14-4396-cr

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

UNITED STATES OF AMERICA,

APPELLEE,

v.

GILBERTO VALLE, AKA SEALED DEFENDANT 1,

DEFENDANT-APPELLANT,

MICHAEL VANHISE, AKA SEALED DEFENDANT 1, ROBERT CHRISTOPHER ASCH, AKA CHRIS, RICHARD MELTZ, AKA RICK,

DEFENDANTS.

On Appeal from the United States District Court
for the Southern District of New York
Case No. 1:12-cr-00847-PGG-1
Honorable Paul G. Gardephe, U.S. District Judge

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AND SCHOLARS IN SUPPORT OF DEFENDANT-APPELLANT GILBERTO VALLE

Hanni Fakhoury
Jamie L. Williams
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
hanni@eff.org

Richard D. Willstatter
Amicus Committee Vice Chair, Second Circuit
NATIONAL ASS'N OF CRIMINAL DEFENSE LAWYERS
Green & Willstatter
200 Mamaroneck Avenue, Suite 605
White Plains, NY 10601
(914) 948-5656
willstatter@msn.com

Harley Geiger
CENTER FOR DEMOCRACY & TECHNOLOGY
1634 I Street NW,
Suite 1100
Washington, D.C. 20006
(202) 637-9800
harley@cdt.org

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* the Electronic Frontier Foundation, the Center for Democracy & Technology, and the National Association of Criminal Defense Lawyers state that they do not have a parent corporation and that no publicly held company owns 10 percent or more of their stock.

Dated: March 9, 2015

By: */s/ Hanni Fakhoury*
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Curiae

TABLE OF CONTENTS

Page

STATEMENT OF INTEREST 1

INTRODUCTION 5

ARGUMENT 6

I. THE COMPUTER FRAUD AND ABUSE ACT DOES NOT PROHIBIT VIOLATIONS OF COMPUTER USE RESTRICTIONS. 6

A. The CFAA Was Meant To Target "Hacking," Not Violations of Computer Use Restrictions. 8

B. This Case Presents a Mere Use Restriction. 15

II. THE DISTRICT COURT'S BROAD READING OF THE CFAA RENDERS IT UNCONSTITUTIONALLY VAGUE. 18

A. Corporate Policies Do Not Provide Sufficient Notice of What Conduct Is Prohibited. 20

B. Allowing CFAA Liability For Mere Use Restrictions Turns a Vast Number of Ordinary Individuals Into Criminals. 23

CONCLUSION 27

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Advanced Aerofoil Technologies, AG v. Todaro,
2013 WL 410873 (S.D.N.Y. Jan. 30, 2013) (unpublished) 10

Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc.,
690 F. Supp. 2d 1267 (M.D. Ala. 2010) 12

Black & Decker, Inc. v. Smith,
568 F. Supp. 2d 929 (W.D. Tenn. 2008) 12

Bouie v. City of Columbia,
378 U.S. 347 (1964) 14

Brett Senior & Assocs., P.C. v. Fitzgerald,
2007 WL 2043377 (E.D. Pa. July 13, 2007) (unpublished) 12, 15

Clarity Servs., Inc. v. Barney,
698 F. Supp. 2d 1309 (M.D. Fla. 2010) 12

Connally v. Gen. Const. Co.,
269 U.S. 385 (1926) 20

Corley v. United States,
556 U.S. 303 (2009) 14

Craigslist Inc. v. 3Taps Inc.,
942 F. Supp. 2d 962 (N.D. Cal. 2013) 15

Craigslist, Inc. v. 3Taps, Inc.,
964 F. Supp. 2d 1178 (N.D. Cal. 2013) 9, 15, 16, 17

Cvent, Inc. v. Eventbrite, Inc.,
739 F. Supp. 2d 927 (E.D. Va. 2010) 9, 17

Diamond Power Int'l., Inc. v. Davidson,
540 F. Supp. 2d 1322 (N.D. Ga. 2007) 12

Dresser-Rand Co. v. Jones,
957 F. Supp. 2d 610 (E.D. Pa. 2013) 12, 13

EF Cultural Travel BV v. Explorica, Inc.,
274 F.3d 577 (1st Cir. 2001) 13

Grayned v. Rockford,
408 U.S. 104 (1972) 23, 24

IBP, Inc. v. Alvarez,
546 U.S. 21 (2005) 20, 22

Int'l Airport Ctrs. v. Citrin,
440 F.3d 418 (7th Cir. 2006) 13

Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda,
390 F. Supp. 2d 479 (D. Md. 2005) 12

Jet One Grp., Inc. v. Halcyon Jet Holdings, Inc.,
2009 WL 2524864 (E.D.N.Y. Aug. 14, 2009) (unpublished) 12

Koch Industries, Inc. v. Does,
2011 WL 1775765 (D. Utah May 9, 2011) (unpublished) 12, 16

Kolender v. Lawson,
461 U.S. 352 (1983) 18

Leocal v. Ashcroft,
543 U.S. 1 (2004) 10

Lewis-Burke Associates, LLC v. Widder,
725 F. Supp. 2d 187 (D.D.C. 2010) 12

Lockheed Martin Corp. v. Speed,
2006 WL 2683058 (M.D. Fla. Aug. 1, 2006) (unpublished) 12

LVRC Holdings LLC v. Brekka,
581 F.3d 1127 (9th Cir. 2009) 7, 8, 11, 12

Major, Lindsey & Africa, LLC v. Mahn,
2010 WL 3959609 (S.D.N.Y. Sept. 7, 2010) (unpublished) 10

