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 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

Page

STATEMENT OF JURISDICTION 1

QUESTION PRESENTED 1

STATEMENT OF THE CASE 2

A. Procedural History 2

B. Statement of Facts 3

1. The Indictment 3

2. The Evidence 4

3. The Rule 29 Motion 6

4. The Court's Sufficiency Ruling and Sentence 7

SUMMARY OF ARGUMENT 8

ARGUMENT 10

I. THE PLAIN LANGUAGE OF THE CFAA DOES NOT IMPOSE CRIMINAL LIABILITY FOR ACCESSING FOR AN IMPROPER PURPOSE A COMPUTER AND DATABASES THAT THE DEFENDANT IS AUTHORIZED TO ACCESS. 10

A. This Court Reviews the Sufficiency of the Evidence and the Meaning of the CFAA De Novo. 10

B. The CFAA Governs Unauthorized Access, Not Unauthorized Purposes. 11

C. The District Court Followed a Misguided Line of Authority That Construes the CFAA To Turn on an Individual's Purpose Rather Than His Access Authority. 18

D. The District Court Improperly Dismissed the Line of Authority Reading the CFAA Narrowly. 25

II. THE CFAA'S STATUTORY HISTORY CONFIRMS THE STATUTE'S PLAIN MEANING. 26

III. THE DISTRICT COURT'S INTERPRETATION OF THE CFAA CREATES SERIOUS CONSTITUTIONAL PROBLEMS AND CONTRAVENES THE RULE OF LENITY. 30

A. The District Court's Expansive Interpretation of the CFAA Violates the Canon of Constitutional Doubt. 31

1. The District Court's Holding Renders the Scope of § 1030 Impermissibly Unclear. 33

2. The District Court's Interpretation Invites Arbitrary and Discriminatory Enforcement. 37

B. The Rule of Lenity Compels a Narrow Reading of the CFAA. 39

CONCLUSION 42

TABLE OF AUTHORITIES

Page(s)

Cases

Advance Watch Co. v. Pennington,
No. 13 Civ. 8169, 2014 WL 5364107 (S.D.N.Y. Oct. 22, 2014) 20

Advanced Aerofoil Technologies, AG v. Todaro,
No. 11 Civ. 9505, 2013 WL 410873 (S.D.N.Y. Jan. 30, 2013).................... 20-21

Advanced Fluid Sys., Inc. v. Huber,
28 F. Supp. 3d 306 (M.D. Pa. 2014) 21

Advanced Micro Devices, Inc. v. Feldstein,
951 F. Supp. 2d 212 (D. Mass. 2013) 23, 35, 36, 38

Ajuba Int'l, L.L.C. v. Saharia,
No. 11 Civ. 12936, 2012 WL 1672713 (E.D. Mich. 2012) 21

Allard K. Lowenstein Int'l Human Rights Project v. Dep't of Homeland Security,
626 F.3d 678 (2d Cir. 2010)... 27

Allstate Ins. Co. v. Serio,
261 F.3d 143 (2d Cir. 2001)... 38

Am. Family Mut. Ins. Co. v. Rickman,
554 F. Supp. 2d 766 (N.D. Ohio 2008)... 21

Amphenol Corp. v. Paul,
993 F. Supp. 2d 100 (D. Conn. 2014), *aff'd*, 2015 WL 405610
(2d Cir. 2015) (summary order)... 20

Badaracco v. Commissioner,
464 U.S. 386 (1984) 25

Bell Aero. Servs. v. U.S. Aero Servs.,
690 F. Supp. 2d 1267 (M.D. Ala. 2010) 13, 21

Bond v. United States,
134 S. Ct. 2077 (2014) 41

Page(s)

Boos v. Barry,
485 U.S. 312 (1988) 32

Booth v. Churner,
532 U.S. 731 (2001) 28-29

Bouie v. City of Columbia,
378 U.S. 347 (1964) 36

Carnegie Strategic Design Engineers, LLC v. Cloherty,
No. 13 Civ. 1112, 2014 WL 896636 (W.D. Pa. Mar. 6, 2014) 14

Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio,
No. 09 Civ. 2751, 2010 WL 4224473 (E.D. Pa. Oct. 22, 2010) 21

Conde v. Kelly,
990 N.Y.S.2d 166 (N.Y. App. Div. 1st Dep't 2014) 40

Cranel Inc. v. Pro Image Consultants Grp., LLC,
No. 13 Civ. 766, 2014 WL 4829485 (S.D. Ohio Sept. 29, 2014) 21

Dana Ltd. v. America Axle & Mfg. Holdings, Inc.,
No. 10 Civ. 450, 2012 WL 2524008 (W.D. Mich. June 29, 2012) 18

Diamond Power Int'l, Inc. v. Davidson,
540 F. Supp. 2d 1322 (N.D. Ga. 2007) 21, 40

Dresser-Rand Co. v. Jones,
957 F. Supp. 2d 610 (E.D. Pa. 2013) 14, 25

Duncan v. Walker,
533 U.S. 167 (2001) 17

EF Cultural Travel BV v. Explorica, Inc.,
274 F.3d 577 (1st Cir. 2001) 22, 23

Facebook, Inc. v. Grunin,
No. 14 Civ. 2323, 2015 WL 124781 (N.D. Cal. Jan. 8, 2015) 33

Farrell v. Burke,
449 F.3d 470 (2d Cir. 2006) 37

Page(s)

Int'l Airport Ctrs., L.L.C. v. Citrin,
440 F.3d 418 (7th Cir. 2006).. 23

Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda,
390 F. Supp. 2d 479 (D. Md. 2005) 21, 39

JBCHoldings NY, LLC v. Pakter,
931 F. Supp. 2d 514 (S.D.N.Y. 2013)... *passim*

Jet One Grp., Inc. v. Halcyon Jet Holdings, Inc.,
No. 08 Civ. 3980, 2009 WL 2524864 (E.D.N.Y. Aug. 14, 2009)..................... 21

Kolender v. Lawson,
461 U.S. 352 (1983) 38

Kreisberg v. HealthBridge Mgmt., LLC,
732 F.3d 131 (2d Cir. 2013).. 11

Lee v. PMSI, Inc.,
No. 10 Civ. 2904, 2011 WL 1742028 (M.D. Fla. May 6, 2011)...................... 23

Leocal v. Ashcroft,
543 U.S. 1 (2004) 35

Lewis-Burke Assocs., LLC v. Widder,
725 F. Supp. 2d 187 (D.D.C. 2010) 21

Lockheed Martin Corp. v. Speed,
No. 05 Civ. 1580, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006) 38

Lurie v. Wittner,
228 F.3d 113 (2d Cir. 2000).. 31

LVRC Holdings LLC v. Brekka,
581 F.3d 1127 (9th Cir. 2009).. *passim*

Major, Lindsey & Africa, LLC v. Mahn,
No. 10 Civ. 4329, 2010 WL 3959609 (S.D.N.Y. Sept. 7, 2010)....................... 21

McNally v. United States,
483 U.S. 350 (1987) 39

Page(s)

Moskal v. United States,
498 U.S. 103 (1990) 39

Nat'l City Bank, N.A. v. Republic Mortg. Home Loans, LLC,
No. 09 Civ. 1550, 2010 WL 959925 (W.D. Wash. Mar. 12, 2010) 21

NetApp, Inc. v. Nimble Storage, Inc.,
No. 13 Civ. 5058, 2014 WL 1903639 (N.D. Cal. May 12, 2014) 33

Nexans Wires S.A. v. Sark-USA, Inc.,
166 Fed. App'x 559 (2d Cir. 2006).. 18

Orbit One Commc'ns, Inc. v. Numerex Corp.,
692 F. Supp. 2d 373 (S.D.N.Y. 2010)... 18, 21, 40

Poller v. BioScrip, Inc.,
974 F. Supp. 2d 204 (S.D.N.Y. 2013).. 20

Power Equipment Maintenance, Inc. v. AIRCO Power Services, Inc.,
953 F. Supp. 2d 1290 (S.D. Ga. 2013)... 23

Pulte Homes, Inc. v. Laborers' Int'l Union of N. Amer.,
648 F.3d 295 (6th Cir. 2011)... 20

ReMedPar, Inc. v. AllParts Med., L.L.C.,
683 F. Supp. 2d 605 (M.D. Tenn. 2010)... 21

