, requiring this kind of evidence precludes CFAA liability unless the defendant was somehow put on notice about the boundaries of his or her authorization. Finally, this approach is consistent with Congress' goal in enacting the CFAA to prevent not only "hacking" but also equally dangerous threats to commercial and personal information.

As early as 2001, the First Circuit applied this approach in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). There, the court found that the defendant likely "exceeded authorized access" by using his knowledge about his former employer's product codes to aid a competing tour group company.

Id. at 581–82. Although these product codes were publicly displayed on the former employer's website, they were meaningless to the general public, and the defendant used his special understanding of these codes to build a "scraper program" that could efficiently scan his former employer's website for pricing information. *Id.* at 579. Because the defendant had signed a confidentiality agreement barring disclosure of anything "which might reasonably be construed to be contrary to the interests of EF," the court held that using "propriety information and know-how" to build the scraper likely exceeded the defendant's authorized access. *Id.* at 583.

Similarly, the Eleventh Circuit held in *United States v. Rodriguez* that someone can "exceed authorized access" through conduct that violates an explicit admonition to use information solely for business purposes. 628 F.3d 1258, 1260 (11th Cir. 2010). That case involved a Social Security Administration (SSA) employee who used his access to the SSA's confidential database to obtain the personal information of a former spouse, as well as the home addresses and birthdates of women he met at a church group. *Id.* at 1260–62. The SSA had an express policy restricting use of the database to "business reason[s]"—a policy expressed through employee trainings, written acknowledgements, and a daily banner on the agency's computer screens. *Id.* at 1260. Accordingly, the First Circuit held that the defendant exceeded his authorized access by using the database for patently non-business purposes. *Id.* at 1263.

As illustrated by the cases applying the contracts-based approach, the government's interpretation of "exceeds authorized access" proves both fair and

administrable in practice. In neither *EF Cultural Travel* nor *Rodriguez* could the defendant claim a lack of notice regarding the boundaries of his authorization to access information, having voluntarily signed a confidentiality agreement, and received written acknowledgements of agency policy, respectively. *See* 274 F.3d at 583; 628 F.3d at 1260. Furthermore, to say that either of these defendants obtained information in a way that they were "entitled so" to do stretches common sense at the seams. *See Rodriguez*, 628 F.3d at 1273 (noting that "the plain language of the [Computer Fraud and Abuse] Act forecloses any argument that Rodriguez did not exceed his authorized access.").

Like the confidentiality agreement in *EF Cultural Travel* or the "business purpose" acknowledgements in *Rodriguez*, the notice on the entry page of Korn/Ferry's database gave the defendant here ample notice that he was not "entitled" to obtain Korn/Ferry's information for purposes of starting his own competing firm. (*See* R. at 13.) Accordingly, this warning left no room for doubt as to whether Nosal's co-conspirators, in proceeding to access the database for patently *non*-business purposes, exceeded their authorized access.

2. The Agency-Based Approach Provides an Alternative Means of Applying the Government's Interpretation of "Exceeds Authorized Access."

The agency approach applies principles of agency law to the employer-employee relationship. Under this theory, an employee who breaches his or her duty of loyalty to an employer extinguishes the agency relationship, along with any authorization the employee might have had to obtain or alter information as an

"agent" of the employer. Urban, *Causing Damage Without Authorization*, *supra*, at 1376–77. This approach may not be quite as easily administrable as the contracts approach in that it requires courts to determine whether the agency relationship had ceased when the information at issue was obtained or altered. *See* Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 U. Pitt. J. Tech. L. & Pol'y 1, 15. The agency approach, however, is strongly supported by the statute's plain language, and offers a workable means of applying the government's interpretation of "exceeds authorized access." *See also* Urban, *Causing Damage Without Authorization*, *supra*, at 1394 (noting that the agency approach "allows for significant flexibility in dealing with advances in computer technology").

