14-4396-cr

United States Court of Appeals
for the Second Circuit

Docket No. 14-4396-cr

UNITED STATES OF AMERICA,

Appellee,

-against-

GILBERTO VALLE,

Defendant-Appellant.

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

CORRECTED
REPLY BRIEF FOR DEFENDANT-APPELLANT GILBERTO VALLE

Federal Defenders of New York, Inc.
Appeals Bureau
52 Duane Street, 10th Floor
New York, New York 10007
Tel. No.: (212) 417-8742
Attorneys for Defendant-Appellant

Robert M. Baum
Julia L. Gatto
Edward S. Zas
Of Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

CONSTITUTIONAL PROVISIONS, STATUTES, AND RULES

OTHER AUTHORITIES

PRELIMINARY STATEMENT

As an NYPD officer, Gilberto Valle was authorized to access the NYPD computer system to obtain information from the federal NCIC database. Yet the government claims he is guilty under the CFAA because he used his authorized access to that database for an unauthorized purpose—looking up his friend Maureen Hartigan in 2012—in violation of NYPD protocol. This is exactly the purpose-based theory of liability that the government has advanced before and that the Fourth and Ninth Circuits (and a growing number of lower courts) have rejected. Contrary to the government's view, the CFAA, a computer-hacking statute, does not transform every violation of a workplace computer-use policy into a federal crime. This remains true even if the workplace is a police station.

The government's brief[1] brims with moral indignation at Valle's violation of NYPD rules—and again distorts the facts by insinuating that his computer search somehow furthered a nefarious plot to kidnap, cook, and eat Hartigan.[2] That

---

[1] "GB" refers to the government's brief; "OB" refers to Valle's corrected opening brief; "A" refers to Valle's Appendix; and "Tr." refers to the trial transcript.

[2] The government falsely suggests that Valle's search of Hartigan's name was among the "most egregious[]" aspects of a plot to "kidnap and torture women." (GB 3–4.) In fact, as Judge Gardephe recognized, Valle never discussed kidnapping or harming Hartigan. Tr. 552 ("[T]he government has not disputed … that there are no Internet chats between the defendant and another person involving a kidnapping

approach cannot substitute for cogent statutory analysis. The government does not and cannot dispute that its broad reading of the CFAA would make a federal criminal of every person who uses his or her work computer for a purpose prohibited by company policy (or by principles of agency law), or who accesses a website from any computer in a way that violates the site's rules. For example, the government's interpretation would mean that any employee who uses his or her work computer to send and receive personal e-mails, in violation of company policy, would be guilty of intentionally "exceed[ing] authorized access" to that computer. *See* 18 U.S.C. § 1030(a)(2)(C). Nothing in the statute supports such a boundless (and likely unconstitutional) expansion of federal criminal law.

To avoid that conclusion, the government erects a series of straw men in place of Valle's actual argument. It attributes to him the absurd position that, if someone has the mere physical or technical ability to access a computer, he has "authorization" and therefore cannot be prosecuted under the CFAA. (GB 7, 11–13.) That, of course, is not Valle's argument. Hackers violate the CFAA *particularly when they are able* to access a computer; indeed, as Valle's opening brief made clear,

---

of Hartigan."). And if the government seriously thought Valle's query was part of a conspiracy, it would not have charged him with a misdemeanor CFAA offense because the statute elevates any violation into a felony when committed in furtherance of a crime. *See* 18 U.S.C. §§ 1030(a)(2)(B) & 1030(c)(2)(B)(ii).

hackers are the statute's targets. The government resorts to this mischaracterization because Valle's personal use of his work computer simply does not qualify as hacking.

The government then asserts that Valle's CFAA conviction is proper because he was not permitted to use other tools of his job, like a gun or handcuffs, to assault people without consequences. Among many other reasons, this argument is puzzling because the CFAA applies to *anyone* who accesses a computer improperly, not only police officers. That employees—*e.g.*, police officers with handcuffs, secretaries with staplers, and judges with gavels—face legal repercussions for crimes they commit using instruments from work is in no way illustrative of the CFAA's prohibition on computer hacking. And the argument thus fails to show that police officers, secretaries, and judges violate the CFAA if they disobey their employer's policy and use work computers for personal reasons.

The government also falsely suggests that its interpretation only concerns "restricted federal databases" rather than routine computer usage. The "restricted," "sensitive," or "confidential" nature of the NCIC database makes for nice rhetorical flourishes by the government, but has no legal relevance. The CFAA applies the same protections to government databases as it does to *every other* computer in the United States and website connected to the Internet. Under the government's reading, the CFAA would cover Valle's conduct even if he had simply used an

NYPD-issued smartphone to google Hartigan. *See* 18 U.S.C. § 1030(a)(2)(C). That reading is wrong.