Sebelius v. Cloer,
133 S. Ct. 1886 (2013) 11

Shamrock Foods Co. v. Gast,
535 F. Supp. 2d 962 (D. Ariz. 2008)... 21, 24

Skilling v. United States,
561 U.S. 358 (2010) 37

Thibodeau v. Portuondo,
486 F.3d 61 (2d Cir. 2007)... 32

Trademotion, LLC v. Marketcliq, Inc.,
857 F. Supp. 2d 1285 (M.D. Fla. 2012).. 23

Page(s)

United States v. Al Kassar,
660 F.3d 108 (2d Cir. 2011) 17

United States v. Aleynikov,
737 F. Supp. 2d 173 (S.D.N.Y. 2010) .... *passim*

United States v. Auernheimer,
748 F.3d 525 (3d Cir. 2014) 20

United States v. Coplan,
703 F.3d 46 (2d Cir. 2012) 10

United States v. Dauray,
215 F.3d 257 (2d Cir. 2000) 27

United States v. Demerritt,
196 F.3d 138 (2d Cir. 1999) 25

United States v. Desposito,
704 F.3d 221 (2d Cir. 2013) 11

United States v. Drew,
259 F.R.D. 449 (C.D. Cal. 2009) 33, 34, 35, 38

United States v. John,
597 F.3d 263 (5th Cir. 2010) 16, 23, 24

United States v. Kleiner,
765 F.3d 155 (2d Cir. 2014) 15

United States v. Kozeny,
541 F.3d 166 (2d Cir. 2008) 17

United States v. Lanier,
520 U.S. 259, 266-67 (1997) 31

United States v. Newman,
773 F.3d 438 (2d Cir. 2014) 10

United States v. Nosal,
676 F.3d 854 (9th Cir. 2012) .... *passim*

Page(s)

United States v. Perez,
575 F.3d 164 (2d Cir. 2009) 10

United States v. Rodriguez,
628 F.3d 1258 (11th Cir. 2010) 22, 23

United States v. Stevens,
559 U.S. 460 (2010) 38

United States v. Teague,
646 F.3d 1119 (8th Cir. 2011) 22

United States v. Valle,
301 F.R.D. 53 (S.D.N.Y. 2014) .... *passim*

University Sports Publications Co. v. Playmakers Media Co.,
725 F. Supp. 2d 378 (S.D.N.Y. 2010) 21

US Bioservices Corp. v. Lugo,
595 F. Supp. 2d 1189 (D. Kan. 2009) 26

WEC Carolina Energy Solutions LLC v. Miller,
687 F.3d 199 (4th Cir. 2012) 20, 23, 26

Wentworth-Douglass Hosp. v. Young & Novis Professional Ass'n,
No. 10 Civ. 120, 2012 WL 2522963 (D.N.H. June 29, 2012) 23

Westbrook Techs., Inc. v. Wesler,
No. 09 Civ. 360, 2010 U.S. Dist. LEXIS 70901 (D. Conn. July 15, 2010) 21

Whitman v. American Trucking Ass'ns,
531 U.S. 457 (2001) 39

Statutes

18 U.S.C. § 1030 .... *passim*

18 U.S.C. § 1030(a)(1) 14

18 U.S.C. § 1030(a)(2) .... *passim*

18 U.S.C. § 1030(a)(2)(B) .... *passim*

Page(s)

18 U.S.C. § 1030(a)(2)(C) 15, 35

18 U.S.C. § 1030(a)(3) 28, 29

18 U.S.C. § 1030(a)(4) 14-15, 19

18 U.S.C. § 1030(a)(7) 14-15

18 U.S.C. § 1030(e)(2)(B) 15

18 U.S.C. § 1030(e)(6) 2, 12, 24,29

18 U.S.C. § 1030(e)(8) 17, 18

18 U.S.C. § 1030(e)(11) 18

18 U.S.C. § 1201(c) 2, 3

18 U.S.C. § 3231 1

28 U.S.C. § 1291 1

Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 .... 28, 29

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 27

Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 28

N.Y. Penal Law §195.00[1] 5, 39-40

Other Authorities

Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Available Internet Websites*, 63 Md. L. Rev. 320 (2004) 22

H.R. Rep. No. 98-894 (1984) 30

Page(s)

Hon. John M. Walker, Jr., *Judicial Tendencies in Statutory Construction: Differing Views on the Role of the Judge*, 58 N.Y.U. Annual Survey of Am. L. 203 (2001) 27

Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010).................... 22

Orin S. Kerr, *Cybercrimes' Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596 (2003) 30

Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 Harv. L. Rev. 751 (2013) 36-37

S. Rep. No. 99-432 (1986) 29, 40

S. Rep. No. 104-357 (1996) 29-30

STATEMENT OF JURISDICTION

Defendant-Appellant Gilberto Valle appeals from a final judgment entered on November 14, 2014, in the United States District Court for the Southern District of New York (Hon. Paul G. Gardephe). Valle was convicted, following a jury trial, of one count of improperly accessing a computer, in violation of 18 U.S.C. § 1030(a)(2)(B), a misdemeanor. The court sentenced him to 12 months in custody, one year of supervised release, and a $25 special assessment.

A notice of appeal was timely filed on November 20, 2014. This Court has jurisdiction under 28 U.S.C. § 1291. The district court had jurisdiction under 18 U.S.C. § 3231.

QUESTION PRESENTED

The Computer Fraud and Abuse Act ("CFAA"[1]) imposes civil and criminal liability on, *inter alia*, any person who "intentionally accesses a computer without authorization or exceeds authorized access … and thereby … obtains information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). The statute does not define the term "without authorization," but does define "exceeds authorized access" to mean "to access a computer with authorization and

[1] Technically speaking, the CFAA was a 1986 amendment to 18 U.S.C. § 1030 *et seq.*, but the common convention, followed here, is to refer to § 1030 as a whole as the CFAA.

to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The statute formerly covered people who use their authorized computer access "for purposes to which such authorization does not extend," but Congress deleted this language in 1986.

In this case, the New York City Police Department ("NYPD") issued police officer Gilberto Valle a laptop computer and log-in credentials that specifically authorized him to access various law enforcement databases. But the government alleged that Valle violated the CFAA when he used that access to obtain information about a friend because NYPD policy limited computer use to official law enforcement business.

The question presented is whether Valle's CFAA conviction should be reversed because the statute does not apply to an employee who violates his employer's computer-use policy by accessing information for personal purposes, when he is authorized to access that same information for professional purposes.

STATEMENT OF THE CASE

A. Procedural History

Following a 13-day trial, a jury in the Southern District of New York found Valle guilty of both counts of a two-count indictment: conspiracy to commit kidnapping, in violation of 18 U.S.C. § 1201(c) (the "Conspiracy Count"), and improperly accessing a computer, a misdemeanor, in violation of the CFAA, 18

U.S.C. § 1030(a)(2)(B) (the "CFAA Count"). After trial, Judge Gardephe entered a judgment of acquittal on the Conspiracy Count, but held the evidence sufficient to support the jury's guilty verdict on the CFAA Count.[2] *See United States v. Valle*, 301 F.R.D. 53, 59, 109-11 (S.D.N.Y. 2014); A. 121, 127, 225-38.[3] The court sentenced Valle to the statutory maximum term of 12 months of imprisonment, one year of supervised release, and a $25 special assessment. A. 261-66.

B. Statement of Facts

1. The Indictment

On November 15, 2012, a federal grand jury returned an indictment charging Valle, a former NYPD police officer, with two counts. A. 37-40. The first count, not at issue in this appeal, charged Valle with conspiracy to commit kidnapping, in violation of 18 U.S.C. § 1201(c). A. 37-38. The second count charged Valle with violating the CFAA by improperly accessing his NYPD computer and thereby obtaining information from a federal law enforcement database. A. 38-39. Specifically, the CFAA Count charged:

> On or about May 31, 2012, … the defendant … intentionally and knowingly accessed a computer without authorization and exceeded authorized access and thereby obtained information from a department and agency of the United States, to wit, VALLE accessed, and obtained

[2] The government has appealed the district court's disposition of the Conspiracy Count. *See United States v. Valle*, No. 14-2710-cr.

[3] "A." refers to the Appendix; "GX" refers to the government's trial exhibits.

> information from, the federal National Crime Information Center database, without authorization, and outside the scope of his authority.
>
> (Title 18, United States Code, Sections 1030(a)(2)(B).)

