UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	No. 12-cr-847 (PGG)
GILBERTO VALLE,	:	
Defendant.	:	

DEFENDANT GILBERTO VALLE'S REPLY MEMORANDUM OF LAW IN SUPPORT OF HIS MOTION FOR A JUDGMENT OF ACQUITTAL ON COUNT TWO

David Patton
Federal Defenders of New York, Inc.
52 Duane Street, 10th Floor
New York, New York 10007
Attorney for Defendant Gilberto Valle

Of Counsel:
Julia Gatto
Robert Baum
Edward S. Zas
James A. Cohen

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Federal Statutes

Rules

Other Authorities

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	No. 12-cr-847 (PGG)
GILBERTO VALLE,	:	
Defendant.	:	

ARGUMENT

In its response brief, the government points to a handful of cases that have reached decisions that appear to adopt a "broad" interpretation of the Computer Fraud and Abuse Act ("CFAA")—an interpretation that would impose criminal liability on employees who violate their employer's policies by accessing their work computers without a valid business purpose. But the government does not actually argue that these cases are correct or even persuasive—and they plainly are not. Not one of the "broad" cases that the government cites conducts a textual analysis of the statute. Not one of those cases reviews the legislative history. And not one of those cases even cites any of the numerous court decisions on this issue. Rather, these cases are almost all unpublished decisions that simply whiffed—overlooking essentially all of the relevant legal authorities and arguments. For this reason, multiple judges in this District have rejected all of these cases as "unpersuasive." This Court should do the same.

The government also argues that the prosecution of Mr. Valle would survive under the better-reasoned cases that adopt a narrow interpretation of the CFAA. But the government's attempts to align this prosecution with the well-reasoned narrow cases simply distorts what those cases actually held. In those cases, the government (or a private plaintiff)

contended that a misbehaving employee had accessed a computer without authorization because the employee did not have a valid business purpose for accessing certain information on his employer's computer. The theory was that, under either state law or written or oral policies of the employer, the employee's authority to use the computer was limited to official business purposes. Thus, when the employee accessed the computer without an official business purpose, the access was unauthorized *ab initio*. This is the same argument the government makes here.

All of the well-reasoned and thoughtful cases correctly rejected this argument. As these decisions recognized, the CFAA is an anti-hacking statute, and it was never intended to elevate mere violations of computer use policies into federal crimes. Thus, CFAA liability is only appropriate when someone hacks into information that they had no authority to access for any purpose. The legislative history—which the government ignores completely—confirms that this is the only correct reading. Congress specifically considered the problem of misbehaving government employees and concluded that administrative sanctions, not federal criminal punishment, were the appropriate remedy. Congress wanted liability to turn on clear rules, not ambiguous questions of an employee's subjective intent. This Court should follow the well-reasoned decisions in this District and decline the government's invitation to flout Congress's clear command. The Court should enter a judgment of acquittal on count two.

I. THE GOVERNMENT'S THEORY HERE IS NO DIFFERENT THAN THE THEORY COUNTLESS COURTS HAVE CONSIDERED AND REJECTED.

A. Numerous Prior Cases Have Considered and Rejected the Exact Same Theory the Government Rehashes in This Case.

As the Ninth Circuit has explained, the CFAA's prohibition on exceeding authorized access to a computer "can be read either of two ways." *United States v. Nosal*, 676 F.3d 854, 856 (9th Cir. 2012). In particular:

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* Def.'s Mem. 5 (ECF No. 179).)

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 to send 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 numerous decisions in this District have rejected the second interpretation. The government contends that its argument today is somehow new and different, but in fact, it merely regurgitates the same theory that these persuasive decisions considered and rejected.

The government's argument is that "a necessary condition to Valle having authorization to access information about any individual was his first having an appropriate law enforcement purpose." (Gov't Mem. 44 (alteration in original).) Because Mr. Valle did not have a "law enforcement purpose" for looking up Ms. Hartigan, the government argues he had no authority to do so. This is the exact same argument made in *Nosal* and several other cases. In *Nosal*, like here, 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 contended that "[b]ecause the [employees] lacked this required purpose" at the time they accessed certain information, the employees did not have any authority to access that information. *Id.* The *en banc* Ninth Circuit rejected this argument, concluding that the prohibitions in the CFAA "apply[] to hackers," not employees who exceed their authority under an employer's computer use policies. *Id.* at 858.

