14-4396

To Be Argued By:
JUSTIN ANDERSON
RANDALL W. JACKSON

United States Court of Appeals

FOR THE SECOND CIRCUIT
Docket No. 14-4396

UNITED STATES OF AMERICA,

Appellee,

—v.—

GILBERTO VALLE, also known as Sealed Defendant 1,

Defendant-Appellant,

MICHAEL VANHISE, also known as Sealed Defendant 1,
ROBERT CHRISTOPHER ASCH, also known as Chris,
RICHARD MELTZ, also known as Rick,

Defendants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF FOR THE UNITED STATES OF AMERICA

PREET BHARARA,
United States Attorney for the Southern District of New York,
Attorney for the United States of America.

RANDALL W. JACKSON,
HADASSA WAXMAN,
BROOKE CUCINELLA,
JUSTIN ANDERSON,
Assistant United States Attorneys,
Of Counsel.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 14-4396

UNITED STATES OF AMERICA,

Appellee,

—v.—

GILBERTO VALLE, also known as Sealed Defendant 1,

Defendant-Appellant,

MICHAEL VANHISE, also known as Sealed Defendant 1, ROBERT CHRISTOPHER ASCH, also known as Chris, RICHARD MELTZ, also known as Rick,

Defendants.

BRIEF FOR THE UNITED STATES OF AMERICA

Preliminary Statement

Gilberto Valle appeals from a judgment of conviction entered on November 14, 2014, in the United States District Court for the Southern District of New York, following a two-week jury trial before the Honorable Paul G. Gardephe, United States District Judge.

Indictment 12 Cr. 847 (PGG) (the "Indictment") was filed on November 15, 2012, in two counts. Count One charged Valle with kidnapping conspiracy, in violation of Title 18, United States Code, Section 1201(c). Count Two charged Valle with the unauthorized access of a restricted federal database, in violation of Title 18, United States Code, Section 1030(a)(2)(B).

Valle's trial commenced on February 25, 2013, and ended on March 12, 2013, when the jury found him guilty of both counts of the Indictment. Valle moved to set aside the jury's verdict. On June 30, 2014, Judge Gardephe granted that motion with respect to Count One but denied it with respect to Count Two.

On November 12, 2014, Judge Gardephe sentenced Valle principally to time served, followed by one year of supervised release.

Valle is currently serving his term of supervised release.

Statement of Facts

A. The Evidence at Trial

Between 2006 and 2012, Valle worked as an officer with the New York City Police Department (the "NYPD"). (Tr. 156).[1] In the final 10 months of his

---

[1] "Tr." refers to the trial transcript; "GX" refers to a Government exhibit admitted at trial; "Br." refers to Valle's brief on appeal; "A." refers to the appendix filed with Valle's brief; and "Amici Br." refers to the brief filed by *amici curiae*.

tenure, Valle plotted with three men to kidnap and torture women. To prepare for these kidnappings, Valle (i) confirmed where his targets lived and worked, contacting them by mail, conducting physical surveillance, and arranging a pretextual meeting; (ii) researched the formula for home-made chloroform, a well-known incapacitating agent, and sent that formula to an accomplice; (iii) sought out information about restraining victims and read news accounts describing the investigation and capture of kidnappers; and (iv) most egregiously, illegally accessed information in a police database about his intended targets.[2] (Tr. 418-652, 1030-34, 1197, 1239, 1275; GX 217, 229, 230, 401-43, 606, 1000-01).

Valle was able to access that database because, as a police officer, he was entrusted with credentials (a login and password) that allowed him to use NYPD computer systems. (Tr. 934, 970, 995). Through those systems, a police officer could learn confidential and restricted personal information about people of interest, including their dates of birth, social security numbers, driver's license information, and home addresses. (Tr. 570-72, 578-84, 940-43; GX 615, 616B, 616C, 616E, 617). That system also allowed Valle to view an individual's criminal record by accessing data

---

[2] The aspects of this plot not involving the illegal access of a police database are described in the Government's opening brief in Docket No. 14-2710, which was filed on November 12, 2014, and is scheduled to be argued in tandem with this appeal (Docket No. 14-4396) on May 12, 2015.

contained in the Federal Bureau of Investigation's National Crime Information Center ("NCIC") database. (Tr. 931, 937-38, 945; GX 610, 613, 614).

Valle's authority to use his credentials to review the data was restricted and limited. The NYPD instructed Valle repeatedly that the databases could be accessed only "in the course of a [police officer's] official duties and responsibilities" and that "[t]here were no exceptions to this policy." (Tr. 940-41; GX 612). Valle was further instructed that accessing the databases for "non-work" purposes was a violation of NYPD policy, state law, and that the penalties for doing so included "arrest, prosecution, termination of employment and fines up to $10,000." (Tr. 940-42, 950). Acknowledging that he understood these access restrictions, Valle signed several NYPD documents certifying his participation in training sessions on the use and misuse of the NYPD computer system. (GX 609-611).

In direct violation of his training, Valle accessed NYPD computer systems to gather information about women he targeted for kidnapping. (Tr. 571-84, 940-43; GX 615, 616B, 616C, 616E, 617). On May 31, 2012, without authorization, Valle accessed the database to obtain information on Maureen Hartigan, a woman Valle had known since he was in high school. (GX 616C). Valle entered Hartigan's name into the NYPD computer system, which in turn queried a number of local, state, and national databases for personal information about her, including any avail-

able criminal records on NCIC.[3] (Tr. 582-84; GX 616E).

The parties did not dispute that Valle lacked a legitimate law enforcement purpose for using the database to access information about Hartigan. *United States* v. *Valle*, 301 F.R.D. 53, 110 (S.D.N.Y. 2014) ("It is undisputed that Valle had no law enforcement purpose for querying Hartigan's name in the databases.").

B. The Jury Instructions and Verdict

Prior to deliberations, Judge Gardephe instructed the jury, without any objection from the defense, that "Valle could be convicted of Court Two only if the Government proved, *inter alia*, that he had 'accessed a computer with authorization, but that he exceeded his authority in accessing the information in question.'" *United States* v. *Valle*, 301 F.R.D. at 110 (quoting Tr. 1662).

After two days of deliberations, the jury found Valle guilty of kidnapping conspiracy and the unauthorized access of a federal database, as charged in the Indictment. (Tr. 1685-86).