A. 38-39.

2. The Evidence

The trial evidence, viewed in the light most favorable to the government, allowed the jury to find the following facts:

Valle was a police officer with the NYPD from 2006 until the time of his arrest in October 2012. A. 42, 129. In that role, Valle received an NYPD laptop computer to access from his patrol car. A. 225. The NYPD issued Valle a username and password that enabled him to access the computer and run searches across various law enforcement databases, including the federal National Crime Information Center ("NCIC") database. A. 51, 53-55, 90, 225.

Valle attended computer training classes for NYPD officers in 2006 and 2010. A. 48-49, 225-26. At the 2010 training, the NYPD gave a PowerPoint presentation stating that NYPD computer resources may be used only "in the course of [an authorized user's] official duties and responsibilities." A. 61, 226; GX 210C. Valle was told that use of NYPD computers for "non-work related purposes w[as] improper and illegal," and against NYPD policy. A. 62, 70, 226. Valle was advised that "unauthorized use of criminal history record information" may result in "arrest, prosecution, termination of employment and fines up to $10,000." A. 62. The NYPD presentation listed at least nine different New York State criminal statutes under which an officer could be prosecuted for misconduct relating to computers. A. 62; GX 210C; *see*, *e.g.*, N.Y. Penal Law §195.00[1] (criminalizing "official misconduct" by a public servant).

On May 31, 2012, Valle used his patrol-car computer to search the name "Maureen Hartigan," a friend of his from high school. A. 44-45, 110-20 (GX 616E). The computer ran the name through several law enforcement databases, including the federal NCIC database, all of which contain confidential information about people. A. 45-46, 225. The search returned information from the NCIC database indicating that no active warrants existed for Hartigan and that she had no criminal record. A. 44-46, 110-20 (GX 616E), 226. The search also returned information from the New York State Department of Motor Vehicles indicating Hartigan's address and other basic information contained on her driver's license. A. 110-20 (GX 616E); 226.

The evidence did not show that Valle had a work-related purpose for this search. A. 129. Nor did it show that he did anything with the information he obtained. A. 236. There was no evidence, for example, that Valle used the information to further the alleged kidnapping conspiracy charged in Count One or that he ever told anyone he had conducted a search for Hartigan on his work computer or even had access to law enforcement databases. A. 159. And, as Judge Gardephe recognized, the government did not contend that Hartigan was a target of the alleged kidnapping conspiracy. A. 128-29. This was the only improper search charged in the CFAA Count.

It was undisputed at trial that Valle was an authorized user of the NYPD computer system. A. 228. It was also undisputed that the NYPD had authorized Valle to access the NCIC database from his patrol-car computer, subject to NYPD policy. A. 228-29. What made his conduct a federal crime under the CFAA, according to the government, was not his otherwise authorized access, but his purpose (or lack thereof): he lacked a law enforcement justification for the search, as required by NYPD rules.

3. The Rule 29 Motion

Defense counsel moved orally for a judgment of acquittal on both counts at the close of the government's case. With respect to the CFAA Count, counsel argued that "Valle was an authorized user of a system and [that] the statute was really essentially [meant] to cover people who are hackers who hack into a system." A. 96-97. The government replied that it knew of "absolutely no legal basis for this argument whatsoever." A. 104. The district court reserved decision until after the verdict.

The court instructed the jurors, without objection, that they could convict Valle of the CFAA Count if they found beyond a reasonable doubt that he had "accessed a computer with authorization, but that he exceeded his authority in accessing the information in question." A. 108-09.[4] On March 12, 2013, the jury found Valle guilty of both counts.

4. The Court's Sufficiency Ruling and Sentence

Following extensive post-trial briefing, the district court granted Valle's motion for a judgment of acquittal (and conditionally granted a new trial) on the Conspiracy Count. *Valle*, 301 F.R.D. at 59; A. 127. But the court sustained his conviction under the CFAA. *Id.* Judge Gardephe rejected Valle's argument that a defendant violates § 1030(a)(2)(B) of the CFAA "only when he accesses information that [he] is not entitled to access for *any* purpose—not when the defendant accesses information for personal purposes, in violation of employer policies or regulations limiting computer use to official purposes or official business." *Valle*, 301 F.R.D. at 109 (emphasis in original); A. 228. Instead, the court held that Valle's "conduct fits the definition of 'exceeds authorized access'" because he "had no valid law enforcement reason" to use his work computer to search Ms. Hartigan's name. *Valle*, 301 F.R.D. at 111; A. 228-29.

[4] The jury also had to find that Valle obtained information from the NCIC database, but that was not disputed. A. 109.

On November 12, 2014, the court sentenced Valle to 12 months in custody—he had already served more than 20 months, much of it in solitary confinement—one year of supervised release, and a $25 special assessment. A. 261-66.

SUMMARY OF ARGUMENT

I. Valle's CFAA conviction must be reversed because the NYPD authorized him to access his patrol-car computer to obtain information from the federal NCIC database. This undisputed fact means that he did not "exceed[] authorized access" within the narrow meaning of the statute. The district court sustained Valle's conviction because, in the case of Maureen Hartigan, Valle accessed the information for an improper, *i.e.*, personal, purpose. But liability under the CFAA does not turn on the purpose for which an individual uses his authorized computer access. By its plain text, the CFAA applies to what is colloquially known as "hacking"—the accessing of data or files on a computer that a person is not authorized to access for any purpose. Valle may have breached his duty of loyalty to the NYPD and violated terms of his employment by putting his authorized computer access to personal use. But Valle never used his access to obtain any information he was not entitled to obtain. Thus, the district court erred by conflating Valle's purpose for using his NYPD computer with his unauthorized "access" to it, and Valle's CFAA conviction therefore cannot stand.

This Court has not yet decided the meaning and scope of the CFAA's term "exceeds authorized access," and other courts are split. The Fourth and Ninth Circuits, and an increasing number of district courts, take a cautious and well-reasoned approach that construes the CFAA narrowly to penalize only those who exceed their authorized access, not those who use their access for an improper purpose. The district court, however, relied on a conflicting line of authority that construes the CFAA broadly. This Court should follow the narrow approach and construe the CFAA so that liability turns on the clear rules set forth in the statute's text, rather than on (often vague) rules set forth in employer computer-use policies, or on nebulous questions concerning why an employee used a computer.

II. The CFAA's statutory history—which the district court did not consider—confirms that the narrow reading of the statute is correct. In 1986, Congress specifically amended the CFAA to delete all references to a user's "purposes." As a number of courts have recognized, the amendment thus eliminated exactly the type of purpose-based liability upon which Valle's conviction rests.

III. To the extent the statute is unclear, the rule of constitutional doubt (also known as the rule of constitutional avoidance) requires rejecting the district court's interpretation of the CFAA. The court's endorsement of purpose-based liability raises serious questions about the statute's vagueness. That is because the court's construction of the statute makes criminality turn on the vagaries of a website's terms of use or a company's computer-use policy. Those usage policies are often opaque, protean, and unread. Accordingly, ordinary people typically have no reasonable way of knowing whether their conduct violates a computer-use policy, and, therefore, no way to know what conduct constitutes the federal crime of "exceed[ing] authorized access" under the district court's broad interpretation. For that same reason, the court's interpretation invites arbitrary and discriminatory enforcement by the government. Finally, the rule of lenity further compels the narrower understanding of the CFAA.

ARGUMENT

I. THE PLAIN LANGUAGE OF THE CFAA DOES NOT IMPOSE CRIMINAL LIABILITY FOR ACCESSING FOR AN IMPROPER PURPOSE A COMPUTER AND DATABASES THAT THE DEFENDANT IS AUTHORIZED TO ACCESS.

A. This Court Reviews the Sufficiency of the Evidence and the Meaning of the CFAA De Novo.

This Court reviews the sufficiency of the evidence de novo. *See, e.g.*, *United States v. Newman*, 773 F.3d 438, 451 (2d Cir. 2014). The test is whether "any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Coplan*, 703 F.3d 46, 62 (2d Cir. 2012). The Court must compare the "[g]overnment's proof against the statutory elements, properly understood." *United States v. Perez*, 575 F.3d 164, 167 (2d Cir. 2009).

The district court's interpretation of the CFAA is likewise reviewed de novo. *See*, *e.g.*, *Kreisberg v. HealthBridge Mgmt., LLC*, 732 F.3d 131, 137 (2d Cir. 2013).