The government finds no refuge in the CFAA's statutory history. A prior version of the CFAA prohibited accessing a computer with authorization but without a valid purpose. (OB 26–30.) In 1986, Congress amended the statute to remove any reference to a defendant's "purposes." That amendment speaks for itself: Congress narrowed the statute to limit liability to improper computer "access," and to eliminate coverage for people who use their authorized access for an improper purpose. The government's argument that Congress merely sought to "simplify" the statute (GB 19) is unfounded.

The government also has no persuasive answer to Valle's reliance on the rules of constitutional avoidance and lenity. To the extent the statute is ambiguous and, if interpreted broadly, potentially unconstitutional, these interpretive tools support construing the CFAA narrowly in Valle's favor.

ARGUMENT

I. THE GOVERNMENT MISREADS THE PLAIN LANGUAGE OF THE CFAA.

The CFAA "can be read either of two ways[,]" *United States v. Nosal*, 676 F.3d 854, 856 (9th Cir. 2012):

> 1) "First, … it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as 'hacking.'" *Id.* at 856–57. For example, an employee might be authorized to access her own e-mail account on the employer's server. If the employee hacks into someone else's account on the same server, the employee has accessed data or files she has no right to access, in violation of the statute. (*See also* OB 11–12.)
>
> 2) "Second, as the government proposes, the language could" cover circumstances where "an employee may be authorized to access customer lists in order to do his job," but not for other reasons, like sending them to a competitor. *Nosal*, 676 F.3d at 857. Under this interpretation, if an employer's policy permitted the employee to access the employer's computers only for official business, the employee would be liable if he accessed the employer's computers without any legitimate business reason.

Nosal and many other decisions have rejected the second interpretation (the "Broad Interpretation"), which the government advances here, in favor of the first interpretation (the "Narrow Interpretation"). *Id.* at 854; (*see* OB 20–21 (collecting cases).) These courts rejected the Broad Interpretation because it: (A) engrafts a subjective intent element onto the statute by making liability turn on a defendant's

purpose for using a computer, when the statute narrowly governs unauthorized computer "access"; (B) improperly renders the CFAA's two distinct terms (accessing a computer "without authorization" and "exceed[ing] authorized access") redundant; (C) stands in tension with the CFAA's damages provisions, which focus on redressing physical harm to computer systems, not intangible harm caused by employees who daydream or procrastinate online; and (D) would ensnare every Internet user who violates an employer's or a website's terms of use.

The Narrow Interpretation avoids these problems by adhering to the statute's text, history, and purpose. Specifically, it: (A) punishes hacking-like activity, *i.e.*, accessing forbidden computers and files; (B) gives distinct meaning to every term in the CFAA; (C) comports with the CFAA's damages provisions by allowing recovery for access breaches that damage a computer system's integrity; and (D) provides a bright-line rule that avoids criminalizing a broad swath of innocent behavior. As discussed below, the government fails to refute these points.

A. The Government Endorses the Same Erroneous Construction of the CFAA That Courts Have Repeatedly and Persuasively Rejected.

Valle's opening brief showed that liability under the CFAA does not turn on a defendant's purpose, but rather on unauthorized computer access. (OB 10–25.) For this reason, Valle's CFAA conviction must be reversed because he was authorized

to access his NYPD computer, including the NCIC database. Under the CFAA, his alleged bad purpose in accessing the computer is irrelevant.

The government responds that Valle's authority to access his NYPD computer was conditioned on having a law-enforcement purpose. (*See* GB 10.) Because he accessed his computer without such a purpose, the government argues, he acted without "permission." (*Id.* 10–11.) As Valle's opening brief explained (OB 19), the government made exactly the same argument unsuccessfully in *Nosal*. There, the government argued that, under the policies of an employer (Korn/Ferry), employees "were not entitled to access information on Korn Ferry computers … unless they had a legitimate Korn Ferry business purpose for doing so." Reply Brief for the United States, *Nosal* (No. 10-10038), 2010 WL 6191782, at *5. The government continued that "[b]ecause the [employees] lacked this required purpose" when they obtained certain information, the employees lacked any authority to access the computer. *Id.* The *en banc* Ninth Circuit rejected this argument because the CFAA's prohibitions "apply[] to hackers," not employees who violate their employer's computer-use policies. *Nosal*, 676 F.3d at 858.