C. The Post-Trial Proceedings

Valle moved to set aside the jury's verdict on both counts of the Indictment. Judge Gardephe granted

---

[3] This instance of unauthorized access provided the factual basis for Count Two of the Indictment.

the motion as to Count One and denied it as to Count Two. *See Valle*, 301 F.R.D. at 115.

On Count Two, Valle argued that his ability to use the NYPD computer system as part of his police duties immunized him from being "held criminally liable . . . for his improper query concerning Hartigan," even if that query went beyond the scope of his authorization. *Id.* at 111. Rejecting that construction of the statute, Judge Gardephe held that Valle "exceed[ed] [his] authorized access" to the NYPD computer system by "obtain[ing] information in the computer that he was not entitled to obtain." *Id.* (quoting 18 U.S.C. § 1030(e)(6)) (internal brackets and ellipses omitted). Because "Valle was barred by NYPD policy from performing a search regarding Hartigan's name unless he had a valid law enforcement purpose for doing so," Judge Gardephe concluded that "the plain language of the statute" outlawed Valle's conduct. *Id.*

D. The Sentence

On November 12, 2014, Judge Gardephe sentenced Valle to time served on Count Two, which was 20 months at that time, followed by one year of supervised release, and he imposed a mandatory $25 special assessment.[4] Among the conditions of Valle's supervised release is that he not contact any of the "women who were alleged targets of the conduct charged in Count One, or the woman who was the

---

[4] The statutory maximum term of imprisonment for a violation of Title 18, United States Code, Section 1030(a)(2)(B) is 12 months.

subject of the conduct that forms the basis for Count Two." (A. 256-57).

ARGUMENT

Valle's unauthorized access of the NCIC database to obtain information about Hartigan violated Title 18, United States Code, Section 1030(a)(2)(B), which protects information belonging to the United States from being obtained in an unauthorized manner. The undisputed trial evidence established that Valle (i) possessed credentials that enabled him to access the NCIC database, (ii) was authorized to do so only in the course of his duties as a police officer, and (iii) queried the database for information on Hartigan without a valid, law enforcement reason. When Valle used his credentials to access the database for non-police purposes, he "exceed[ed] his authorized access" to the database in violation of the statute. 18 U.S.C. § 1030(a)(2).

Valle resists this logic, arguing that because he was able to access the database for improper purposes, he was also authorized to so. That reading of the statute is unsustainable. The NYPD provided Valle with several law enforcement tools—credentials to access the NCIC database, handcuffs, a gun—but that does not mean Valle was authorized to use those tools however he saw fit, limited only by his abilities. To accept Valle's construction of the statute is to conflate ability with authorization. But there is nothing in the statutory text that recommends, much less compels, that unnatural result, particularly where it would run counter to the weight of precedent and

serve only to undermine the statute's purpose of protecting information belonging to the United States from unauthorized disclosure.

POINT I

The Statute Prohibits the Use of Validly Issued Credentials in an Unauthorized Manner

A. Applicable Law

1. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). Under the statute, individuals "exceed[ ] authorized access" when they "access a computer with authorization and . . . use such access to obtain or alter information in the computer that [they are] not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

Construing the CFAA, this Court has held that "authorization" has no "technical or ambiguous meaning" as used in the statute. *United States* v. *Morris*, 928 F.2d 504, 511 (2d Cir. 1991) (holding that "it was unnecessary to provide the jury with a definition of 'authorization'" because "the word is of common usage"). The term is readily understood to mean "[o]fficial permission to do something." Black's Law Dictionary (10th ed. 2014). That commonsense understanding applies equally to a user who "exceeds

authorized access" by "obtain[ing] . . . information" that she has no "entitle[ment]" or permission to obtain. 18 U.S.C. § 1030(e)(6). Official permission, not technical ability, is therefore the touchstone of whether information belonging to the U.S. has been accessed in violation of the CFAA.

Users who inadvertently access U.S. data do not run afoul of the statute because only intentional acts are prohibited. *See* 18 U.S.C. § 1030(a)(2). For an act to be intentional, it must have been done "deliberately and purposefully," as "the product of [an individual's] conscious objective rather than the product of mistake or accident." *United States* v. *Kelly*, 147 F.3d 172, 177 (2d Cir. 1998) (approving district court's instruction).

2. Principles of Statutory Construction

The interpretation of statutes "must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." *United States* v. *Albertini*, 472 U.S. 675, 680 (1985) (internal quotation marks omitted); *see also Smith* v. *United States*, 508 U.S. 223, 228 (1993) ("When a word is not defined by statute, we normally construe it in accord with its ordinary or natural meaning."). If the statute's language is "'plain, the sole function of the courts is to enforce it according to its terms.'" *United States* v. *Ron Pair Enters.*, 489 U.S. 235, 241 (1989) (quoting *Caminetti* v. *United States*, 242 U.S. 470, 485 (1917)); *see also Connecticut Nat'l Bank* v. *Germain*, 503 U.S. 249, 253-54 (1992) ("We have stated

time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there."). Where there is ambiguity, however, "a court may resort to the canons of statutory interpretation and to the statute's legislative history to resolve the ambiguity." *United States* v. *Awadallah*, 349 F.3d 42, 51 (2d Cir. 2003).

B. Discussion

1. The Statutory Text Prohibits Valle's Unauthorized Use of His Credentials

Valle's search of the NCIC database for information on Hartigan ran afoul of the unambiguous text of the CFAA. Under the undisputed facts of this case, Valle had permission to use his credentials to access NYPD computer systems only in furtherance of his duties as a police officer. (Br. 4). Equally beyond dispute is that Valle had no legitimate law enforcement reason for entering Hartigan's name into those systems and searching records maintained by the NCIC. (Br. 5). Nor is there any dispute that Valle's conduct was deliberate and purposeful and not the product of mistake or accident. (Br. 5). Those facts—none of which are contested on appeal—fall squarely within the CFAA's straightforward prohibition on "exceed[ing] authorized access" to a computer system in order to intentionally obtain information belonging to the United States without any "entitle[ment]" to that information. 18 U.S.C. § 1030(a)(2)(B), (e)(6). Because Valle had no permission to access the NCIC to learn anything about Hartigan, he "exceed[ed] [his] authorized access" in viola-

tion of the statute. That is why Judge Gardephe concluded that "Valle's conduct falls squarely within the plain language of Section 1030(a)(2)(B)." *Valle*, 301 F.R.D. at 111.