B. The CFAA Governs Unauthorized Access, Not Unauthorized Purposes.

In construing a statute, this Court "begin[s] with the plain language, giving all undefined terms their ordinary meaning." *United States v. Desposito*, 704 F.3d 221, 226 (2d Cir. 2013) (citations omitted). If the statutory language is unambiguous, and "the statutory scheme is coherent and consistent," the Court's interpretive inquiry must cease, and the statute must be enforced according to its terms. *Sebelius v. Cloer*, 133 S. Ct. 1886, 1895 (2013).

The CFAA, 18 U.S.C. § 1030(a)(2)(B), provides that: "Whoever … intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any department or agency of the United States … shall be punished as provided in … this section."

This provision, therefore, penalizes two distinct types of computer trespass, or "hacking" scenarios: (1) when a person "intentionally accesses a computer without authorization;" and (2) when a person who has permission to access a computer "exceeds authorized access." 18 U.S.C. § 1030(a)(2)(B).[5]

The plain meaning of both prongs is that liability turns on whether a person was authorized to access the particular information at issue, not the purposes for which the person did so, or the use, if any, the person made of the information. Congress's definition of "exceeds authorized access" makes this clear: "[t]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter *information* in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (emphasis added). Under this definition, the purpose of access is irrelevant—what matters is whether the person was "entitled … to obtain" the information in question.

Suppose, then, that Acme Company has a computer-use policy governing databases A and B, both found on the same computer. The policy forbids lower-level employees from accessing database A for any purpose because it contains highly confidential information. The same policy allows lower-level employees to access database B, but for professional purposes only, with the expectation that employees use that database routinely as part of their employment. Under that policy, a lower-

[5] The government admitted that Valle had authorization to access his computer, thus making the "without authorization" prong of 18 U.S.C. § 1030(a)(2)(B) irrelevant. *Valle*, 301 F.R.D. at 111 n.62; A. 227 n.62.

level employee who accesses database A thereby "exceeds authorized access" and violates the CFAA because he was not entitled to access that information under any circumstance whatsoever. This result makes sense under the statute because the employee effectively "hacked" or "trespassed" into database A.

But an employee who accesses database B for personal instead of professional purposes would not violate the CFAA. He may be fired for violating Acme's computer-use policy, and face actions for breach of contract or misappropriation. Yet, because the employee was "entitled to obtain" and use the information in database B, he cannot be prosecuted under the CFAA. That follows because "'[e]xceeds authorized access' should not be confused with exceeds authorized use." *Bell Aero. Servs. v. U.S. Aero Servs.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010).

The district court, however, did just that, confusing Valle's "authorized access" to his NYPD computer with his "unauthorized use" of that access. Specifically, Judge Gardephe held that: "[a]lthough Valle—as an NYPD officer—*was authorized to access* the [NYPD] system and thereby *perform queries* of the associated databases, including the NCIC database, he was not *authorized to input a query regarding Hartigan's name*, because he had no valid law enforcement reason to do so." *Valle*, 301 F.R.D. at 111 (emphasis added); A. 228-29. The error here is pronounced: the district court mistook Valle's unauthorized use (inputting a query of Hartigan's name without having a law enforcement reason) for unauthorized "access," ignoring the determinative fact that Valle was "authorized to access" the information he obtained. This mistake was straightforward, for it was undisputed at trial that the NYPD authorized Valle to access its computers to obtain exactly the sort of information about private citizens that Valle obtained about Hartigan. A. 91-94.

Valle, of course, violated NYPD computer-use policy. But mere violations of *usage* conditions on access are not enough under the CFAA. If they were, the CFAA would elevate every violation of workplace policy prohibiting use of its "computer system for anything other than business purposes into a violation of the CFAA." *Carnegie Strategic Design Engineers, LLC v. Cloherty*, 2014 WL 896636, at *9 (W.D. Pa. Mar. 6, 2014). The CFAA does no such thing, and the district court erred by reading Valle's "intent … and use of the information into the CFAA despite the fact that the statute narrowly governs access, not use." *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 619 (E.D. Pa. 2013); *see also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-35 (9th Cir. 2009).

The district court's theory of liability is particularly implausible given the CFAA's overall structure. In addition to § 1030(a)(2)(B), "exceeds authorized access" appears in four other provisions of the statute. *See* 18 U.S.C. § 1030(a)(1), (2), (2)(C), (4), & (7). The interpretation of this phrase in § 1030(a)(2)(B) must apply across the statute, as "identical words used in different parts are intended to have the same meaning." *United States v. Kleiner*, 765 F.3d 155, 159 (2d Cir. 2014) (internal citation omitted).

One of these provisions in particular, § 1030(a)(2)(C), makes it a federal crime to "exceed[] authorized access" to "obtain … information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). A "protected computer" includes any computer connected to the Internet. *See* 18 U.S.C. § 1030(e)(2)(B) ("[T]he term 'protected computer' means a computer … which is used in or affecting interstate or foreign commerce or communication"); *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (Kozinski, C.J.) (en banc). As a result, the district court's imposition of purpose-based liability on Valle under § 1030(a)(2)(B) extends through § 1030(a)(2)(C) not only to the millions of employees subject to computer-use policies at work, but also to the many more millions who use the Internet at home every day. Under the district court's sweeping interpretation, terms of use for virtually every workplace computer and Internet website would have the force of federal criminal law.

That broad interpretation of the CFAA leads to results that Congress could not have intended. For example, under the court's reading of the CFAA, someone who misrepresents his height and weight on a dating website, which violates the website's terms of use, would be liable under the CFAA for "exceed[ing] authorized access," just like someone who hacks into the profiles of other users to read their intimate conversations. *See Nosal*, 676 F.3d at 862 (noting that, under a broad reading of the CFAA, "describing yourself [on a dating website] as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit"). Likewise, a law clerk who improperly uses the Court's Westlaw account to see if his law school note has been cited would be a criminal, just like someone who breaks into his co-clerk's email account maintained on the same server. As these examples show, the court's interpretation of the CFAA cannot distinguish between minor computer dalliances and the kind of inherently wrongful hacking the statute was meant to cover.

Further proof that Judge Gardephe's interpretation misreads § 1030 is that it collapses the two distinct prongs of the CFAA—accessing a computer "without authorization" on the one hand, and "exceed[ing] authorized access" on the other—thus creating surplusage. If an impermissible purpose revokes authorization "*ab initio*," as the district court here stated (*Valle*, 301 F.R.D. at 111; A. 229), then any computer use with an improper purpose is necessarily both "without authorization" and in "exce[ss] [of] authorization." *See United States v. Aleynikov*, 737 F. Supp. 2d 173, 193 (S.D.N.Y. 2010) (criticizing *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010), for "improperly infer[ring] that 'authorization' is automatically terminated where an individual 'exceeds *the purposes* for which access is "authorized."'") (emphasis in original). The district court reasoned that Valle "*was* *not authorized* to input a query regarding Hartigan's name, because he had no valid law enforcement reason to do so," and, therefore, "Valle's conduct fits the definition of '*exceeds authorized access*.'" *Valle*, 301 F.R.D. at 111 (emphasis added); A. 228-29. This reasoning renders the distinct statutory terms "without authorization" and "exceeds authorized access" redundant, in violation of basic rules of interpretation. *See United States v. Kozeny*, 541 F.3d 166, 171 (2d Cir. 2008) ("Statutory enactments should … be read so as 'to give effect, if possible, to every clause and word of a statute.'") (quoting *Duncan v. Walker*, 533 U.S. 167, 174 (2001)); *see also United States v. Al Kassar*, 660 F.3d 108, 124 (2d Cir. 2011).

The CFAA's damages provisions also underscore the district court's error. The CFAA authorizes recovery in some cases for "damage" or "loss." The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). It further defines "loss" as "a reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). These definitions, by focusing on physical damage to computer systems, are "inconsistent or in tension with a broader interpretation of improper 'access'" beyond conduct equivalent to computer hacking. *Orbit One*

Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385-86 (S.D.N.Y. 2010) (citing 18 U.S.C. § 1030(e)(8)-(11)); *see also Nexans Wires S.A. v. Sark-USA, Inc.*, 166 Fed. App'x 559, 563 (2d Cir. 2006) (summary order) (holding that similar loss provisions exclude losses incurred as a result of plaintiff's misuse of proprietary information).

C. The District Court Followed a Misguided Line of Authority That Construes the CFAA To Turn on an Individual's Purpose Rather Than His Access Authority.