In *International Airport Centers, L.L.C. v. Citrin*, Judge Posner applied this theory to an employee who, in breach of his employment contract, decided to go into business for himself and proceeded to delete data on an employer-owned laptop. 440 F.3d 418, 421–22 (7th Cir. 2006). The Seventh Circuit concluded that as soon as the employee breached his duty of loyalty to the employer, this terminated any authorization he might previously have had to access the laptop, since the defendant was no longer the employer's "agent." *Id.* Similarly in *NCMIC Financial Corp. v. Artino,* one district court applied the agency theory in concluding that a lease financing company's Vice President exceeded authorized access in using the company's customer database to divert potential business to a competitor. 638 F. Supp. 2d 1042, 1061 (S.D. Iowa 2009).

This approach is forcefully supported by the CFAA's plain language: specifically, by the phrase "*entitled* so to obtain or alter." *See* 18 U.S.C. § 1030(e)(6) (emphasis added). One of the meanings of "entitle" is to "grant a legal right." *Entitle Definition*, *Black's Law Dictionary*, *supra*. Under agency law, cessation of an agency relationship terminates any legal rights that inhered to that agency relationship—including access to the employer's computers. *See Citrin*, 440 F.3d at 420. Accordingly, it can scarcely be said that someone secretly working on a competitor's behalf retains whatever "authorized access" he or she had prior to this breach of loyalty.

As with the contracts-based approach, the agency theory can be easily applied to the facts of this case. Like the employee in *Citrin* who decided to start his own company, Nosal's co-conspirators breached their duty of loyalty to Korn/Ferry when they decided to channel Nosal confidential information for the purpose of forming a new firm. *See* 440 F.3d at 421–22; (R. at 13). Accordingly, Nosal's co-conspirators' agency relationship with Korn/Ferry had ceased, and they lacked authorization to obtain or alter any information from their employer's confidential database. Their conduct thus "exceeded authorized access" under Section 1030(a)(4).

B. The Ninth Circuit's Approach Focuses Myopically on "Hacking" at the Expense of the CFAA's Broader Objective to Prevent Computer-Related Threats to Property.

The Ninth Circuit's approach to separating criminal from non-criminal conduct under the CFAA is entirely divorced from the actual *harm* such activities are likely to engender. The narrow construction would exculpate the destructive use

of computerized information simply because the perpetrator was entitled to access that information for legitimate, non-destructive ends.

1. An Individual Should Not Evade Culpability Under the CFAA Based Merely on the Timing of the Destructive Conduct.

The Ninth Circuit's narrow construction would allow individuals in the employment context to evade CFAA liability based simply on the timing of computer-facilitated theft. This is because, in practice, CFAA liability would often depend on whether someone stole company information *before* or *after* leaving an employer.

Two pre-CFAA criminal cases help illustrate this point. *See* H.R. Rep. No. 98-894, at 6 (1984) (citing *United States v. Seidlitz*, 589 F.2d 152 (4th Cir. 1978) and *United States v. Langevin*, an unreported criminal case). The first, *United States v. Seidlitz*, involved a computer security specialist who stole confidential software by accessing his former employer's computer system through a phone line. 589 F.2d at 154. The second case, *Langevin*, involved a former Federal Reserve Board employee who continued to access the Federal Reserve's "money supply file" after leaving the agency, acquiring information that would have been "extremely helpful" to his new client. H.R. Rep. No. 98-894, at 6. The House Judiciary Committee described these two cases as illustrating the "dilemma facing Federal prosecutors," and demonstrating the need for "specific Federal legislation in the area of computer crime." *Id.*

Under the Ninth Circuit's narrowing interpretation of "exceeds authorized access," the defendants in *Seidlitz* and *Langevin* would have evaded liability under the CFAA merely by obtaining the information at issue *before* parting ways with their respective employers. Had the *Seidlitz* defendant still been authorized to access his employer's confidential software for company business, for instance, the Ninth Circuit rule would have insulated him from the CFAA's criminal penalties—even if he downloaded the software for patently illegitimate ends, such as aiding a future, competing employer.

The arbitrary line-drawing that results from the narrow construction can be stated as such: downloading proprietary information for your future clients five minutes *before* quitting your job? Not covered by the CFAA. Obtaining the same information through a virtual log-in five minutes *after* departing your company? A federal crime.