Disputing Judge Gardephe's conclusion, Valle invites this Court to ignore the straightforward command of CFAA's unambiguous text. First, he argues that liability under the statute cannot turn on the planned "purposes" an individual had in mind for restricted information, "or the use, if any, the person made of the information." (Br. 12). Insofar as Valle believes his conviction stems from his use or intended use of restricted information about Hartigan, he is mistaken. The statute is not concerned with what Valle did or intended to do with that restricted information, but whether he had permission to obtain it in the first place. As Judge Gardephe explained, "How Valle intended to use any information about Hartigan that he hoped to obtain from the NCIC database is . . . irrelevant" because all that "matter[ed] is that Valle was not authorized to access the . . . system to perform a query regarding Hartigan's name." *Valle*, 301 F.R.D. at 115. Valle's offense was thus premised on whether he was allowed to enter Hartigan's name into the NCIC database, not whether his intended uses of the information violated the CFAA.

Second, Valle contends that he was "authorized" to obtain Hartigan's information, notwithstanding the NYPD's prohibition on doing so, because he had the technical ability to "obtain exactly the sort of information about private citizens that Valle obtained about Hartigan." (Br. 14). Valle's position boils down

to the following proposition: Because he was able to misuse his credentials to obtain restricted information about Hartigan, Valle had permission to do so. That argument improperly conflates ability with authorization. The CFAA, however, does not speak in terms of ability; it speaks about authorization. And this Court has held that the CFAA's use of the word "authorization" has no "technical or ambiguous meaning." *United States* v. *Morris*, 928 F.2d at 511. It means permission, which is far different from ability. Valle might very well not have exceeded his ability to obtain restricted information when he accessed Hartigan's records, but he did exceed his authorization because he did not have official permission to obtain her records. Because the CFAA refers to "authorization," and not ability, Valle's argument is unmoored from the statutory text.

It is also unmoored from common sense. Valle's redefinition of "authorization" to mean "ability" would be shocking if applied to any of the other tools he possessed as a police officer. Were Valle to claim that he was authorized to restrain a member of the public on a lark because the NYPD had issued him handcuffs, no reasonable person, let alone a court, would take his claim seriously. It would be equally absurd for Valle to claim authorization to use his firearm in a reckless manner simply because the NYPD had given him the weapon in the first place. No less absurd is Valle's argument that, because the NYPD issued him computer credentials, he was authorized to misuse them to obtain information from the NYPD computer system that he had no permission to view.

There is nothing complicated or ambiguous about this principle: many forms of authorization have conditions that must be met before the authorization comes into effect. A police officer, for example, might have authorization to use deadly force, but only when the condition is met that his life or the safety of civilians is threatened. Valle's authorization to use the NYPD's computer systems to access NCIC data was conditioned on his having a law enforcement purpose. (Tr. 940-41; GX 612). When he chose to access NCIC, in spite of the fact that he had no law enforcement purpose, he violated the explicit prohibitions of his department and the plain language of the statute by "exceed[ing] his authorized access" to the NYPD computer system. There is a vital and obvious difference between ability and authorization. Valle's efforts to inject ambiguity into the statute by conflating the terms are misguided.

Third, Valle envisions a parade of horribles that will flow from this Court's enforcing the unambiguous text of the statute. He fears that a lonely heart will be prosecuted for "misrepresent[ing] his height and weight on a dating website" (Br. 15) or a law clerk might be brought to justice for shepardizing his "law school note" (Br. 16). There is good reason why Valle would prefer to ponder these outlandish hypothetical scenarios rather than the inhospitable facts of his own case: his actions violate the simple command of the CFAA prohibiting unauthorized access to information that belongs to the United States.

But even if they had some relevance here, Valle's hypothetical musings present no basis to ignore the

plain meaning of the relevant statutory text. Most starkly, they do not pertain to Valle's offense of conviction at all. Valle violated Section 1030(a)(2)(B) because he intentionally obtained information belonging to the United States without permission. Neither the user of the dating website, nor the scholarly law clerk appears to have obtained U.S. data through the hypothetical use of computers, which is reason enough to set aside Valle's hypotheticals. But even if other sections of the CFAA were at issue here, Valle's concerns about allegedly absurd results would be misplaced. While it is a well-established canon of statutory interpretation that "absurd results" should be avoided, *see SEC* v. *Rosenthal*, 650 F.3d 156, 162 (2d Cir. 2011), that canon comes into play only when the statutory text is ambiguous, *see Connecticut Nat'l Bank* v. *Germain*, 503 U.S. at 253-54. Where, as here, the text is unambiguous, courts must apply only the "cardinal canon"—namely, that "a legislature says in a statute what it means and means in a statute what it says there." *Connecticut Nat'l Bank*, 503 U.S. at 253-54.

Insofar as other provisions of the statute might sweep in conduct that seems less troubling than Valle's, those concerns must be raised in the first instance by individuals actually affected by the provision at issue. *See Farrell* v. *Burke*, 449 F.3d 470, 494 (2d Cir. 2006) ("Federal courts as a general rule allow litigants to assert only their own legal rights and interests, and not the legal rights and interests of third parties. This rule against third-party or *jus tertii* standing helps to avoid unnecessary pronouncements and serves to ensure that the issues before the court

are 'concrete and sharply presented.'" (citing *Secretary of Maryland* v. *Joseph H. Munson Co.*, 467 U.S. 947, 955 (1984) (citations omitted)). Valle cannot challenge his conviction under Section 1030(a)(2)(B) by pointing out that unnamed people might face misdemeanor prosecutions under a different provision of the CFAA in ways that might seem unfair in the abstract.[5] Those cases will present fact-specific questions not relevant here, including whether the applicable authorization was clearly defined and whether the abuse of computer access was intentional in the sense of being purposeful and deliberate.[6] Valle cannot avail himself of such hypothetical claims to ex-

---

[5] And breadth alone is insufficient because, as this Court has recognized, federal criminal statutes can often apply to a "broad range of conduct." *See United States* v. *Shellef*, 507 F.3d 82, 106 (2d Cir. 2007) (noting "the broad range of conduct covered by the federal fraud statutes").

[6] Congress's decision to adopt a heightened *mens rea* requirement demonstrates not only that it recognized the need to limit the scope of the statute, but also that it took steps it considered appropriate to impose such limitations. *See* S. Rep. No. 99-432, at 6 (1986) (describing the substitution of the word "intentionally" for "knowingly" in order to guard against concerns of sweeping too broadly: "[t]he substitution of an 'intentional' standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another").

cuse his conduct, which falls squarely within the prohibition.