In basing Valle's liability on his subjective purpose, the district court sided with several courts that have construed § 1030 broadly, and against several others that have interpreted it narrowly. The broad interpretation, however, betrays the CFAA's text by conflating unauthorized computer access with unauthorized use of information. This Court should follow the persuasive and "growing number of cases [that] are adopting the narrow view." *Dana Ltd. v. America Axle & Mfg. Holdings, Inc.*, 2012 WL 2524008, at *4 (W.D. Mich. June 29, 2012).

The narrow view reads "exceeds authorized access" to refer only to someone who is authorized to access certain information but accesses other information beyond that authorization. *See, e.g.*, *Brekka*, 581 F.3d at 1133.

The Ninth Circuit's en banc decision in *Nosal*, written by Chief Judge Kozinski, represents the narrow reading. There, the government charged David Nosal with aiding and abetting his former coworkers in "exceed[ing their] authorized access" with intent to defraud. *See* 18 U.S.C. § 1030(a)(4); *Nosal*, 676 F.3d at 856. After leaving his employer (Korn/Ferry, an executive search firm), Nosal convinced his former coworkers to help him start a competing business. *Id.* While these coworkers were still employed at Korn/Ferry, they downloaded confidential information from a company database and gave it to Nosal. This violated company policy limiting use of its database "for work on Korn/Ferry business only." *Id.* at 856 n.1.

The government argued in *Nosal* that this conduct violated § 1030(a)(4) because the 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 asserted that "[b]ecause the [employees] lacked this required business purpose," they did not have any authority to access that information. *Id.* The *en banc* Ninth Circuit rejected this argument, ruling that the employees "had permission to access the company database and obtain the information contained within," and that the phrase "exceeds authorized access" only "refer[s] to data or files on a computer that one is not authorized to access." 676 F.3d at 857, 864. The court emphasized the CFAA's anti-hacking focus, which does "not extend to violations of use restrictions," like those alleged against the employees. *Id.* at 858. *Nosal* thus concluded that CFAA liability turns on the circumvention of "technological access barriers," not breaches of "use restrictions." *Id.* at 864.

Faced with the same argument from a private plaintiff, the Fourth Circuit agreed with *Nosal*'s "narrow reading of the terms 'without authorization' and 'exceeds authorized access'" to apply only "when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access." *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012).[6] In this circuit, Judges Engelmayer and Cote, among others,[7] have rebuffed similar purpose-based liability theories. *See JBCHoldings NY,*

[6] Although the Sixth Circuit has not squarely decided the issue, *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Amer.*, 648 F.3d 295, 304 (6th Cir. 2011), indicates that it would follow the narrow view, as it relied heavily on *Brekka* in defining "without authorization." The Third Circuit likewise has yet to weigh in, but has suggested in *dicta* that it favors the narrow approach. *See United States v. Auernheimer*, 748 F.3d 525, 534 n.5 (3d Cir. 2014) ("We also note that in order to be guilty of accessing 'without authorization, or in excess of authorization' under New Jersey law, the Government needed to prove that [defendants] circumvented a code- or password-based barrier to access.").

[7] *See also Advance Watch Co. v. Pennington*, 2014 WL 5364107, at *4 (S.D.N.Y. Oct. 22, 2014); *Amphenol Corp. v. Paul*, 993 F. Supp. 2d 100, 109 (D. Conn. 2014), *aff'd*, 2015 WL 405610 (2d Cir. 2015) (summary order); *Poller v. BioScrip, Inc.*, 974 F. Supp. 2d 204, 232 (S.D.N.Y. 2013); *Advanced Aerofoil Technologies, AG v. Todaro*, 2013 WL 410873 (S.D.N.Y. Jan. 30, 2013); *Orbit One Commc'ns*, 692 F. Supp. 2d at 385; *Major, Lindsey & Africa, LLC v. Mahn*, 2010 WL 3959609, at *6 (S.D.N.Y. Sept. 7, 2010); *University Sports Publications Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378 (S.D.N.Y. 2010); *Westbrook Techs., Inc. v. Wesler*, 2010 U.S. Dist. LEXIS 70901, at *13 (D. Conn. July 15, 2010); *Jet One Grp., Inc. v. Halcyon Jet Holdings, Inc.*, 2009 WL 2524864, at *5 (E.D.N.Y. Aug. 14, 2009).

LLC v. Pakter, 931 F. Supp. 2d 514, 521 (S.D.N.Y. 2013) (Engelmayer, J.) (refusing to expand the CFAA to penalize an "employee [who] has permission to access certain information and then uses that information for an improper purpose"); *Aleynikov*, 737 F. Supp. 2d at 191 (Cote, J.) (holding that the CFAA fails to support the "infer[ence] that 'authorization' is automatically terminated where an individual 'exceed[s] the purposes for which access is "authorized."'") (quoting *Brekka*, 581 F.3d at 1133). And many other courts[8] and legal scholars[9] have further endorsed the narrow interpretation.

[8] *See, e.g.*, *Advanced Fluid Sys., Inc. v. Huber*, 28 F. Supp. 3d 306, 329 (M.D. Pa. 2014); *Cranel Inc. v. Pro Image Consultants Grp., LLC*, 2014 WL 4829485, at *7-8 (S.D. Ohio Sept. 29, 2014); *Ajuba Int'l, L.L.C. v. Saharia*, 2012 WL 1672713, at *11-12 (E.D. Mich. 2012); *Lewis-Burke Assocs., LLC v. Widder*, 725 F. Supp. 2d 187, 192 (D.D.C. 2010); *Nat'l City Bank, N.A. v. Republic Mortg. Home Loans, LLC*, 2010 WL 959925, at *2 (W.D. Wash. Mar. 12, 2010); *Bell Aero. Servs*, 690 F. Supp. 2d at 1272; *ReMedPar, Inc. v. AllParts Med., L.L.C.*, 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010); *Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio*, 2010 WL 4224473, at *5 (E.D. Pa. Oct. 22, 2010); *Am. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766, 771 (N.D. Ohio 2008); *Shamrock Foods*, 535 F. Supp. 2d at 965; *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342-43 (N.D. Ga. 2007); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 498-99 (D. Md. 2005).

[9] *See, e.g.*, Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1561 (2010); Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Available Internet Websites*, 63 Md. L. Rev. 320, 323-24, 331 (2004).

The district court here, however, declined to read § 1030 narrowly, and instead followed other courts that take an expansive view of the statute. *Valle*, 301 F.R.D. at 111 (collecting cases); A. 229-32, 236.[10] These decisions treat an individual's improper purpose as enough for CFAA liability.

The First Circuit, for example, applied the CFAA to punish an employee on the basis of his intent to directly compete with his employer, in violation of a confidentiality agreement. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581-82 (1st Cir. 2001). The Eleventh Circuit concluded that a Social Security Administration employee exceeded his authorized access in accessing databases for nonbusiness reasons, which the agency's policies prohibited. *United States v. Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010). The Fifth Circuit upheld a defendant's CFAA conviction on the basis of her intent to commit fraud in accessing her employer's databases. *John*, 597 F.3d at 271-72. Finally, the Seventh Circuit held that an employee who "scrubbed" his work computer after resolving to quit but before doing so, accessed that computer without authorization because his purpose in scrubbing it was adverse to his employer. *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440

[10] The district court's reliance on *United States v. Teague*, 646 F.3d 1119 (8th Cir. 2011), was misplaced because the defendant there did not contest that accessing information for an improper purpose could violate the CFAA. The Eighth Circuit's decision was limited to rejecting the defendant's argument that there was insufficient evidence that she was the person who accessed President Obama's student-loan records. *Id.* at 1122.