The government mischaracterizes *Nosal* in a vain effort to distinguish it. The government says that "nothing in [Korn/Ferry's] disclosure policy barred access to the data, just the subsequent use of it." (GB 28 (citing *Nosal*, 676 F.3d at 863–64).) That is untrue: Korn/Ferry's policy restricted computer activity to "Korn/Ferry

business only." *Nosal*, 676 F.3d at 856 n.1. For this reason, the issue in *Nosal* was not whether an employee's misuse of data, *after* the employee accessed it, violated the CFAA. Rather, the issue was whether an employee could be prosecuted for accessing data without a valid business purpose, in violation of company policy, which is the same issue here. The *Nosal* court made this clear by framing the question presented as follows: "Many employers have adopted policies prohibiting the use of work computers for nonbusiness purposes. Does an employee who violates such a policy commit a federal crime?" *Nosal*, 676 F.3d at 856. The Ninth Circuit answered in the negative. The government simply disagrees with *Nosal*'s holding, but fails to distinguish it or offer any persuasive reason why this Court should not follow it.

The district court made the same error as the government in falsely distinguishing the cases that support the Narrow Interpretation, including *Nosal,* as "disloyal employee misappropriation and misuse cases." (A. 236.) The supposed distinction is that Valle was not accused of misappropriating or misusing information. (GB 30.) But as Valle's opening brief detailed, the defendants in those cases all violated an employer's computer policy that forbade accessing its computers for non-business reasons. (OB 26.) And the evidence of the subsequent use of the information in those cases was relevant only to show that the defendants had an improper purpose in the first place. (*Id.*) Thus, the district court's departure

from those cases based on Valle's "non-use" results in the absurdity of punishing Valle for *not* using the information he obtained, while excusing Nosal and the other defendants for *nefariously* using their information, when all had an "improper purpose." (*Id.* 25–26.)

The government's confusion of improper use and improper access does not stop there. For example, the government concedes that the CFAA "is not concerned with what Valle did or *intended to do* with that restricted information." (GB 11 (emphasis added).) But then the government avers that Valle's conviction arises from his impermissible "purpose." (*Id.*) This is double-talk: either the CFAA punishes Valle based on *why* he accessed his computer or it does not. No amount of semantic gymnastics about "intended use" versus "purposes" for use[3] should obscure that Valle's conviction rests entirely on his use of his authorized computer access for an unauthorized personal reason. While some courts have allowed purpose-based liability under the CFAA (*see* GB 24–27 (collecting cases)), others, like *Nosal* and *WEC Carolina Energy Solutions LLC v. Miller*, have disagreed and stressed the many flaws of those holdings. *See Nosal*, 676 F.3d at 856; *Miller*, 687 F.3d 199, 206

---

[3] Though relying heavily on this distinction, the government utterly fails to explain the purported difference between what Valle "intended to do" when he accessed his NYPD computer and his "purpose" for accessing it.

(4th Cir. 2012). *Nosal* and *Miller* have the better of the argument, namely that a defendant does not violate an "access" restriction merely by violating a "purpose" restriction.[4]

For that reason, Valle devoted much of his opening brief to *Nosal* and *Miller*, and to showing that their criticisms of the cases relied upon by the district court are persuasive. The government, on the other hand, never comes close to addressing the merits of *Nosal*'s and *Miller*'s criticisms. Instead, the government relies on non-existent distinctions to avoid the circuit split. But that division between the circuits bears directly on the soundness of the district court's holding and deserves this Court's full attention.

To start, *Nosal* was "unpersuaded by the decisions of [its] sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty," and that look "only at the culpable behavior of the defendants before them" rather than "the effect on millions of ordinary citizens caused by the statute's unitary definition of 'exceeds authorized

---

[4] The government raises no arguments in favor of purpose-based liability not addressed in Valle's opening brief. (*See* OB 22–24.) But the government repeats the district court's error in reading *United States v. Teague* to support its position (GB 26) because, in that case, the defendant never contested that accessing information for an improper purpose violated the CFAA. 646 F.3d 1119, 1122 (8th Cir. 2011).

access.'" *Nosal*, 676 F.3d at 862 (citing *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006)). *Miller* rejected the cases adopting the Broad Interpretation because they "transform[] a statute meant to target hackers into a vehicle for imputing liability to workers" who use their "access for a purpose contrary to the employer's interests." *Miller*, 687 F.3d at 206, 207. In this Circuit, Judge Engelmayer held that reading the CFAA "to turn on the employee's *purpose* in making use of his permitted access to the information, as the Seventh Circuit does, would effectively add to the statute a subjective intent requirement that Congress did not impose." *JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 523 (S.D.N.Y. 2013) (emphasis in original). Judge Cote similarly criticized "[t]he interpretation of the CFAA adopted in this line of cases" for relying on an "individual's *subjective intent* in accessing a computer system, whereas the text of the CFAA calls for only an objective analysis of whether an individual had sufficient 'authorization.'" *United States v. Aleynikov*, 737 F. Supp. 2d 173, 194 (S.D.N.Y. 2010) (emphasis added).