Fourth, Valle contends that giving "authorization" its plain meaning of permission would "creat[e] surplusage" because his misconduct was both without authorization and in excess of his authorized access. (Br. 16). Again, the canons—this time the one against surplusage—are relevant only where there is ambiguity in the text, but they play no role when the text is unambiguous. *Connecticut Nat'l Bank*, 503 U.S. at 253-54. Here, there is neither ambiguity, nor surplusage.

The CFAA protects information belonging to the United States from those who lack any authorization to use a computer system as well as those who are authorized to use a computer system for a limited purpose. *See* 18 U.S.C. § 1030(a)(2) (reaching those who "access[ ] a computer without authorization or exceed[ ] authorized access"). The former category pertains to those who never received any permission whatsoever to access the computer, and the latter reaches those, like Valle, who were given limited or restricted access but did not abide by those restrictions or limitations. Far from surplusage, this language provides a complete answer to those like Valle who claim they could improperly access any information they wanted simply because they were issued the credentials to do so. It clarifies that abusing

the ability to access data is just as impermissible as having no ability to access the data in the first place.[7]

2. The History and Purpose of the Statute Support the Jury's Verdict

While the absence of textual ambiguity makes it unnecessary to examine the purpose and history of the CFAA, *see United States* v. *James*, 478 U.S. 597, 606 (1986), those factors provide further support for Valle's conviction. The CFAA was enacted in 1984 largely to deter and punish "so-called 'hackers' who have been able to access (trespass into) both private and public computer systems" belonging to the federal government and certain financial institutions. H.R. Rep. No. 98-894, at 10 (1984); *see also* S. Rep. No. 99-

---

[7] Amici claim to see surplusage in another provision of the CFAA: Section 1030(a)(4)'s prohibition of computer access with fraudulent intent. Under their theory, Section 1030(a)(4) would be "superfluous" if Section 1030(a)(2) punished those who "misuse their authorization in order to engage in fraudulent activity." (Amici Br. 14-15). That argument has no merit. While Section 1030(a)(2) requires that an individual "obtain[ ] information" from unauthorized access, Section 1030(a)(4) has no such requirement. It predicates liability instead on the much different requirement that the access "further[ ] the intended fraud" in some fashion. Accordingly, Section 1030(a)(4) would reach unauthorized access that furthers a fraud even if no information is obtained in violation of Section 1030(a)(2). There is no redundancy or surplusage.

432, at 3 (1986) (describing 1984 law as largely prohibiting "trespass into a Government computer"). In the years that followed, the CFAA was broadened to protect data stored on private computers not belonging to the federal government or financial institutions. *See P.C. Yonkers, Inc.* v. *Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005) (observing that "the scope of [the CFAA's] reach has been expanded over the last two decades").

From the outset, the CFAA reached both those who lack computer credentials and those who abuse them. Originally, the statute addressed the latter concept using the following language: "[whoever] having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend [violates the statute]." S. Rep. No. 99-432, at 9. Congress found that formulation "cumbersome" and therefore replaced that language with the concise term "exceeds authorized access," which remains in the current version of the statute. *Id.*

Valle believes that this change had a substantive impact on the CFAA by "eliminating civil and criminal liability for employees who might use their valid computer credentials for an improper purpose." (Br. 28). But Valle has misread the legislative history. The basis for Valle's argument is his reference to page 21 of the 1986 Senate Report. (Br. 28-29 (quoting S. Rep. No. 99-432, at 21)). Far from discussing Section 1030(a)(2), Valle's offense of conviction, that section of the Senate Report addressed the "complete revision of section 1030(a)(3)," which pertains to the

use of federal *computers* (not access to federal *information*) and does not have an "exceeds authorized access" provision at all. *See* S. Rep. No. 99-432, at 21-22; 18 U.S.C. § 1030(a)(3). This passage of the Senate Report has absolutely nothing to do with the revision or subsection at issue.

The relevant portion of the Senate Report explains that replacing the "cumbersome" text of the original statute with the phrase "exceeds authorized access" served one purpose: "to simplify the language" in Section 1030(a)(2). S. Rep. No. 99-432, at 9. In making that substitution, Congress expressed no dissatisfaction with the reach of the original language, merely with the particular formulation. And the definition of "exceeds authorized access" that Congress adopted in Section 1030(e)(6)—"access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"—is entirely consistent with the language it replaced. Both convey that those who are able to access federal data using duly issued credentials violate the statute when they abuse those credentials. If Congress had intended, as Valle claims, to eliminate liability for those who misuse their credentials, it could have done so by eliminating that basis for liability entirely, as it did in Section 1030(a)(3). *See* Rep. No. 99-432, at 21 (noting that Section 1030(a)(3) does not address "abuses of authorized access to Federal computers"). Congress's decision to retain that basis of liability under Section 1030(a)(2) is further proof that Valle has misconstrued the statute and its history.

Valle is equally mistaken about the statute's purpose. In his view, the CFAA was directed at hackers and "is designed to punish trespass-by-computer." (Br. 29). According to Valle, he is neither a hacker nor a trespasser because he had computer credentials that allowed him to enter the NYPD computer system. He is mistaken. The 1984 House Report expressed concern not simply about "hackers" but also "other criminals who access computers without authorization." H.R. Rep. No. 98-894, at 21. Even assuming for the argument that the CFAA is concerned principally with hackers, there is no reason to believe that Valle would not qualify as one. Hacker is not defined (or used) by the CFAA, and in the legislative history, the term is used to describe those "who have been able to access (trespass into) both private and public computer systems." *Id*. at 10; *see also* Oxford Online Dictionary (defining "hacker" as "[a] person who uses computers to gain unauthorized access to data"); Miriam-Webster Online Dictionary (defining "hacker" as "a person who illegally gains access to and sometimes tampers with information in a computer system").[8] As understood by Congress, a hacker

---

[8] Commentators have noted just how much "hacking" involves no technological capability more complicated than exploiting different forms of authorized access to sensitive data. *See, e.g.,* Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 Am. U. Bus. L. Rev. 225, 241 (2013) ("Hackers have long relied on 'social engineering'—convincing people to disclose information that they should not—to gain the trust of targets and compro-

is simply an unauthorized viewer of data analogous to a trespasser.