F.3d 418, 420-21 (7th Cir. 2006). The Seventh Circuit reasoned that the defendant's adverse purpose breached his duty of loyalty to his employer and, therefore, terminated his authority to access the computer. *Id.*

These four decisions just discussed have been roundly discredited by more carefully reasoned authority, including *Nosal*, *Miller*, and *Aleynikov;* even courts within those circuits have been reluctant to follow them.[11] The decisions are not persuasive because they depart from the statutory text, which "target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation." *Nosal,* 676 F.3d at 863 (quoting *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008)). As Judge Engelmayer has explained,

[11] *See, e.g.*, *Power Equipment Maintenance, Inc. v. AIRCO Power Services, Inc.*, 953 F. Supp. 2d 1290 (S.D. Ga. 2013) (noting that, notwithstanding *Rodriguez*, "district courts in this circuit have also continued to find that simply accessing an employer's computer for nonbusiness reasons is insufficient to support a claim under the CFAA") (citing *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d 1285, 1291 (M.D. Fla. 2012); *Brekka*, 581 F.3d at 1133; *Lee v. PMSI, Inc.*, 2011 WL 1742028, at *2 (M.D. Fla. May 6, 2011)); *Advanced Micro Devices, Inc. v. Feldstein*, 951 F. Supp. 2d 212, 218 (D. Mass. 2013) (claiming that the First Circuit "has not clearly articulated its position on this issue," after noting that "[a]s between a broad definition that pulls trivial contractual violations into the realm of federal criminal penalties, and a narrow one that forces the victims of misappropriation and/or breach of contract to seek justice under state, rather than federal, law, the prudent choice is clearly the narrower definition"); *Wentworth-Douglass Hosp. v. Young & Novis Professional Ass'n*, 2012 WL 2522963, at *3 (D.N.H. June 29, 2012) (concluding that "in light of the court of appeals' limited holdings in its *EF Cultural* opinions, the court agrees that the better (and more reasonable) interpretation of the phrase 'exceeds authorized access' in the CFAA is a narrow one").

"exceeds authorized access" cannot "turn on the employee's *purpose* in making use of his permitted access to the information," because that reading "effectively add[s] to the statute a subjective intent requirement that Congress did not impose." *JBCHoldings*, 931 F. Supp. 2d at 523 (emphasis added).

The Fifth Circuit, for example, announced with little analysis "that access may be exceeded [under the CFAA] if the purposes for which access has been given are exceeded." *John*, 597 F.3d at 272. The court even asserted that an employee violates the CFAA whenever she violates "*expected norms of intended use* or *the nature of the relationship* established between the computer owner and the user." *Id.* at 271 (emphasis added). This is an extraordinary expansion of statutory language that focuses on whether "the accesser is . . . entitled . . . to obtain" the "information," 18 U.S.C. § 1030(e)(6), not her purpose for obtaining it, and certainly not the "expected norms of intended use" or "nature of the relationship"—whatever those might be.

This Court should decline to convert a statute that punishes conduct "tantamount to trespass in a computer" into a far broader one punishing everyday violations of computer-use policies. *Dresser-Rand*, 957 F. Supp. 2d at 619; *see United States v. Demerritt*, 196 F.3d 138, 143 (2d Cir. 1999) ("[O]ur role as a court is to apply the provision as written, not as we would write it.") (citing *Badaracco v. Commissioner*, 464 U.S. 386, 398 (1984)).

D. The District Court Improperly Dismissed the Line of Authority Reading the CFAA Narrowly.

The district court dismissed the cases relied on by Valle as distinguishable "disloyal employee misappropriation and misuse cases," not relevant here insofar as "the Government has not alleged that Valle made any use of the information he obtained." *Valle*, 301 F.R.D. at 115; A. 236. This distinction is illusory. What matters under the CFAA is *access to a computer*, not *later use of information*. *See* 18 U.S.C. § 1030(a)(2)(B) ("intentionally *accesses a computer* … [to] obtain[] . . . information") (emphasis added). It would be odd indeed if what saved the *Nosal* defendant was that he used the information in hopes of sabotaging his former employer—an immunity that Valle cannot claim by the district court's logic because he did not use the information he obtained from his NYPD computer.

The district court also suggested that, "[u]nlike the disloyal employees in the cases cited by Defendant, Valle did not have unrestricted access to [the NYPD's computer] system and its associated databases—he was not free to access the information in these databases under all circumstances." *Valle*, 301 F.R.D. at 115; A. 237.[12] But those "disloyal employees" were likewise not free to access their

[12] That Valle lacked unfettered access to every piece of information on the NYPD's computers is irrelevant because he had authorization to access the databases in question. *See US Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189, 1194 (D. Kan. 2009) (dismissing CFAA claims against defendants who "did at least have initial access to the confidential information in plaintiffs' computer system in the course of

employers' computers under all circumstances—indeed, that was the reason they found themselves facing prosecution. Nosal's access was subject to Korn/Ferry's policy limiting computer use to "Korn/Ferry business only," *Nosal*, 676 F.3d at 856 n.1; the *Miller* defendant's downloading of information to his personal computer "was contrary to company policies regulating use," *Miller*, 687 F.3d at 202 (citation omitted); the *Aleynikov* defendant's access was subject to Goldman's computer-use "policies," *Aleynikov*, 737 F. Supp. 2d at 190; and the *JBCHoldings* defendant's access was subject to the plaintiffs' "electronic media policy," *JBCHoldings*, 931 F. Supp. 2d at 525. Just as with these defendants, the sweep of the CFAA does not reach Valle even though he violated his employer's computer-use policy.

II. THE CFAA'S STATUTORY HISTORY CONFIRMS THE STATUTE'S PLAIN MEANING.

The district court did not consider the CFAA's statutory history. This history compels Valle's narrow construction of the CFAA because it is the only reading "consistent with [the CFAA]'s statutory amendments." *United States v. Dauray*, 215

their employment," where plaintiffs did not allege "that the defendants had no access whatsoever to plaintiffs' computer system at the time of their allegedly wrongful acts.").

F.3d 257, 263 (2d Cir. 2000); *see also Allard K. Lowenstein Int'l Human Rights Project v. Dep't of Homeland Security*, 626 F.3d 678, 681 (2d Cir. 2010).[13]

The original version of § 1030(a), enacted in 1984, penalized anyone who "knowingly accesses a computer without authorization, or having accessed a computer with authorization, *uses the opportunity such access provides for purposes to which such authorization does not extend*," and thereby obtains information. 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).[14] This language specifically covered those who used their authorized computer access for "purposes to which such authorization d[id] not extend."

But Congress deleted that language in 1986 and replaced it with different language limited to a person who "*intentionally* accesses a computer without

[13] Statutory history—the official changes Congress makes to a statute over time—answers many questions of statutory interpretation that legislative history alone is often unable to resolve. *See* Hon. John M. Walker, Jr., *Judicial Tendencies in Statutory Construction: Differing Views on the Role of the Judge*, 58 N.Y.U. Annual Survey of Am. L. 203, 234 (2001) ("[S]tatutory history accounts for the collective action of the legislature and thus is more objectively determined and less susceptible to judicial and legislative manipulation than legislative history as it is generally understood.").

[14] In 1984, § 1030(a)(2) only applied to covered financial institutions, but the quoted language also appeared in § 1030(a)(3), which included government computers.

authorization, *or exceeds authorized access*," and thereby obtains information. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(a)(1), (c), 100 Stat. 1213, 1213 (emphasis added). Congress defined the new term "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter . . . ." *Id.* This definition has persisted to the present day.

The 1986 textual change thus eliminated any reference to the "purposes" for which information was accessed. That change shows that Congress did not intend for liability to turn on a defendant's purpose.[15] *See Booth v. Churner*, 532 U.S. 731, 739 (2001) (noting the "significance of deleting [a] term" in construing a statutory scheme).

Congress deleted "purposes" from § 1030 to eliminate civil and criminal liability for employees who might use their valid computer credentials for an improper purpose. Congress wanted to "remove[] from the sweep of the statute one of the murkier grounds of liability, under which a[n] … employee's access to

[15] Congress further amended § 1030(a)(2) in 1996 to cover federal government computers. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201(1)(B)(ii), 110 Stat. 3488, 3492. This amendment closed a gap in the 1986 statute, which prohibited hacking into a federal government computer *only* if the defendant was "without authorization to access *any* computer of [the] department or agency" at issue. *See* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(b)(1), 100 Stat. 1213, 1213 (codified as amended at 18 U.S.C. § 1030(a)(3)) (emphasis added).

computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances." S. Rep. No. 99-432, at 21, 1986 U.S.C.C.A.N. 2479, 2494.

Instead, Congress intended to cover individuals who accessed information they were "not entitled to … obtain or alter" under *any* circumstances, regardless of purpose or motivation. 18 U.S.C. § 1030(e)(6). The statutory history thus puts the CFAA into focus: it is designed to punish trespass-by-computer. *See* S. Rep. No. 99-432, at 7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485 (referring to "unauthorized access" as a "trespass offense"); *see also* S. Rep. No. 104-357, at 7 (1996) (stating that the purpose of § 1030(a)(2) is to "protect against the interstate or foreign *theft of information* by computer") (emphasis added).