The government instead proffers hypotheticals that purport to show that Valle's conviction for a computer crime under the CFAA is proper because he was not allowed to use other police equipment, such as his gun and handcuffs, in an improper manner. (GB 12.) For example, the government notes that a police officer could not plausibly claim that "he was authorized to restrain a member of the public

on a lark [simply] because the NYPD had issued him handcuffs." (*Id.*) Like all of the government's hypotheticals, this example has no bearing on the CFAA's specific provisions. (*Id.*) The examples all involve police officers using their tools for an improper purpose; they say nothing about what Congress intended when it sought to punish unauthorized "*access*"—*by anyone*—to information on a computer. Valle agrees that the CFAA does not grant employees the right to trample over the constitutional rights of others so long as they use their employer's computer. And nobody would defend a statute that lets police officers use their guns and handcuffs "on a lark" without consequences. That does not mean, of course, that every improper use of a work computer amounts to a criminal offense under the CFAA.

The government proceeds to knock down another straw man by claiming that Valle's position is that, if someone has the "ability" to access a computer, she has "authority" to do so. In other words, according to the government, Valle advocates rewarding successful hackers with CFAA immunity, and only punishing inchoate offenses, *i.e.*, those who try but are unable to access a computer without authorization or in excess of authorization. This is a gross mischaracterization.

As Valle's opening brief explained, the CFAA punishes hackers who are *unauthorized* but *able* to[5] access computer information by, for example, bypassing technical access barriers or stealing the log-in credentials of an authorized user. Valle's opening brief even affirmatively cited several cases following *Nosal* that applied the CFAA to defendants who successfully accessed information they were not authorized to access for any purpose. (OB 32 (citing *Facebook, Inc. v. Grunin*, No. 14 Civ. 2323, 2015 WL 124781 (N.D. Cal. Jan. 8, 2015); *NetApp, Inc. v. Nimble Storage, Inc.*, No. 13 Civ. 5058, 2014 WL 1903639 (N.D. Cal. May 12, 2014)).) Thus, the Narrow Interpretation does not mistakenly equate the ability to access a computer with the authority to do so, as the government claims.

B. The Government's Interpretation Creates Surplusage.

The government, like the district court, improperly collapses the CFAA's distinct provisions—"without authorization" and "exceeds authorized access." If an impermissible purpose revokes authorization "*ab initio*," then "exceeds authorized access" has no meaning distinct from "without authorization." (OB 16.) The Narrow Interpretation, in contrast, affords these distinct phrases distinct meanings: the first prong targets "*outside* hackers (individuals who have no authorized access to a

---

[5] The CFAA also punishes hackers who attempt to procure restricted information but are unable to do so. *See* 18 U.S.C. § 1030(b).

computer at all)," and the second prong targets "*inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." *Nosal*, 676 F.3d at 858 (emphasis in original).

The government responds that any surplusage is irrelevant because the "text is unambiguous." (GB 16.) This is untrue: § 1030(e)(6)'s definition of "exceeds authorized access" shows that Congress did not speak redundantly. This definition applies to a user who *had authorization* to access a computer (making the "without authorization" prong inapplicable), but then used that access to gain "information to which he is not entitled." *Diamond Power Int'l, Inc. v. Davidson* 540 F. Supp. 2d 1322, 1342–43 (N.D. Ga. 2007) (observing that the purpose-based liability theory "conflates the meaning of those two distinct phrases and overlooks their application in § 1030(e)(6)"). As Judge Cote explained, the Broad Interpretation "improperly infer[s] that 'authorization' is automatically terminated where an individual 'exceeds *the purposes* for which access is 'authorized.'" *Aleynikov*, 737 F. Supp. 2d at 193–94 (quoting *John*, 597 F. 3d at 272; *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)) (emphasis in original).

The government then shifts gears and denies that its interpretation creates surplusage. (GB 16.) But the rest of the government's brief exposes the surplusage inherent in the government's position: the government repeatedly argues that Valle's improper purpose means he acted without authorization *and* exceeded authorized

access. For example, the government opens its brief by stating that "[o]n May 31, 2012, *without authorization*, Valle accessed the database to obtain information on Maureen Hartigan." (GB 4 (emphasis added).) The government later contends that "all that 'mattered is that Valle *was not authorized* to access the system to perform a query regarding Hartigan's name. . . .'" (*Id.* at 11 (quoting A. 236) (emphasis added).) The government thus inadvertently confirms that the Broad Interpretation does violence to the text of the CFAA by rendering its distinct terms redundant.

C. The Government Cannot Harmonize Its Sweeping Interpretation with the CFAA's Damages Provisions.

The government does not respond to Valle's argument that the Broad Interpretation is irreconcilable with the CFAA's damages provisions. (*See* OB 17–18.) Those provisions speak in terms of "impairment to the integrity or availability of data," "restoring the data program," and "revenue lost, cost incurred or other consequential damages incurred because of interruption of service." 18 U.S.C. §§ 1030(e)(8) & (11).