Once again, Valle's argument boils down to the proposition that because he was able, he was authorized. In Valle's view, he could not have committed a trespass against the NYPD's computer system because the NYPD gave him the ability to enter it (albeit under limited circumstances) and therefore authorized any entry he undertook. For that argument to be correct, it would also have to be correct that the rightful holder of a key cannot ever commit a trespass using that key. Courts and common sense say otherwise. In *Protect-All Ins. Agency, Inc.* v. *Surface*, for example, a landlord argued that because it "had a key to the premises and was entitled, pursuant to the lease agreement, to enter for purposes of inspection and repair," it could not be found to be a trespasser. 957 N.E.2d 215, 2011 WL 5071922, at *5 (Ind. Ct. App. 2011). The reviewing court rejected that argument, explaining that the landlord's possession of "a key and [its] entitle[ment] to enter the premises for certain agreed-upon purposes does not dispense with

---

mise their networks"); Brent Wible, *A Site Where Hackers Are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime*, 112 Yale L.J. 1577, 1584 (2003) ("[M]any hackers turn to 'social engineering,' not technology, when looking for weaknesses in computer networks. Hackers often manipulate authorized users to gain access to networks, a practice that is impossible to stop with technological solutions.").

the . . . trespass claim" which was based on the allegation that the landlord's entry went beyond the agreed-upon purposes. *Id.*; *see also Pari* v. *Phelps Corp.*, 61 A.D.2d 1072 (3d Dep't 1978) (affirming judgment against landlord for trespass). While the tool of access (there a key, here computer credentials) might permit unrestricted access, the scope of access was in fact limited by the terms of authorized use.

Similarly in *People* v. *Licata*, the New York Court of Appeals affirmed a trespass conviction, notwithstanding the defendant's possession of "an admission ticket," because he knew that he was not allowed to enter the premises. 28 N.Y.2d 113, 116 (N.Y. 1971). The Court explained, "While it is ordinarily true that the purchase of an admission ticket to a race track or a place of amusement entitles one to enter the premises, this right is not without limitation." *Id.* The defendant could not rely on that ticket, which certainly would authorize access when used properly, as a defense because the "defendant was guilty of criminal trespass when he entered the track premises with knowledge that he was not 'licensed or privileged to do so.'" *Id.* at 117. The ticket, much like Valle's computer credentials, when properly used might authorize entry, but when improperly used was no defense to trespass. Placed in context, Valle's claim that he did not commit "trespass-by-computer" is not well founded in law or reason.

Valle's interpretation would also frustrate the overarching purpose of the legislation: to protect information belonging to the United States from unauthorized disclosure. Under Valle's reading of Section

1030(a)(2)(B), an employee with credentials enabling him to view classified information in a federal database would face no penalty for abusing those credentials to view information that was beyond his level of security clearance. The rogue employee could violate his training and ignore any number of warnings that information was beyond his clearance, so long as it was not beyond his technical abilities. That is because, under Valle's version of the CFAA, a government entity could not place any limitations on how an employee used his credentials unless it was able to create a computer infrastructure that made it impossible for employees to access data that they did not have official permission to view. Valle does not explain how such a system could be created where, as here, official permission turns not on entering a password or possessing a particular level of clearance but on having a legitimate, law enforcement reason for accessing the data. Technology has not yet progressed—and certainly had not in 1984—to the point where a computer program could make that verification. Accordingly, there is no good reason to believe, and every reason to doubt, that Congress intended to erect such a substantial barrier to the CFAA's purpose of protecting federal information.

3. Precedent Supports the Jury's Verdict

The weight of appellate precedent provides further support for the jury's verdict and Judge Gardephe's decision to uphold it. While this Court has not yet considered the scope of Section 1030(a)(2), other Courts of Appeals have. Where the issue has been squarely presented, those courts have held that

Section 1030(a)(2) prohibits an employee from using his credentials to access information that he lacks official permission to view. Rejecting that precedent, Valle relies on two appellate rulings declining to extend the CFAA to reach those who have permission to access data but then misuse it. Those decisions are no help to Valle because this case is not about subsequent misuse of data, but a lack of permission to access data in the first place.

In *United States* v. *Rodriguez*, the Eleventh Circuit affirmed the conviction of a Social Security Administration employee who obtained information concerning 17 women from a sensitive federal database without any business reason for doing so. 628 F.3d 1258, 1260-61 (11th Cir. 2010). That employee had credentials—a personal identification number and password—enabling him to access federal databases "that contained sensitive personal information, including any person's social security number, address, date of birth, father's name, mother's maiden name, amount and type of social security benefit received, and annual income." *Id.* at 1260. He had also been trained that he was prohibited "from obtaining information from [these] databases without a business reason . . . through mandatory training sessions, notices posted in the office, and a banner that appeared on every computer screen daily." *Id.* In violation of that training, the employee misused his credentials to view "the personal records of 17 different individuals for nonbusiness reasons." *Id.*

On appeal, the defendant in *Rodriguez* argued, like Valle, that "he did not violate section

1030(a)(2)(B) because he accessed only databases that he was authorized to use as" an employee. *Id.* at 1263. Rejecting this argument, the Eleventh Circuit held that the "the plain language of the [CFAA] forecloses any argument that [the defendant] did not exceed his authorized access" because the defendant's "access of the victims' personal information was not in furtherance of his duties." *Id.* at 1263; *see id*. ("Rodriguez exceeded his authorized access and violated the Act when he obtained personal information for a nonbusiness reason."). Faced with facts and arguments strikingly similar to those presented here, the Eleventh Circuit concluded that the CFAA reaches employees who misuse their credentials to obtain information they had no permission to view.

Similarly in *United States* v. *John*, the Fifth Circuit affirmed a conviction under Sections 1030(a)(2)(A) and (C) that involved data belonging to a bank, rather than the government. 597 F.3d 263, 269-70 (5th Cir. 2010). In that case, a bank employee had access to customer information contained within a bank computer system. *Id.* at 269. The bank's "official policy, which was reiterated in training programs that [the defendant] attended, prohibited misuse of the company's internal computer systems and confidential customer information," *id.* at 272, including by "access[ing it] to perpetrate a fraud" and "tak[ing] material . . . regarding accounts from [the] office building," *id.* at 271. The defendant argued on appeal, as Valle does here, that she could not have violated the CFAA because "she was authorized to use [the bank's] computers and to view and print information" and criminal liability could not turn on "her mental

state or motive at the time she accessed or printed account information." *Id.* at 271.