The government's attempts to distinguish *Nosal* simply mischaracterize that case. The government argues that "the Ninth Circuit merely held that . . . Section 1030 cannot be used to prosecute individuals for misuse of data." (Gov't Mem. 47 (emphasis added) (citing *Nosal*, 676 F.3d at 858).) But 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 liable for accessing data without a valid business purpose, in violation of company policy. The *Nosal* court made this clear, by summarizing the issue it was deciding 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 correctly answered this question, "no." The government simply disagrees with *Nosal*'s clear holding—but the government fails to distinguish it and does not offer any presuasive reason why this Court should not follow it.[1]

The government's attempt to distinguish the other cases rest on similar mischaracterizations. *See*, *e.g.*, *United States v. Aleynikov*, 737 F. Supp. 2d 173 (S.D.N.Y. 2010). The government argues that *Aleynikov* merely held that an individual cannot be prosecuted under the CFAA for misusing information they acquire legally. (Gov't Mem. 45-46.) The government asserts that "the software engineer in *Aleynikov* . . . accessed and manipulated the contested data for a proper purpose as a necessary component of his job." (Gov't Mem. 46.)

[1] Indeed, the government's contention that concerns about prosecutions for Farmville and CNN.com are "unfounded" confirms that the government's argument is directly at odds with *Nosal*. (*See* Gov't Mem. 48.) As *Nosal* explained, if every violation of employer policies restricting computer use to official business purposes were a federal crime, whole swaths of otherwise innocuous behavior would be criminal. Employees could face criminal liability for visiting ESPN.com or www.dailysudoku.com (both examples cited in *Nosal*). *See* 676 F.3d at 860-62. On the theory the government presses today, if police officers had been told in training that they cannot use computers in the station house for personal purposes, an officer who visited CNN.com on his lunch break would be just as liable as Mr. Valle.

This miststates the facts of *Aleynikov*. The allegations in that case were that "[o]n his last day of employment at Goldman, June 5, 2009, Aleynikov copied, compressed, encrypted, and transferred to an outside server in Germany hundreds of thousands of lines of source code for the Trading System." *Aleynikov*, 737 F. Supp. 2d at 175. There was no suggestion that Aleynikov had any "proper [business] purpose" for downloading "hundreds of thousands of lines of source code" to foreign servers. Quite the contrary, it was obvious that he downloaded the code for an improper purpose, because after downloading the code, Aleynikov tried to cover his tracks by "delet[ing] his 'bash history,'" and he later tried to misappropriate the code and use it for his own benefit at a new employer. *Id.* at 175.

Contrary to the government's assertions, the prosecutor's argument in *Aleynikov* was not that Aleynikov's after-the-fact attempt to misappropriate the code at a new company was a CFAA violation. Rather, the prosecutor contended that Aleynikov had violated the CFAA the moment he accessed Goldman's source code without a valid business purpose, "in violation of . . . policies" of Goldman. *Id.* at 191. Judge Cote correctly rejected this argument. She concluded that the "broad" interpretation that "construe[s] the CFAA . . . to encompass use of a computer for an improper purpose" is "unpersuasive." As she explained, the statute does not allow courts to simply "infer that 'authorization' is automatically terminated where an individual 'exceed[s] the purposes for which access is "authorized."'" *Id.* (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)). Thus, Judge Cote squarely rejected the government's contention that access is "unauthorized" simply because an employee accessed a work computer without a valid business purpose, in violation of company policy.

Judge Holwell also rejected this argument in *University Sports Publications Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378 (S.D.N.Y. 2010). An employer argued that a

former employee had "accessed the [employer's] database 'without authorization' . . . by using the database for an improper purpose." *Id.* at 384. Like the government here, the employer tried to argue that the employee had no authority to access information outside the scope of the employee's official "job duties." *Id.* But the court held that a violation of the CFAA "requires proof that the offender entered some forbidden virtual space," by "violat[ing] limitations on his access rights." *Id.* In other words, only "circumvention of *technological* access barriers," *i.e.*, hacking, creates a CFAA violation. *Nosal*, 676 F.3d at 863 (emphasis added). Mere violations of employer policies imposing conditions or limitations on access are not enough.