The CFAA had this focus from the start. Congress enacted the statute to do "for computers what trespass and burglary laws did for real property." Orin S. Kerr, *Cybercrimes' Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1617 (2003). The 1984 House Report proposing the legislation stated that "[i]t is obvious that traditional theft/larceny statutes are not the proper vehicles to control the spate of computer abuse and computer-assisted crimes" because hackers "have been able to access (trespass into) both private and public computer systems" without using means of interstate commerce necessary for prosecution under wire and mail fraud statutes. H.R. Rep. No. 98-894, at 9-10

(1984), *reprinted in* U.S.C.C.A.N. 1984, 3689, 3695; *see also id.* at 10, *reprinted in* U.S.C.C.A.N. 1984, 3689, 3696 (adding that advances in computer networking capabilities "enabled the recent flurry of electronic trespassing incidents").

The district court overlooked this statutory history and incorrectly applied the statute based on Valle's improper purpose, not his trespass, in accessing the NYPD computer system. In effect, by making Valle's subjective purpose the linchpin of his liability, the court improperly rendered the 1986 statutory amendment a nullity. Courts that have carefully considered the CFAA's statutory amendments and history have not made the same mistake. *See, e.g.*, *JBCHoldings*, 931 F. Supp.2d at 524 n.8 (noting that the history of the CFAA "accords with the narrow interpretation of 'exceeds authorized access'"); *Aleynikov*, 737 F. Supp. 2d at 192 n. 23 (concluding from the statutory history that Congress intended to eliminate coverage for authorized access that aims at "purposes to which such authorization does not extend").

III. THE DISTRICT COURT'S INTERPRETATION OF THE CFAA CREATES SERIOUS CONSTITUTIONAL PROBLEMS AND CONTRAVENES THE RULE OF LENITY.

The requirement that criminal statutes provide fair warning further compels a narrow reading of the CFAA. Two manifestations of the fair notice requirement apply here, both of which the district court overlooked. First, the vagueness doctrine "'bars enforcement of a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application.'" *Lurie v. Wittner*, 228 F.3d 113, 126 (2d Cir. 2000) (quoting *United States v. Lanier*, 520 U.S. 259, 266-67 (1997)). Second, "'as a sort of junior version of the vagueness doctrine, *the canon of strict construction of criminal statutes, or rule of lenity, ensures fair warning by so resolving any ambiguity in a criminal statute as to apply it only to conduct clearly covered*.'" *Lurie*, 228 F.3d at 126 (emphasis by this Court; quoting *Lanier*, 520 U.S. at 266-67).

A. The District Court's Expansive Interpretation of the CFAA Violates the Canon of Constitutional Doubt.

The broad construction of the CFAA advanced by the government and endorsed by the district court creates serious questions about the statute's constitutionality. In particular, that construction, by making criminal liability turn on violations of often vague computer-use policies, potentially renders the CFAA itself unduly vague. The court, therefore, should have adopted the more plausible and narrower interpretation of the CFAA, pursuant to the rule of constitutional doubt.

An interpretation of a statute can be so vague that it denies due process for either of two independent reasons: (1) "if it fails to provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits," *or* (2) "if it authorizes or even encourages arbitrary and discriminatory enforcement."

Thibodeau v. Portuondo, 486 F.3d 61, 65-66 (2d Cir. 2007) (internal citations omitted). The canon of constitutional doubt obligates courts to construe a statute narrowly, where "fairly possible," to avoid constitutional concerns that it is void-for-vagueness. *Boos v. Barry*, 485 U.S. 312, 331 (1988).

Here, the narrower interpretation of the CFAA is more than "fairly possible." As shown in Parts I and II, it remains the best reading of the CFAA's text in light of its history. And that interpretation provides a clear, bright-line rule for prosecutors, courts, and the public: the CFAA makes it illegal to access information (regardless of purpose) in the absence of authorization to access (1) the computer containing the information, or (2) the specific information at issue. *Cf. Facebook, Inc. v. Grunin*, 2015 WL 124781, at *4 (N.D. Cal. Jan. 8, 2015) (distinguishing *Nosal* by noting that Facebook blocked the defendant from using its website for any purposes, fraudulent or social); *NetApp, Inc. v. Nimble Storage, Inc.*, 2014 WL 1903639, at *10 (N.D. Cal. May 12, 2014) (explaining that, in light of *Nosal*, the CFAA applied to defendant who accessed former employer's computer database after he quit, knowing that the employer limited access to current employees and registered partners). In contrast, the district court's broad interpretation violates the avoidance canon by placing the CFAA on questionable constitutional grounds of intelligibility and enforcement, as discussed below.

1. The District Court's Holding Renders the Scope of § 1030 Impermissibly Unclear.

Applying the CFAA to punish Valle requires an interpretation of the statute that makes it difficult, if not impossible, to know exactly what conduct it covers. By equating Valle's CFAA liability with his noncompliance with the NYPD's computer-use policy, the district court made a criminal of every employee who violates his employer's similar policy (or a website's terms of use). That construction would criminalize conduct that nobody would expect (or want) to be covered, raising serious notice problems. *See United States v. Drew*, 259 F.R.D. 449, 467 (C.D. Cal. 2009) (holding that misdemeanor CFAA conviction, based only on intentional violation of website's terms of use, would violate the void-for-vagueness doctrine). As *Nosal* explained:

> Significant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read. Consider the typical corporate policy that computers can be used only for business purposes. What exactly is a 'nonbusiness purpose'? If you use the computer to check the weather report for a business trip? For the company softball game? For your vacation to Hawaii? And if minor personal uses are tolerated, how can an employee be on notice of what constitutes a violation sufficient to trigger criminal liability?

Nosal, 676 F.3d at 860.

Beyond the workplace, even casual Internet users who violate a website's terms of use in some minor way would potentially fall within the district court's interpretation of the statute. Website terms of use often specifically condition access on permissible uses and purposes, yet are written so broadly and abstrusely that users violate them unknowingly as a matter of course.[16] To avoid making each of these violations a federal crime, courts read § 1030 narrowly and decline to treat terms of use as governing access rights. *See Nosal*, 676 F.3d at 861-62; *Drew*, 259 F.R.D. at 464-65. By doing the opposite, the district court transformed the CFAA "into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals." *Drew*, 259 F.R.D. at 466.

While the district court did not address these notice problems, the government did in its post-trial briefing. First, the government argued that its interpretation would not ensnare computer users who violate website terms of use because these websites are "public" and distinct from the "NYPD's restricted electronic facilities," so that the CFAA, "as applied to Valle, covers a very narrow subset of activity over computer network." (Government Opposition to the Defendant's Motions for a New Trial and Judgment of Acquittal 48, *Valle*, No. 12-Cr.-847 (PGG) (S.D.N.Y. filed Aug. 16, 2013), ECF No. 195 [hereinafter "Post-Trial Opp."].)

[16] Website users also are generally unaware of terms of use and these terms can change at the website owner's discretion, which further compounds the notice problem. *Nosal*, 676 F.3d at 862.

This supposed distinction is illusory. There is no textual basis to distinguish among the iterations of "exceeds authorized access" in § 1030, and the government identified none. *See Feldstein*, 951 F. Supp. 2d at 218 ("It is not possible to define authorization narrowly for some CFAA violations and broadly for others.") (citing *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007)); *see also Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). Although this prosecution was brought under 18 U.S.C. § 1030(a)(2)(B), the government's reading would apply equally to § 1030(a)(2)(C) charges. In any event, the government's argument is unworkable—it does not explain *how* restricted, *how* valuable, or *how* sensitive data needs to be to trigger § 1030 liability. Any such line-drawing would be arbitrary. Because § 1030 uses the same phrase—"exceed[ing] authorized access"—with respect to computers containing "sensitive" or "restricted" information, and to computers merely affecting interstate commerce, the government's broad reading of the phrase would apply to virtually all users of computers. *See Feldstein*, 951 F. Supp. 2d at 218 (noting the impossibility of applying § 1030's subsections to "differentiate[] between harmless workplace procrastination and more serious theft of intellectual property").