Rejecting that argument, the Fifth Circuit reasoned "that the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'" *Id.* at 272. Where "access to . . . data [is] confined," a person is "not authorized to access that information for any and all purposes but for limited purposes." *Id.* Accordingly, "[a]ccess to a computer . . . may be exceeded if the purposes for which access has been given are exceeded," as it was when the defendant in *John* exceeded her access to customer information by obtaining it in furtherance of a fraud. *Id.*

The Eighth Circuit reached a similar conclusion in *United States* v. *Teague*, 646 F.3d 1119 (8th Cir. 2011). There, an employee of a Department of Education contractor was able to access student loan records using her "unique user ID and password." *Id.* at 1122. Those credentials enabled her to view President Barack Obama's loan records, but that action was not in furtherance of her duties. *Id.* at 1121. The Eighth Circuit affirmed her CFAA conviction, holding that the defendant "intentionally exceeded her authorized computer access" by using her credentials to view records that were beyond the scope of her right to access the database. *Id.* at 1122.

Under the reasoning of these Courts, Valle exceeded his authorized access when he used his credentials to view information that he was unauthorized to see unless he had a legitimate law enforcement justification for doing so. Valle asks this Court

to depart from that precedent based in part on reasoning advanced by the Fourth and Ninth Circuits. But that reasoning—which arose from misuse of data, not a lack of permission to view data—does not support Valle's position.

In *WEC Carolina Energy Solutions LLC* v. *Miller*, the Fourth Circuit examined a civil suit brought under the CFAA between an employer and its former employee. 687 F.3d 199, 201-02 (4th Cir. 2012). The employer alleged that the employee obtained information "without authorization" or by "exceed[ing] authorized access" when he downloaded confidential documents and sent them to his personal email account. *Id.* at 201. The employer had "instituted policies that prohibited using the information without authorization or downloading it to a personal computer" but those "policies did not restrict [the employee's] authorization to access the information" in the first place. *Id.* at 202. Based on these facts, the employee (unlike Valle) had not violated the terms of his access to the database because the policy violation occurred later when the employee emailed the records to himself. The Fourth Circuit therefore concluded that "an employee 'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access." *Id.* at 204. Because the employer's policy prohibited certain *uses* of information but not *access* to it, the employee's "improper use of information validly accessed" did not violate the CFAA. *Id.* at 204.

The Ninth Circuit reached a similar conclusion in *United States* v. *Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc). The employer in that case had implemented "a policy that forbade disclosing confidential information," and the litigation turned on whether current employees had "exceed[ed] authorized access" by obtaining confidential information and improperly disclosing it to a former employee who had formed a competing business. *Id.* at 856-57. The Ninth Circuit found no violation of the CFAA, concluding that "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." *Id.* at 863. According to that Court, access, not use, is the focus of the CFAA, and nothing in the employer's disclosure policy barred access to the data, just the subsequent use of it. *See id.* at 863-64 ("[W]e hold that 'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.").[9]

The majority decision in *Nosal* drew a vigorous dissent. Under the dissenter's reasoning, the employer's use restrictions created an access restriction because the employees knew that if they accessed the

---

[9] Notably, the Ninth Circuit recognized that "individuals whose initial access to a computer is authorized but who access unauthorized information or files" would violate the CFAA. *Id.* at 858; *see also id.* at 857 ("[A]ssume an employee is permitted to access only product information on the company's computer but accesses customer data: He would 'exceed[ ] authorized access' if he looks at the customer lists.").

data for the sole purpose of making an unauthorized disclosure, they were effectively barred from accessing the data in the first place. *See id.* at 866 ("[A]t the time the employee coconspirators accessed the database they knew they only were allowed to use the database for a legitimate business purpose because the co-conspirators allegedly signed an agreement which restricted the use and disclosure of information on the database." (Silverman, J., dissenting)).

Other Courts of Appeals, in accord with the dissenting opinion in *Nosal*, have concluded that the improper use of data can violate the CFAA. *See Int'l Airport Ctrs., L.L.C.* v. *Citrin*, 440 F.3d 418, 420-421 (7th Cir. 2006) (reinstating civil suit where employee's "breach of his duty of loyalty" by violating employment agreement "terminated . . . his authority to access [a company-issued] laptop," making any subsequent access to data "without authorization"); *EF Cultural Travel BV* v. *Explorica*, 274 F.3d 577, 583 (1st Cir. 2001) (holding that violation of "broad confidentiality agreement" by subsequent misuse of proprietary information could violate the CFAA).[10]

---

[10] Valle submits that the Third and Sixth Circuits have suggested without deciding that they would align with the Fourth and Ninth Circuits in this inter-circuit debate. (Br. 20 n.6). There is no good reason to credit that speculation. The Third Circuit's decision in *United States* v. *Auernheimer* had nothing to do with this issue and, in the section Valle cites, construed the elements of a state computer crime, not the CFAA. 748 F.3d 525, 534 (3d Cir. 2014) ("none of

While this debate might be interesting, it has nothing to do with Valle because, as Judge Gardephe observed, Valle's conviction was based on an access restriction, not a use restriction. *See Valle*, 301 F.R.D. at 115 ("Unlike the disloyal employees" in the use-restriction cases, "Valle did not have unrestricted access to the [NYPD computer] system and its associated databases—he was not free to access the information contained in these databases under all circumstances."). As established at trial, Valle violated an access restriction when he viewed information in the NCIC database without a law enforcement purpose. Any subsequent use (or non-use) of the information he saw, either planned or actual, was irrelevant to whether he violated the terms of his access.[11]

---

the essential conduct elements of a violation of the New Jersey statute occurred in New Jersey"). Likewise, the Sixth Circuit's reference to *LVRC Holdings LLC* v. *Brekka*, 581 F.3d 1127 (9th Cir. 2009), does not suggest it would follow the majority decision in *Nosal*. *See Pulte Homes, Inc.* v. *Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011) (citing *Brekka* in effort to construe CFAA's "without authorization" language). After all, both the majority and the dissenters in *Nosal* believed that *Brekka* supported their respective positions. *See Nosal*, 676 F.3d at 864 (majority), 864-65 (dissent).

[11] Notably, in an unpublished decision, the Fourth Circuit rejected an expansion of its holding in *WEC Carolina Energy Solutions* roughly analogous to the one Valle presses here. In *United States* v. *Steele*, a defendant challenged his CFAA conviction, arguing

In light of that basis of liability, Judge Gardephe was right to conclude that "even assuming arguendo that the CFAA does not provide a cause of action to employers whose employees steal confidential computer data and provide it to a competitor, such a conclusion would not justify granting Valle's motion for a judgment of acquittal on Count Two." *Id.* Valle's violation of limitations the NYPD placed upon his access to data—and not his planned use of that data—ran afoul of the CFAA.