B. None of the Cases the Government Cites Are Persuasive.

The cases that the government cites as supporting a "broad" interpretation of the CFAA are all unpersuasive.

The government relies heavily, for instance, on a summary order. *See United States v. Bossinger*, 311 F. App'x 512 (2d Cir. 2009). Even setting aside that summary orders have no precedential effect, *see* 2d Cir. R. 32.1.1(a), the order the government cites does not even mention the issue before the Court today. In that case, "[t]he defendant concede[d] that she accessed [a computer] in excess of her authorization." 311 F. App'x at 514. Accordingly, the Second Circuit had no occasion to even consider this issue, let alone opine on it. "It is well established that 'an argument not raised on appeal is deemed abandoned' and lost, and . . . a court of appeals will not consider the argument . . . ." *United States v. Joyner*, 313 F.3d 40, 44 (2d Cir. 2002). The fact that this issue was not discussed in *Bossinger* only confirms what numerous district courts have recognized is still the case years later: "The Second Circuit has yet to provide guidance on how 'unauthorized access' should be interpreted under the CFAA . . . ." *Advanced Aerofoil Technologies, AG v. Todaro*, No. 11-cv-9505-ALC-DCF, 2013 WL 410873 (S.D.N.Y. Jan. 30, 2013); *see also JBCHoldings NY, LLC v. Pakter*, No. 12-cv-7555 PAE, 2013

WL 1149061, at *5 (S.D.N.Y. Mar. 20, 2013) ("The Second Circuit has not squarely addressed the issue.").

The three district court cases the government cites (Gov't Mem. 48-49) also have no persuasive value. Those cases devoted little more than a sentence or two to the analysis; they overlooked the ambiguity in the statutory text, the legislative history, and the relevant case law; and they did not address how their decision was consistent with the rule of lenity. For this reason, numerous carefully reasoned opinions have considered and rejected every one of the cases the government cites. *See Aleynikov*, 737 F. Supp. 2d at 193 (rejecting all three of the district court decisions the government cites as "unpersuasive"); *JBCHoldings NY, LLC*, 2013 WL 1149061, at *5 (same); *see also Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); *Major, Lindsey & Africa, LLC v. Mahn*, No. 10-cv-4329 CM, 2010 WL 3959609, at *6 (S.D.N.Y. Sept. 7, 2010); *Playmakers Media Co.*, 725 F. Supp. 2d at 384.

Even if this Court found any merit to the cursory analysis in these cases, moreover, the rule of lenity would compel this Court to reject them. The fact that numerous judges have found that the "narrow" interpretation is the best reading of the statute demonstrates, at the very least, that there is an ambiguity in the statute. Any "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *Skilling v. United States*, 130 S. Ct. 2896, 2932 (2010) (quoting *Cleveland v. United States*, 531 U.S. 12, 25 (2000)) (internal quotation marks omitted). Accordingly, the Court must adopt the narrower view.

II. THE GOVERNMENT'S POSITION IGNORES THE LEGISLATIVE HISTORY.

The government tellingly had no response at all to the legislative history, which undermines whatever superficial appeal its arguments might otherwise have. As noted in the previous briefing, in 1986, Congress specifically deleted a provision of the statute that had imposed liability on defendants who accessed a computer with authorization, but "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). The committee report made explicit that Congress intended to avoid criminal prosecutions of government employees who simply use a computer for a subjective purpose not permitted by their employer:

> It is not difficult to envision an employee or other individual who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at. . . . The Committee believes that administrative sanctions are more appropriate than criminal punishment in such a case.

S. Rep. No. 99-432, at 7 (1986) (emphasis added), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485; *see also Nosal*, 676 F.3d at 858 n.5 (legislative history supports the narrower interpretation).

The government had no response to this legislative history. None. It simply ignored it in the evident hope that this Court would flout the congressional intent. This Court should decline the invitation.

CONCLUSION

For these reasons, the Court should enter a judgment of acquittal on count two of the indictment.

Dated: New York, New York
October 1, 2013

Respectfully submitted,

David Patton
Federal Defenders of New York

By: /s/ Julia Gatto
Julia Gatto
52 Duane Street, 10th Floor
New York, New York 10007
Attorney for Defendant Gilberto Valle

Of Counsel:
Julia Gatto
Robert Baum
Edward S. Zas
James A. Cohen