The government also argued that Valle was "warned repeatedly that the very activity in which he engaged would lead to criminal prosecution and other sanctions." (Post-Trial Opp. 48.) This argument misses the mark. *First*, the determination of whether a statute provides fair warning "must be made on the basis of the statute itself and other pertinent law, rather than on the basis of an ad hoc appraisal of the subjective expectations of particular defendants." *Bouie v. City of Columbia*, 378 U.S. 347, 355 n.5 (1964); *see also United States v. Tolczeki*, 614 F. Supp. 1424 (D.C. Ohio 1985). *Second*, even assuming the relevance of Valle's "subjective expectations," no evidence suggested that Valle received warnings that using his computer for personal reasons violated a federal statute, much less a federal *computer-hacking* statute.[17]

In sum, making CFAA liability turn on violations of employer and website terms of computer use—which are often hopelessly unclear and constantly changing—raises serious vagueness problems. Relatedly, construing the statute to make federal criminal liability turn on standards set by websites and private employers (a municipal employer in this case)—rather than on standards set by Congress—potentially renders the CFAA an unconstitutional delegation of legislative authority. *See* Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 Harv. L. Rev. 751, 771 (2013) (arguing

[17] The NYPD training PowerPoint listed a number of *New York state* criminal offenses that may result from computer misconduct, but made no reference to any federal offenses. GX 210C; *see United States v. Facchini*, 874 F.2d 638, 645 (9th Cir. 1989) (Alarcon, J., concurring) (explaining that applicant for state employment had "[n]o actual notice" that making false statements in application "would subject the applicant to *federal* prosecution") (emphasis in original).

that the CFAA if construed broadly, would violate the federal private nondelegation doctrine). The district court should have avoided these constitutional difficulties by construing the statute narrowly. *See Skilling v. United States*, 561 U.S. 358, 408 n.42 (2010) ("Apprised that a broader reading of § 1346 could render the statute impermissibly vague, Congress, we believe, would have drawn the honest-services line, as we do now, at bribery and kickback schemes."); *see also Allstate Ins. Co. v. Serio*, 261 F.3d 143, 150 (2d Cir. 2001).

2. The District Court's Interpretation Invites Arbitrary and Discriminatory Enforcement.

The district court's interpretation of § 1030(a)(2) also risks arbitrary and discriminatory enforcement. Courts considering as-applied vagueness challenges ask whether (1) "a statute as a general matter provides sufficiently clear standards to eliminate the risk of arbitrary enforcement," or (2) "even in the absence of such standards, the conduct at issue falls within the core of the statute's prohibition, so that the enforcement before the court was not the result of the unfettered latitude that law enforcement officers and factfinders might have in other, hypothetical applications of the statute." *Farrell v. Burke*, 449 F.3d 470, 493 (2d Cir. 2006).

As discussed in Part III.A.1, the district court's interpretation of § 1030(a)(2) encourages arbitrary enforcement by criminalizing routine (and often trivial) computer misuse. If any violation of workplace computer-use policies or website terms of use renders access unauthorized, "there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution." *Drew*, 259 F.R.D. at 467 (quoting *Kolender v. Lawson*, 461 U.S. 352, 358 (1983)). "Nor is it acceptable to rely solely upon prosecutorial discretion to refrain from prosecuting trivial offenses." *Feldstein*, 951 F. Supp. 2d at 218 (citing *Nosal*, 676 F.3d at 862); *see also United States v. Stevens*, 559 U.S. 460, 480 (2010) ("We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly.").

And Valle's conduct is hardly a paradigmatic CFAA offense. The core prohibition of the CFAA is hacking. The statute targets "*outside* hackers (individuals who have no authorized access to a computer at all)," and "*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); *see supra* Part II. Valle fits neither type, whatever his purpose for querying Hartigan's name. *See Lockheed Martin Corp. v. Speed*, 2006 WL 2683058, at *6 (M.D. Fla. Aug. 1, 2006) ("Congress singled out those accessing 'without authorization' (or below authorization) and those 'exceeding authorization' (or above authorization) while purposefully leaving those in the middle untouched (those accessing *with* authorization), regardless of their subjective intent.") (emphasis in original).

B. The Rule of Lenity Compels a Narrow Reading of the CFAA.

The district court also did not address the rule of lenity. This rule requires courts to resolve ambiguity in a criminal statute in the defendant's favor on the theory that "[i]f Congress desires to go further, it must speak more clearly." *McNally v. United States*, 483 U.S. 350, 360 (1987). The rule of lenity applies when "a reasonable doubt persists about a statute's intended scope even *after* resort to the language and structure, legislative history, and motivating policies of the statute." *Moskal v. United States*, 498 U.S. 103, 108 (1990).

For the reasons discussed in Part I, far more than a "reasonable doubt" exists over whether the CFAA creates purpose-based liability. Indeed, many courts that have closely examined the statute have concluded that it unambiguously *does not* turn on a defendant's purposes. *See Brekka*, 581 F.3d at 1132-35; *JBCHoldings*, 931 F. Supp. 2d at 524 ("[T]he Court does not find the statute ambiguous."); *Diamond Power*, 540 F. Supp. 2d at 1342; *Werner-Masuda*, 390 F. Supp. 2d at 498-99.

The CFAA also must be narrowly construed to the extent it reaches conduct traditionally governed by state contract and tort laws, without any clear indication from Congress that it sought to do so. *Whitman v. American Trucking Ass'ns*, 531 U.S. 457, 468 (2001) (Congress "does not … hide elephants in mouseholes"). Valle was prosecuted under the CFAA for conduct—misusing his workplace computer—traditionally subject to administrative and state remedies. *See, e.g.*, N.Y. Penal Law

§ 195.00[1] (cited in NYPD training class and criminalizing "official misconduct" by a public servant); *Conde v. Kelly*, 990 N.Y.S.2d 166, 167-78 (N.Y. App. Div. 1st Dep't 2014) (upholding police commissioner's firing of officer for wrongfully accessing and obtaining confidential information from police computer system). Nothing in the CFAA or its statutory or legislative history suggests that Congress intended to convert this type of state misconduct into a federal crime. *See supra* Part II; *Orbit One Commc'ns,* 692 F. Supp. 2d at 386 (applying the rule of lenity and observing that "[i]t would be imprudent to interpret the CFAA … to transform the common law civil tort of misappropriation of confidential information into a criminal offense").

Rather, in the 1986 amendments, Congress stated that "administrative sanctions are more appropriate than criminal punishment" when a government employee uses otherwise valid computer access for an improper purpose. S. Rep. No. 99-432, at 7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485. Congress, moreover, "reject[ed]" proposals to "enact as sweeping a Federal statute as possible," given its confidence in "the interests and abilities of the 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. Here, in fact, the NYPD suspended Valle upon his indictment (and fired Valle upon his conviction), and the NYPD plainly has the ability to impose "administrative sanctions" on officers who access law enforcement databases for improper purposes. That appears to be exactly what Congress intended. *See Bond v. United States*, 134 S. Ct. 2077, 2090 (2014) (insisting on "a clear indication that Congress meant to reach purely local crimes, before interpreting the statute's expansive language in a way that intrudes on the police power of the States.").

JBCHoldings illustrates this point further. There, in addition to the CFAA claim, the plaintiffs brought several state law contract and tort causes of action against the defendant for accessing a computer with an improper purpose. 931 F. Supp. 2d at 525. In discussing the rule of lenity vis-à-vis the CFAA claim, Judge Engelmayer observed that "because computers today are ubiquitous, the broad reading of the CFAA would permit such localized wrongs—breaches of contract, in form if not substance—to be litigated in federal court." *Id.* "Absent a clearer statement," the court declined to "ascribe to Congress an intent thus to dramatically expand federal criminal and civil jurisdiction." *Id.*

****

In sum, the CFAA does not cover every unethical, blameworthy, or morally offensive use of a computer. Rather, it narrowly focuses on people who have no authority to access a computer (or no authority to access specific files or databases on a computer) for *any* purpose. It does not cover people who simply use their authorized computer access for an inappropriate purpose. The district court was wrong to read the CFAA more expansively. Accordingly, since the statute does not cover his conduct, the evidence is legally insufficient to sustain Valle's CFAA conviction, and this Court should reverse it.

CONCLUSION

For these reasons, under the proper interpretation of the CFAA, the evidence is insufficient to support Valle's conviction. This Court should therefore reverse the judgment of conviction and remand for entry of a judgment of acquittal.

Dated: New York, New York
March 3, 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 brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because:

this brief contains 11,767 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This corrected 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:

this brief has been prepared in a **Times New Roman** typeface using **Microsoft Word 2007**.

Dated: March 3, 2015

/s/____________________________
Edward S. Zas

CERTIFICATE OF SERVICE

I certify that a copy of this Corrected 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
March 3, 2015

/s/
Edward S. Zas