---

that he was authorized to access a former employer's data because his computer credentials provided him the ability to access it, even though his employment had been terminated. No. 13-4567, 2014 WL 7331679, at *2 (4th Cir. Dec. 24, 2014) (defendant argued that "because [former employer] did not change his access password when he resigned, [defendant's] post-employment access, though 'ethically dubious' was not 'without authorization' as contemplated by the statute"). The Fourth Circuit disagreed, holding that because the defendant "was not an employee" when "he improperly accessed the company's server" he had no permission to access the information, even if his credentials gave him the technical ability to do so. *Id.* at *2-3. Similarly, Valle's technical ability to access NCIC data using his credentials did not give him authorization or permission to do so.

POINT II

The Statute Raises No Genuine Constitutional Concerns

Valle relies on the vagueness doctrine, the canon of constitutional avoidance, and the rule of lenity to rescue his poorly founded construction of the statute. None of these principles applies here because of the lack of any real ambiguity in the statute and the absence of any genuine constitutional doubts arising from the application of its clear mandate.

A. Applicable Law

1. Vagueness Doctrine

Under the void-for-vagueness doctrine, "a penal statute [must] define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender* v. *Lawson*, 461 U.S. 352, 357 (1983). To meet that standard, a law need only "provide explicit standards" and "need not achieve meticulous specificity, which would come at the cost of flexibility and reasonable breadth." *Mannix* v. *Phillips*, 619 F.3d 187, 197 (2d Cir. 2010) (internal quotation marks omitted). To determine whether a statute provides the requisite "fair notice," this Court examines "whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal." *United States* v. *Rosen*, 716 F.3d 691, 699 (2d Cir. 2013).

Where, as here, there is no claimed violation of the First Amendment, a vagueness challenge is evaluated "only as applied to the facts of the particular case." *Mannix* v. *Phillips*, 619 F.3d at 197. If a defendant's conduct was "clearly proscribed" by the statute, he "cannot complain of the vagueness of the law as applied to the conduct of others." *Id.* at 197 (internal quotation marks omitted).

To preserve a vagueness challenge for appellate review, a defendant must first raise the claim in the district court; otherwise, this Court deems the challenge "waived." *United States* v. *Feliciano*, 223 F.3d 102, 125 (2d Cir. 2000). Even if an unpreserved vagueness challenge could be considered on appeal, it would be subject to stringent plain error review. *See id.* To establish plain error, an appellant must demonstrate that "(1) there is an error; (2) the error is clear or obvious, rather than subject to reasonable dispute; (3) the error affected the appellant's substantial rights, which in the ordinary case means it affected the outcome of the district court proceedings; and (4) the error seriously affects the fairness, integrity or public reputation of judicial proceedings." *United States* v. *Marcus*, 560 U.S. 258, 262 (2010) (internal quotation marks and citations omitted).

2. The Canon of Constitutional Avoidance

The canon of constitutional avoidance advises "that where an otherwise acceptable construction of a statute would raise serious constitutional problems, a court should construe the statute to avoid such problems unless such construction is plainly contrary to

the intent of Congress." *United States* v. *Magassouba*, 544 F.3d 387, 404 (2d Cir. 2008) (internal quotation marks omitted). Far from being "a method of adjudicating constitutional questions by other means," the canon is simply "a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts." *Clark* v. *Suarez Martinez*, 543 U.S. 371, 381 (2005). Like all canons of statutory interpretation, "the canon of constitutional avoidance has no application in the absence of statutory ambiguity." *United States* v. *Oakland Cannabis Buyers' Cooperative*, 532 U.S. 483, 494 (2001).

3. The Rule of Lenity

Under the rule of lenity, "ambiguous criminal laws [are] to be interpreted in favor of the defendants subjected to them." *United States* v. *Banki*, 660 F.3d 665, 675 (2d Cir. 2011). The rule is applicable in very limited circumstances and only where "after considering text, structure, history, and purpose, there remains a grievous ambiguity or uncertainty in the statute." *Barber* v. *Thomas*, 560 U.S. 474, 488 (2010) (internal quotation marks omitted); *see also United States* v. *Edelman*, 726 F.3d 305, 309-10 (2d Cir. 2013). Emphasizing its narrow application, this Court has cautioned that "the rule of lenity is not a catch-all maxim that resolves all disputes in the defendant's favor—a sort of juristical 'tie goes to the runner.'" *United States* v. *Gonzalez*, 407 F.3d 118, 124 (2d Cir. 2005). In the absence of unresolved, grievous ambiguity, the rule of lenity has no application.

B. Discussion

1. Valle Has No Valid Basis to Raise a Void-For-Vagueness Challenge

To the extent that Valle brings a void-for-vagueness challenge to the CFAA, it is unavailing. (Br. 30-32). First, the challenge is unpreserved and therefore either "waived" or, at best, reviewed only for plain error. *See United States* v. *Feliciano*, 223 F.3d at 125. Even assuming that the plain error standard applies here, it could not be met because the purported error was far from "clear or obvious." *United States* v. *Marcus*, 560 U.S. at 262. Judge Gardephe's reading of the statute is entirely consistent with the holdings of the Fifth, Eighth, and Eleventh Circuits and does not directly conflict with the holdings of the Fourth or Ninth Circuits, much less any decision of this Court. Against that precedential backdrop, there can be no plain error. *See United States* v. *Weintraub*, 273 F.3d 139, 152 (2d Cir. 2001) ("Without a prior decision from this court or the Supreme Court" establishing the relevant legal principle, "we could not find any such error to be plain, if error it was.").

Second, regardless of the standard of review, Valle cannot demonstrate that the CFAA is vague as applied to him. The CFAA prohibits accessing NCIC data "without authorization" or by "exceed[ing] authorized access." 18 U.S.C. § 1030(a)(2). The trial evidence established that Valle knew his authorization to access NCIC data was contingent on having a law enforcement justification for doing so. (Tr. 940-42,

972). It was therefore "reasonably clear" that accessing NCIC data without having such a justification would violate the CFAA either because it was unauthorized or because it was in excess of his authorization. *United States* v. *Rosen*, 716 F.3d at 699; *see also United States* v. *Simmons*, 343 F.3d 72, 82 (2d Cir. 2003) (rejecting vagueness challenge to prohibition on possessing pornography because relevant definition "avoids reference to subjective standards and is sufficiently specific to give adequate notice as to what conduct violates a prohibition on pornographic material").