Besides creating a perverse incentive to complete any self-serving thefts of computerized information *before* parting ways with an employer, the Ninth's Circuit's rule precludes criminal liability in the area where the CFAA's deterrent effect is arguably of the greatest importance. After all, individuals who do possess authorization to access certain information arguably present the gravest risk to a business or agency. The problem presented by so-called "inside hackers," (R. at 18), is at least one that technology can address. *See, e.g.*, S. Rep. No. 99-432, at 3 (noting that according to an American Bar Association survey, the "most effective means" of preventing computer crime is self-protection). Preventing employees from accessing

information for unauthorized *purposes*, however, is an issue beyond the reach of firewalls and password protection. It is arguably in this arena that criminal sanctions are of even greater importance.

2. The CFAA Caselaw Illustrates the Importance of the Broader Interpretation to Addressing Serious Threats to Financial and Personal Security.

While "hacking" is certainly among the tools from which computer-assisted criminals may choose, it is hardly the *only* source of computer-related fraud, theft and abuse of information. As the caselaw demonstrates, the narrow construction of "exceeds authorized access" would insulate a dangerous range of conduct—with serious ramifications for financial and personal security—from the reach of CFAA liability.

One Eighth Circuit case, for instance, involved an employee working for a Department of Education contractor, Vangent Corporation. *See United States v. Teague*, 646 F.3d 1119, 1121 (8th Cir. 2011). As a Vangent employee, the defendant in *Teague* had "privileged access" to the National Student Loan Data System (NSLDS), which she allegedly used to look up President Obama's student loan records. *Id.* at 1121.[2] The court upheld the defendant's conviction under Section 1030(a)(2) for "exceeding [her] authorized access." Under the Ninth Circuit's narrow construction, however, the CFAA would *not* have barred Teague from obtaining the President's financial information, even for some patently personal or political

[2] Teague conceded that her log-in and password were used to access President Obama's records, but contended that someone else must have used them. The court did not reach the question of statutory interpretation at issue in this case.

purpose, since she was authorized to access the NSLDS in furtherance of her job duties. *See id.*

A narrow reading of "exceeds authorized access" would present a similar conundrum in a case like *United States v. Rodriguez*, where an SSA employee used his access to the Social Security database to obtain acquaintances' personal information. 628 F.3d at 1260. Since the defendant was fully authorized to obtain such information for *business* purposes, the CFAA would not reach his abuse of such access—no matter the consequences to innocent citizens' sense of security. *Id.* at 1263.

Finally, *United States v. John* underscores the importance of the broader reading in the context of financial fraud. *See* 597 F.3d 263 (5th Cir. 2010). There, a Citigroup account manager obtained customer information to give to her half-brother, who then used the account numbers to incur fraudulent charges. *Id.* at 269. Again, the CFAA would be silent as to such conduct under the narrow construction of "exceeds authorized access," since the defendant was authorized to access customers' account information by "virtue of her position." *Id.*

These cases implicate critical issues of personal and financial security—not the innocent workplace diversions or innocuous online dalliances that drew so much of the Ninth Circuit's focus. (*See* R. at 21–26.) They fall, moreover, well within the scope of the problems discussed in the CFAA's legislative history: substantial business losses, theft of financial account numbers, and incursions on individuals' private information. *See* S. Rep. No. 99-432, at 2–3 (1986). These destructive

consequences can all be achieved just as readily through misuse of authorized access as through "hacking." It is only logical that the significant deterrent effect of federal criminal liability attach to either *modus operandi*.

IV. THE RULE OF LENITY DOES NOT REQUIRE THE COURT TO VACATE CONGRESS' INTENT TO CRIMINALIZE THE USE OF COMPUTER ACCESS FOR UNAUTHORIZED PURPOSES.

A. The CFAA's Plain Language, Legislative History, and Purposes Sufficiently Foreclose Ambiguity so as to Render the Rule of Lenity Inapt as an Interpretive Aid.