Such provisions "are consistent with the CFAA's prohibition of computer hacking, which compromises the integrity and availability of data and may cause an interruption of computer service." *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385–86 (S.D.N.Y. 2010). But the damages provisions are "inconsistent or in tension with a broader interpretation of improper 'access.'" *Id.* As Judge Engelmayer explained, "it would be illogical" for the CFAA to prohibit

those who use their authorized access for an improper purpose, but not to define loss to include the loss resulting from such conduct. *JBCHoldings*, 931 F. Supp. 2d at 524 (citing *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 563 (2d Cir. 2006) (summary order)). The government's response—silence—is a tacit concession that the Broad Interpretation cannot be reconciled with the CFAA's damages provisions, and is therefore untenable.

D. The Government's Interpretation Is Unsustainable Across the CFAA.

Further evidence that the Broad Interpretation of "exceeds authorized access" is wrong is that it cannot be applied consistently throughout the statute. Valle was charged under a subsection of § 1030(a)(2), which punishes:

> [whoever] intentionally accesses a computer without authorization or *exceeds authorized access*, and thereby obtains:
>
> (A) information contained in a financial record of a financial institution . . . .
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer[.]

18 U.S.C. § 1030(a)(2) (emphasis added). This unitary iteration of "exceeds authorized access" covers both information from the United States and information from a "protected computer." And the definition of a "protected computer" includes any computer connected to the Internet. 18 U.S.C. § 1030(e)(2)(B).

This is important because it means that if Valle can be convicted for exceeding his authorized access to a computer and thereby obtaining information from the United States, simply because his purpose was prohibited by his employer, every employee who accesses his employer's Internet-connected computer with an improper purpose is also guilty. Moreover, because websites are housed on protected computers, any violation of a website's rules restricting access also amounts to a CFAA violation. Thus, by the government's and district court's reading, the CFAA necessarily criminalizes the following actions, among many others:

- Using a work-issued smartphone to send and receive personal e-mails, in violation of company policy. *Nosal*, 676 F.3d at 860 n.6.
- Using a work computer to watch sports highlights, in violation of company policy. *Id.* at 860.
- Using a home computer to post an item for sale on eBay but listing the item in an inappropriate category, in violation of the website's terms of use. *Id.*
- Logging into a relative's Facebook account at her request and uploading pictures from a family reunion, in violation of Facebook's restriction on using another's account. *Id.* at 861.

Valle's opening brief cited two similar examples of the overreach at the heart of the district court's interpretation of the CFAA—specifically, that it necessarily

criminalizes exaggerating on a dating website or shepardizing a law school note online while clerking for a federal judge. (OB 16.)

In response, the government does not dispute that its interpretation would ensnare the "lonely heart … for misrepresenting his height and weight on a dating website" and "a law clerk … for shepardizing his law school note." (GB 13.) It answers that such "hypothetical musings" can be "set aside" because these people presumably did not "obtain[] U.S. data through the hypothetical use of computers," and, in any event, present "fact-specific questions not relevant here." (GB 13–15.)

The government made these same arguments in *Nosal*, which the *en banc* Ninth Circuit correctly rejected under "the 'standard principle of statutory construction … that identical words and phrases within the same statute should normally be given the same meaning.'" *Nosal*, 676 F.3d at 859 (quoting *Powerex Corp.* v. *Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007)). The Ninth Circuit continued:

> Giving a different interpretation to each is impossible because Congress provided a *single* definition of 'exceeds authorized access' for all iterations of the statutory phrase. Congress obviously meant 'exceeds authorized access' to have the same meaning throughout section 1030. We must therefore consider how the interpretation we adopt will operate wherever in that section the phrase appears.

Nosal, 676 F.3d at 859.

Interpreting "exceeds authorized access" narrowly and consistently throughout the statute avoids dangers that are not merely hypothetical. In *United States v. Drew*, for example, the government used the Broad Interpretation to prosecute a woman for creating a fake Myspace.com profile. 259 F.R.D. 449 (C.D. Cal. 2009). The government charged her under the CFAA for exceeding authorized access because she violated the website's rules requiring users to provide "truthful and accurate" information. *Id.* at 454. The court acquitted the defendant after trial, ruling that the government's sweeping interpretation of the CFAA resulted in absurd consequences and left "federal law enforcement entities … free to 'pursue their personal predilections.'" *Id.* at 467 (quoting *Kolender v. Lawson*, 461 U.S. 352, 358 (1983)). This Court should acquit Mr. Valle as well.[6] *See Feldstein*, 951 F. Supp. 2d at 218 (rejecting Broad Interpretation by explaining that "[i]t is obviously absurd to impose criminal liability for checking personal email at the workplace, or some similarly innocuous violation of an employee computer use agreement.").