Any claim of inadequate notice is particularly misplaced here. As established at trial, Valle was repeatedly warned that the unjustified use of the NCIC database could result in his termination and prosecution. (Tr. 940-42, 950). Valle cannot now be heard to complain that he was unaware that he might be held criminally responsible for his misconduct. *See Maynard v. Cartwright*, 486 U.S. 356, 361 (1988) ("Objections to vagueness under the Due Process Clause rest on the lack of notice, and hence may be overcome in any specific case where reasonable persons would know that their conduct is at risk.").

2. Neither the Canon of Constitutional Avoidance Nor the Rule of Lenity Weighs in Favor of Valle's Position

Valle next invokes the canon of constitutional avoidance and the rule of lenity to press his vagueness challenges to the CFAA. (Br. 33-41). For either of these principles to have any application here, the

CFAA must be ambiguous. The constitutional-avoidance canon requires that there be two equally "plausible interpretations of a statutory text," *Clark* v. *Suarez Martinez*, 543 U.S. at 381; while the rule of lenity requires that there be "grievous ambiguity or uncertainty" in the text, even after considering every tool of statutory interpretation, *Barber* v. *Thomas*, 560 U.S. at 488. *See Spina* v. *Dep't of Homeland Sec.*, 470 F.3d 116, 130 (2d Cir. 2006) ("[T]he rule of lenity and the doctrine of constitutional . . . have no application where, as in this case, traditional rules of construction permit us to conclude that there is no ambiguity in the statute."). For the reasons set forth in Point I, neither predicate condition has been met here. Judge Gardephe's interpretation of the CFAA is mandated by the statute's text, structure, purpose, and legislative history; it is also consistent with the weight of appellate precedent on the matter.

Assuming for the argument that Valle's construction of the CFAA is as plausible as the one adopted by Judge Gardephe, the constitutional-avoidance canon would not mandate that Valle's view be adopted because Valle has failed to identify any true constitutional difficulty that would be avoided by adopting his preferred construction. Searching for one, Valle argues that access restrictions are not always as precise as the NYPD's, which would "rais[e] serious notice problems" if they were used as basis for prosecution. (Br. 33, 34 (referring to "broadly and abstrusely" written access restrictions); Amici Br. 19). But where the relevant prohibition is imprecise, the element of Section 1030(a)(2) that requires an "intentional[ ]" violation would remain unsatisfied. *See United States*

v. *Kelly*, 147 F.3d at 177 (approving district court's instruction that for an act to be intentional, it must have been done "deliberately and purposefully," as "the product of [an individual's] conscious objective rather than the product of mistake or accident."). Valle does not explain how an imprecise, ambiguous access restriction could give rise to an intentional violation.[12]

And it is no answer to say that juries cannot be entrusted with determining whether an access restriction made particular conduct authorized or unauthorized. (Br. 36 (faulting computer access policies for being "hopelessly unclear")). As this Court has previously held, the CFAA's use of the word "authorization" has no "technical or ambiguous meaning" such that trial courts are not even "obliged to instruct the jury on its meaning." *Morris*, 928 F.2d at 511. It is no more complicated for a jury to determine whether access was authorized in light of an access restriction than it is for juries to make any of the other innumerable determinations that they routinely make. For example, juries have been asked to deter-

---

[12] Even if Valle's view of the statute was preferable as a policy matter, which it is not, a policy preference would not be a sufficient basis to adopt his construction. The Supreme Court has cautioned that "[t]he canon favoring constructions of statutes to avoid constitutional questions does not . . . license a court to usurp the policymaking and legislative functions of duly elected representatives." *Heckler* v. *Mathews*, 465 U.S. 728, 741 (1984).

mine whether a defendant had "an affirmative duty of disclosure, and breached it by his failure to disclose material information." *United States* v. *Margiotta*, 688 F.2d 108, 128 (2d Cir. 1982). Juries that are capable of determining the existence of fiduciary duties, whether conduct breached such a duty, and whether information is material are equally well suited to determine whether a user had authorization to access data in light of an access restriction.[13] Valle presents no valid basis to conclude that the CFAA presents unique challenges to the jury system.

Valle is equally wrong to invoke the rule of lenity. (Br. 39-41). His ability to "articulat[e] a narrower construction [of the statute] does not by itself make the rule of lenity applicable," as it will be the rare case where a litigant cannot conceive of a more restricted construction of any given statute. *Smith* v. *United States*, 508 U.S. 223, 239 (1993). The rule ap-

---

[13] Valle also expresses concern about arbitrary enforcement, but does not explain how a prohibition on viewing data in violation of an access restriction would invite greater arbitrariness than a prohibition on fraud based on a breach of a fiduciary duty. (Br. 37-38). Likewise, Amici offer no reason to believe that juries would be incapable of examining "employer-employee" relationships, "company-consumer relationships" and other "relationships traditionally governed by tort and contract law" to determine whether an access restriction exists (Amici Br. 21), when they examine precisely those relationships under existing law to determine whether a fiduciary duty exists.

plies only when a court can do no more than "guess as to what Congress intended." *Muscarello* v. *United States*, 524 U.S. 125, 139 (1998). No such guesswork is required here, where the statute uses neither technical nor ambiguous words to restrict unauthorized access to protected data. Valle's repackaging of his erroneous understanding of the CFAA's legislative history and precedent construing use restrictions are no more persuasive here than when presented earlier in his brief. The rule of lenity has no bearing on the proper construction of the CFAA.

CONCLUSION

The judgment of conviction should be affirmed.

Dated: New York, New York
April 1, 2015

Respectfully submitted,

PREET BHARARA,
United States Attorney for the Southern District of New York,
Attorney for the United States of America.

RANDALL W. JACKSON,
HADASSA WAXMAN,
BROOKE CUCINELLA,
JUSTIN ANDERSON,
Assistant United States Attorneys,
Of Counsel.

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 32(a)(7)(C) of the Federal Rules of Appellate Procedure, the undersigned counsel hereby certifies that this brief complies with the type-volume limitation of Rule 32(a)(7)(B). As measured by the word processing system used to prepare this brief, there are 9,598 words in this brief.

PREET BHARARA,
United States Attorney for the Southern District of New York

By: JUSTIN ANDERSON,
Assistant United States Attorney