In its decision below, the Ninth Circuit cited the rule of lenity as favoring the narrow construction of "exceeds authorized access," explaining that under this rule, any doubts about Congressional intent must be resolved in favor of "the interpretation least likely to impose penalties unintended by Congress." (R. at 29 (citing *United States v. Cabaccang*, 332 F.3d 622, 635 n.22 (9th Cir. 2003)).) This rule is based on the reasoning that because criminal punishment is serious and "usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity." (*Id.* (citing *United States v. Bass*, 404 U.S. 336, 348 (1971)).) Yet here, the legislature sufficiently defined the phrase "exceeds authorized access," and it was the Ninth Circuit that redefined the scope of criminal liability through its unnecessarily narrowing construction.

The rule of lenity "comes into operation at the end of the process of construing what Congress has expressed, not at the beginning as an overriding consideration of being lenient to wrongdoers." *Callanan v. United States*, 364 U.S. 587, 596 (1961). As this Court recently noted in *Barber v. Thomas*, the "rule of

lenity only applies if, after considering text, structure, history, and purpose, there remains a 'grievous ambiguity or uncertainty in the statute,' such that the Court must simply 'guess as to what Congress intended.'" 560 U.S. 474, 488 (2010) (citations omitted). Here, the phrase "exceeds authorize access" is not so grievously ambiguous to require such a blunt instrument of statutory construction.

Notably, this Court has declined to apply the rule of lenity even in cases where the indicia of legislative intent were far scarcer than in the case at bar. In *Kasten v. Saint-Gobain Performance Plastics Corp.*, this Court was asked to apply the rule of lenity in deciding whether lodging an oral complaint counted as "filing" a complaint for purposes of the "protected activities" provision of the Fair Labor Standards Act (FLSA). 131 S. Ct. 1325, 1336 (2011). "Filing" lacked a statutory definition, and finding the text alone inconclusive, the Court looked to functional considerations derived from the FLSA's purpose. *Id.* at 1333–34. The Court concluded that having "engag[ed] in traditional methods of statutory interpretation," it could not find the statute "sufficiently ambiguous to warrant application of the rule of lenity . . . ." *Id.* at 1336 (citations omitted). Similarly in *United States v. Hayes*, this Court concluded that the phrase "misdemeanor crime of domestic violence" was not sufficiently ambiguous to apply the rule of lenity, even though the language was "not a model of the careful drafter's art." 555 U.S. 415, 429 (2009).

These cases illustrate the Court's understandable reluctance to apply the rule of lenity if "traditional methods of statutory interpretation" can resolve the

ambiguity. *See Saint-Gobain Performance Plastics*, 131 S. Ct. at 1336. These methods include not only analysis of the statute's plain language and legislative history but also its purpose, functional considerations, and context. *See id.* at 1333; *Hayes*, 555 U.S. at 417. Here, the Court has the benefit of not only a statutory definition, *see* 18 U.S.C. § 1030(e)(6), but also clear explanations of the phrase "exceeds authorized access" in the CFAA's legislative history. Given, finally, the CFAA's stated policy objectives and the functional consequences of construing "exceeds authorized access" narrowly, it is hardly necessary for the Court here to simply "guess as to what Congress intended." *See Barber*, 560 U.S. at 488.

B. Adopting the Government's Interpretation of "Exceeds Authorized Access" Would Not Have the Purported Impact on "Day-to-Day" Activities that the Ninth Circuit Fears.

Rather than converting the rule of lenity into an "overriding consideration," *see Callanan,* 364 U.S. at 596, a more advisable approach would be to look to the constitutional due process principle underlying the rule: namely, that "no individual be forced to speculate, at peril of indictment, whether his or her conduct is prohibited." *See Dunn v. United States*, 442 U.S. 100, 112 (1979). This principle has been expressed in some CFAA cases as an admonition against interpreting the statute in a way that would render it "void for vagueness" or create "absurd results." *See United States v. Drew*, 259 F.R.D. 449, 451 (C.D. Cal. 2009); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000). Whatever the formulation of this inquiry, the government's interpretation of "exceeds authorized access" survives.