---

[6] Although the *Nosal* dissent did not share the *en banc* majority's concern over "the parade of horribles that might occur under *different* subsections of the CFAA," *Nosal*, 676 F.3d at 866 (Silverman, J. dissenting) (emphasis in original), subsequent cases brought under § 1030(a)(2)(C) have "demonstrat[ed] the shortcomings of that position," because it is impossible to apply § 1030's subsections to "differentiate[] between harmless workplace procrastination and more serious theft of intellectual property." *Advanced Micro Devices, Inc. v. Feldstein*, 951 F. Supp. 2d 212, 218 (D. Mass. 2013).

Moreover, to the extent the government implies that the CFAA guards "U.S. data" more jealously than general information on the Internet or on a dating website, nothing in the CFAA supports that position. The CFAA draws no distinction between "information from … the United States" and information from "any protected computer." Yet the government goes out of its way to suggest that the CFAA specially protects "information belonging to the United States from unauthorized disclosure" (GB 8 (citing 18 U.S.C. § 1030(a)(2)(B)), and punishes "rogue employee[s]" for misappropriating "classified information" from the United States. (*Id.* 23.) These are nothing more than thinly veiled scare tactics designed to shift the Court's focus from the language of the CFAA. And disclosing or misappropriating classified information is a separate federal crime.

In short, the Narrow Interpretation of the CFAA is the best reading of the statutory text. This Court should join the Fourth and Ninth Circuits in adopting it.

II. THE GOVERNMENT'S ATTEMPT TO ESCAPE THE STATUTORY HISTORY SHOULD BE REJECTED.

The CFAA's statutory history confirms that the statute does not impose purpose-based liability. In 1986, Congress deleted language from the CFAA making it a crime to "access[] a computer with authorization" and "use[] the opportunity such access provides *for purposes to which such authorization does not extend.*" Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 1837, 2190 (codified as amended at 18 U.S.C. § 1030)

(emphasis added). This is straightforward evidence of congressional intent: Congress removed any reference to "purposes" so that CFAA liability would not turn on a defendant's "purposes."

The government's attempt to drown out this clear signal with noise from the legislative history is unpersuasive. The government first contends that the 1986 amendments did not have a "substantive impact on the CFAA," but merely clarified "cumbersome" text. (GB 18.) The 1986 amendments did clarify the CFAA, but not in a way that helps the government. That is, Congress clarified that the statute targets hackers who access information they may not access for any purpose. (OB 26.) As Valle's opening brief detailed, Congress initially enacted and later amended the CFAA to specifically deter hacking. (*Id.* 27–28.) The 1986 Senate Report states that Congress passed the original version of the CFAA in haste with a legislative rider. *See* S. Rep. No. 99-432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494. When the statute was enacted in 1984, the House of Representatives had not voted on a series of narrowing amendments that the Senate had unanimously approved. *Id.* The 1986 amendments thus fixed the shortcomings of the original version by narrowing its language to focus on hackers.

In particular, the 1986 Senate Report explained that Congress added a new defined term, "exceeds authorized access," to "eliminate coverage for authorized access that aims at purposes to which such authorization does not extend," thereby

"remov[ing] from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed authorization." *Id.* at 2479, 2494–95.

The government's purpose-based theory of liability is exactly the one Congress eliminated. The government dismisses this Senate Report by claiming it only applied to § 1030(a)(3), which, according to the government, has "nothing to do with" the changes to § 1030(a)(2). (GB 19.) But the 1986 amendments made the *same* deletion of "purposes" from § 1030(a)(2) as from § 1030(a)(3). Thus, the explanations for the amendment apply equally to both.

III. THE GOVERNMENT CANNOT OVERCOME THE CANON OF CONSTITUTIONAL AVOIDANCE AND THE RULE OF LENITY.

Valle's opening brief showed that the district court's interpretation of the CFAA raises serious constitutional problems (including vagueness), in violation of the canon of constitutional avoidance, and also contravenes the rule of lenity. (*See* OB 30-41.) The government's response is unpersuasive.

A. The Government Fails to Cure the Serious Vagueness Problems Underlying the District Court's Interpretation.

The government makes two arguments to escape the vagueness caused by the Broad Interpretation of the CFAA. First, the government asserts that Valle waived his vagueness argument. (GB 35.) Second, the government contends that Valle

cannot claim the CFAA is vague as to him because he was warned against using NYPD computers for non-work purposes. (*Id.* 36.) Both arguments lack merit.

Valle did not waive his vagueness argument. The vagueness doctrine is part of the fair warning requirement (OB 30), and Valle's motion for acquittal on the CFAA Count argued that the "need for fair warning" militated against a "construction of the statute broader than that clearly warranted by the text." (Memorandum of Law in Support of Valle's Motion for Acquittal on Count Two 11, *Valle*, No. 12-Cr.-847 (PGG) (S.D.N.Y. filed June 17, 2013), ECF No. 179.) Valle's briefing in the district court also extensively quoted *Nosal*'s discussion of the vagueness problems caused by the Broad Interpretation. (*Id.* 8–9 (quoting *Nosal*, 676 F.3d at 860–62).) Thus, the government's preservation argument fails.

The government also contends that the Broad Interpretation raises no serious vagueness concerns because the CFAA makes "reasonably clear" that employees may not use their work computers for personal purposes, in violation of their employer's computer-use policies. (GB 36 (quotation omitted).) As discussed above, this is not what the statute says. And the government misses the point: making CFAA liability turn on standards set by an employer (or a website) exacerbates, rather than diminishes, the vagueness problems raised by the Broad Interpretation. Again, *Nosal* rejected this same argument:

> Were we to adopt the government's proposed interpretation, millions of unsuspecting individuals would

> find that they were engaging in criminal conduct. Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes.

Nosal, 676 F.3d at 859–60. In other words, even if the CFAA could be construed to elevate workplace computer-use policies into federal law, the terms of those policies are often too vague for people to understand (assuming they even read them), and also invite arbitrary and discriminatory enforcement. (*See* OB 33.) Moreover, policies forbidding personal use of work computers, like the NYPD's here, fare no better because what constitutes "personal" versus "professional" purposes is inherently elusive. *See Nosal*, 676 F.3d at 860.

That Valle was told that he could use NYPD computers only for official business does not address the vagueness underlying the Broad Interpretation. First, a statute's vagueness results from the interpretation of the statute itself, not the "subjective expectations of particular defendants." *Bouie v. City of Columbia*, 378 U.S. 347, 355 n.5 (1964). Second, no evidence showed that Valle knew that using his NYPD computer for personal reasons violated a federal *computer-hacking* statute. Third, to imply that Valle could have known the CFAA applied to his conduct ignores the wide divisions among courts interpreting § 1030, especially

within this Court's jurisdiction after *Aleynikov* and *JBCHoldings*. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1616 (2003).

Fourth, any warnings Valle received cannot save a construction of the CFAA that equates hacking with personal use of a work computer against company policy. That is why *Nosal* rejected the argument that the CFAA encompasses workplace computer-use restrictions, even though the defendant there encountered a warning prior to accessing Korn/Ferry's database stating, "[t]his product is intended to be used … for work on Korn/Ferry business only." *Nosal*, 676 F.3d at 856 n.1. The NYPD's similar instructions likewise fail to cure the vagueness of § 1030 as interpreted by the government.

B. The Canon of Constitutional Avoidance Favors the Narrow Interpretation.

Because the Broad Interpretation likely renders the CFAA unconstitutionally vague, the canon of constitutional avoidance favors the Narrow Interpretation. The government claims that the canon does not apply here because the Narrow Interpretation is neither "plausible" nor necessary to avoid constitutional concerns. These objections ignore virtually every case that has considered the canon in light of the CFAA.

First, the Narrow Interpretation is the most "plausible" reading of the CFAA. Indeed, as explained above and by *Nosal*, *Miller*, *Aleynikov,* and many other

decisions, the Narrow Interpretation is far more compelling than the Broad Interpretation. It remains the only interpretation faithful to the statute's computer-hacking focus, and it provides fair warning that hackers violate federal law by accessing information they have no entitlement to access for any purpose. For all of its bluster about "plausibility," the government fails to cite a single case holding that the Narrow Interpretation is implausible.

Second, the government is wrong to say that "Valle has failed to identify any true constitutional difficulty" posed by the district court's decision. (GB 37.)[7] As detailed above and in Valle's opening brief, the Broad Interpretation raises real

---

[7] The government claims that computer users "who inadvertently access U.S. data" do not violate the CFAA "because only intentional acts are prohibited." (GB 9.) Not so. Only the unauthorized access to a computer needs to be intentional, not the obtaining of information from the United States or from a protected computer. *See* 18 U.S.C. § 1030(a)(2) (covering whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information...."). Indeed, the jury instructions here—which the government requested—did not require a finding that Valle intended to obtain federal data. Tr. 1663.

The government also wrongly claims that the intentionality requirement prevents the Broad Interpretation from ensnaring minor computer dalliances and violating the void-for-vagueness doctrine. (GB 37–38.) Because a user need only intend to access a computer in excess of his authority, the Broad Interpretation necessarily covers anyone who, for example, intentionally violates company policy by accessing a workplace computer to send and receive personal e-mails, to make an online dinner reservation, to search a friend's name on Google, and to perform many other quotidian and innocent online activities.

vagueness concerns. This argument is no novelty. Courts and scholars have recognized that the Broad Interpretation threatens to criminalize an astonishingly wide variety of routine behavior but provides no clear standard separating the criminal conduct from non-criminal conduct. *See, e.g.*, *Nosal*, 676 F.3d at 860; *Drew*, 259 F.R.D. at 466; *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 618 (E.D. Pa. 2013); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1586 (2010). This Court should avoid such serious doubts about the statute's vagueness by reading it narrowly.