In its opinion below, the Ninth Circuit expressed concern that the government's interpretation of "exceeds authorized access" would criminalize "a broad range of day-to-day activity." (R. at 26 (citing *United States v. Kozminski*, 487 U.S. 931, 949 (1988)).) The examples offered in the Ninth Circuit's "parade of horribles," (*see* R. at 36), can be sorted into two categories: workplace diversions such as using an employer's computer to play sudoku or check Facebook, and inadvertent violations of "terms of use" agreements for services like Craigslist, dating websites, and Internet service providers. (*See* R. at 22–25.) Contrary to the Ninth Circuit's concerns, the broader construction of "exceeds authorized access" would not convert these "day-to-day" activities into federal crimes. (*See* R. at 26.)

This is because—even under the government's interpretation—the statutory definition of "exceeds authorized access" requires more than mere use of a computer for unauthorized purposes. "Exceed[ing] authorized access" is instead defined as accessing a computer "*with authorization*" and then "obtain[ing] or alter[ing] information *in the computer* that the accesser is not entitled so to obtain or alter." § 1030(e)(6). Two elements are noteworthy in this context. First, someone must actually obtain or alter information. Second, and most significantly, that information must be "in *the* computer" that the person initially accessed "with authorization." *See id.* (emphasis added).

With respect to the first element, it is true that "obtaining information" can include the "mere observation" of data. S. Rep. No. 99-432, at 6. Thus playing sudoku, checking a Facebook page, or browsing Craigslist could arguably be

characterized as "obtain[ing] information." The second element, however, prevents innocuous workplace diversions and innocent violations of terms-of-use agreements from being swept up in the CFAA's net.

A close reading of Section 1030(e)(6) is instructive. To "exceed authorized access," someone must "obtain or alter information" in the same computer that the person first accessed *with* authorization. *Id.* To violate the CFAA by "obtaining information" from Facebook while at work, for example, someone would have to first access *Facebook*'s "computer"—not merely her *employer*'s computer—"with authorization." The question, of course, is whether logging onto a Facebook page constitutes authorized access to Facebook's "computer."

Under the CFAA, a "computer" is a " . . . high speed data processing device . . . and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." § 1030(e)(1). Accordingly, accessing a "computer" entails more than merely interacting with a website. Instead, it would require accessing the underlying information that makes that interface work—for example, the user passwords or program code stored within a "processing device" or "data storage facility." *See id.*

While a Facebook user is obviously authorized to access his or her *account*, this is not synonymous—based on the statutory definition—with authorized access to Facebook's "computer." This means that, even under the government's interpretation, conduct on a work computer implicates the CFAA only when it involves obtaining or altering information on the *employer*'s "data processing

device" or related data storage/communications facility. Mere *use* of a workplace computer for unauthorized purposes would not be implicated.

Similar logic applies to inadvertent violations of a website's "terms of use." To borrow one of the Ninth Circuit's examples, posting a prohibited item for sale on Craigslist in violation of their terms of use might fairly be characterized as obtaining or altering information in *a* computer. Here again, however, to "exceed authorized access" one must "access a computer *with authorization*" and proceed to "obtain or alter information in *the* computer." The average Craigslist user would not be able to "access [Craigslist's] computer with authorization." *See* § 1030(e)(1) (defining "computer" as a "data processing device," or associated "data storage facility" or "communications facility").

Based on the plain language of Section 1030(e)(6), even the government's broader definition of "exceeds authorized access" would not impact "playing sudoku, checking email, fibbing on dating sites, or any of the other activities that the [Ninth Circuit] majority rightly values." (*See* R. at 31.) Accordingly, neither the rule of lenity nor due process concerns require this Court to vacate Congress' intent to include restrictions on use within the scope of the CFAA.

CONCLUSION

The statute's plain language, legislative history, and purposes demonstrate Congress' intent to address not only access restrictions but also use restrictions through the phrase "exceeds authorized access." Having accessed Korn/Ferry's database for patently unauthorized purposes, Nosal's co-conspirators' conduct falls

squarely within the definition of "exceeds authorized access." Petitioner thus asks this Court to reverse the decision of the Ninth Circuit Court of Appeals.

Dated: February 24, 2014

Respectfully submitted,

JESSICA L. DIAZ
Counsel for Petitioner