Finally, the government offers no response whatever to Valle's argument that the Broad Interpretation would effectively delegate to private companies and "to prosecutors and juries the inherently legislative task of determining what types of activity are so morally reprehensible that they should be punished as crimes." *United States v. Mathur*, No. 11 Cr. 312, 2012 WL 4742833, at *12 (D. Nev. Sept. 13, 2012) (citing *Nosal*, 676 F.3d at 859); (*see* OB 36). The government's silence suggests that the government has no persuasive answer.

C. The Rule of Lenity Favors the Narrow Interpretation.

Valle's opening brief showed that, to the extent the statute is ambiguous, the rule of lenity compels adopting the Narrow Interpretation. That so many courts have embraced the Narrow Interpretation is powerful evidence that, at the very least, the Broad Interpretation is not "unambiguously correct." *United States* v. *Duray*, 215

F.3d 257, 264 (2d Cir. 2000) (citations omitted). And Valle was prosecuted for conduct traditionally governed by state and administrative remedies, without any clear indication that Congress sought to federalize such conduct. Accordingly, the rule of lenity requires interpreting the CFAA in Valle's favor.

The government does not dispute that the Broad Interpretation makes a federal crime of employee misconduct like Valle's that has traditionally been regulated by state, local, and administrative laws. And the government has no answer to the 1986 Senate Report's statement that Congress did not intend to "enact as sweeping a Federal statute as possible," given its confidence in "the interests and abilities of States to proscribe and punish such offenses." S. Rep. No. 99-432, at 4, *reprinted in* 1986 U.S.C.C.A.N. at 2482. Nor does the government counter Valle's discussion of *JBCHoldings*, which rejected the Broad Interpretation because it would "ascribe to Congress an intent thus to dramatically expand federal criminal and civil jurisdiction." (OB 41 (quoting *JBC Holdings*, 931 F. Supp. 2d at 525).)

Instead, the government simply dismisses the rule of lenity, claiming that a litigant can always conjure "a more restricted construction of any given statute." (GB 39.) The rule of lenity cannot be so easily dismissed. The government's stock response about the general pleading strategies of litigants is obviously misplaced, given the many cases that have actually adopted the construction Valle urges. *See, e.g.*, *Nosal*, 676 F.3d at 862; *Miller*, 687 F.3d at 207; *Sebrite Agency, Inc. v. Platt*,

884 F. Supp. 2d 912, 917–98 (D. Minn. 2012); *Jones*, 957 F. Supp. 2d at 619. These cases show that the Narrow Interpretation is at least as plausible as the Broad Interpretation. Thus, to the extent ambiguity exists, the rule of lenity favors the Narrow Interpretation.

* * * *

In summary, the Narrow Interpretation of the CFAA is the best reading of the statute's text, especially when read in light of the statute's overall structure, history, and purpose. The Broad Interpretation, in contrast, violates basic rules of construction, transforms a computer-hacking statute into a sweeping federal Internet-policing mandate, and potentially renders the statute unconstitutional. The government invites the Court to simply apply the statute to Valle and leave all of these problems for future panels to resolve. The Court should decline this invitation.

CONCLUSION

For these reasons and those stated in Valle's opening brief, this Court should reverse the judgment of conviction and remand for entry of a judgment of acquittal.

Dated: New York, New York
April 20, 2015

Respectfully submitted,

/s/ Edward S. Zas

FEDERAL DEFENDERS OF NEW YORK, INC.
APPEALS BUREAU
52 DUANE STREET, 10TH FLOOR
NEW YORK, NEW YORK 10007
(212) 417-8742

Attorneys for Defendant-Appellant
Gilberto Valle

CERTIFICATE OF COMPLIANCE

1. This *Corrected* Reply Brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because:

it contains 6,707 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This *Corrected* Reply Brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and type style requirements of Fed. R. App. P. 32(a)(6) because:

it has been prepared in a **Times New Roman** typeface using **Microsoft Word 2013**.

Dated: April 20, 2015

/s/
Edward S. Zas

CERTIFICATE OF SERVICE

I certify that a copy of this *Corrected* Reply Brief has been served by CM/ECF and first-class mail on the United States Attorney/S.D.N.Y.; Attention: **Justin Anderson, Esq.,** Assistant United States Attorney, One St. Andrew's Plaza, New York, New York 10007.

Dated: New York, New York
April 20, 2015

/s/
Edward S. Zas