Nat'l City Bank, N.A. v. Republic Mortgage Home Loans, LLC,
2010 WL 959925 (W.D. Wash. Mar. 12, 2010) (unpublished) 12

Orbit One Commc'ns, Inc. v. Numerex Corp.,
692 F. Supp. 2d 373 (S.D.N.Y. 2010) 9, 10, 12

Pulte Homes, Inc. v. Laborer's Int'l Union of N. Am.,
648 F.3d 295 (6th Cir. 2011) 9

ReMedPar, Inc. v. AllParts Med., LLC,
683 F. Supp. 2d 605 (M.D. Tenn. 2010) 12

Scottrade, Inc. v. BroCo Investments, Inc.,
774 F. Supp. 2d 573 (S.D.N.Y. 2011) 9, 12

Shamrock Foods Co. v. Gast,
535 F. Supp. 2d 962 (D. Ariz. 2008) 12

Skilling v. United States,
561 U.S. 358 (2010) 18

United States v. John,
597 F.3d 263 (5th Cir. 2010) 13, 14

United States v. Kozminski,
487 U.S. 931 (1988) 25, 26

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

United States v. Rodriguez,
628 F.3d 1258 (11th Cir. 2010) 13

United States v. Santos,
553 U.S. 507 (2008) 13, 19

United States v. Shabani,
513 U.S. 10 (1994) 19

United States v. Stevens,
559 U.S. 460 (2010) 26

United States v. Valle,
301 F.R.D. 53 (S.D.N.Y. 2014) 6, 15, 17

United States v. Velastegui,
199 F.3d 590 (2d Cir. 1999) 19

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

Wentworth-Douglass Hospital v. Young & Novis Professional Association,
2012 WL 2522963 (D.N.H. June 29, 2012) (unpublished) 16

Federal Statutes

18 U.S. § 1030 ..... *passim*

18 U.S.C. § 1832 27

Legislative Materials

H.R. Rep. 98–894, reprinted in 1984 U.S.C.C.A.N. 3689 (July 24, 1984) 7

S. Rep. No. 99–432, reprinted in 1986 U.S.C.C.A.N. 2479 (September 3, 1986) ... 7

Other Authorities

Dartmouth College, Employment Policies and Procedures Manual 23

Employee Handbook, Policies and Procedures 23

Facebook's Statement of Rights and Responsibilities, 4.1 26

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

Susan M. Heathfield, Internet and Email Policy 22

The American Heritage Dictionary (5th ed.) 6

Virginia Dep't of Human Resource Management, Use of the Internet and
Electronic Communications Systems 23

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation, the Center for Democracy & Technology, the National Association of Criminal Defense Lawyers, and the below-listed scholars (collectively, "*Amici*") respectfully submit this brief in support of Defendant-Appellant Gilberto Valle, urging reversal of Mr. Valle's CFAA conviction.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect consumer interests, innovation, and free expression in the digital world. With over 25,000 active donors and dues-paying members, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age, and it publishes a comprehensive archive of digital civil liberties information at www.eff.org. As part of its mission, EFF has served as counsel or amicus in key cases addressing the application of law to the Internet and other new technologies. EFF is particularly interested in the principled and fair application of computer crime laws generally and the Computer Fraud and Abuse Act ("CFAA")

[1] Pursuant to Federal Rule of Appellate Procedure 29(c)(5), no party's counsel authored this brief in whole or in part, and neither any party, nor any party's counsel, contributed money towards the preparation of this brief. No person other than *amici*, its members, or its counsel contributed money that was intended to fund preparing or submitting this brief. All parties have consented to the filing of this brief.

specifically. In that regard, EFF has served as counsel or *amicus curiae* in key cases addressing the CFAA. *See United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (appellate co-counsel); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) (amicus); *United States v. Cioni*, 649 F.3d 276 (4th Cir. 2011) (amicus); *Craigslist, Inc. v. 3Taps, Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013) (amicus); *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (amicus).

The Center for Democracy & Technology ("CDT") is a nonprofit public interest group that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized Internet. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of Internet users. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of approximately 10,000 direct members in 28 countries, and 90 state, provincial and local affiliate organizations totaling up to 40,000 attorneys. NACDL's members include private criminal defense lawyers, public defenders, military defense

counsel, law professors, and judges. NACDL files numerous *amicus* briefs each year in the Supreme Court, this Court, and other courts, seeking to provide *amicus* assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole. In furtherance of NACDL's mission to safeguard fundamental constitutional rights, the Association often appears as *amicus curiae* in cases involving overcriminalization. NACDL is particularly interested in this case given the Association's concerns about the implications of the overly broad application of statutes like the Computer Fraud and Abuse Act (CFAA).

The following scholars—who have diverse expertise on the science and practice of computer and data security, computer crime, and Internet law—also join this brief, in their individual capacities, as *Amici*:[2]

- Sergey Bratus, Research Associate Professor at Dartmouth College and Chief Security Advisor to Dartmouth's Institute for Security, Technology, & Society;
- Professor Gabriella Coleman, Wolfe Chair in Scientific and Technological Literacy, McGill University;

[2] The titles of the listed scholars are given for affiliation purposes only.

- Professor Eric Goldman, law professor and co-director of the High Tech Law Institute at Santa Clara University School of Law. Professor Goldman has taught and researched Internet Law for two decades. He is interested in the development of Internet law, especially restricting trespass-to-chattels doctrines from interfering with ordinary every-day computer interactions; and
- Jeffrey Vagle, Lecturer in Law and Executive Director, Center for Technology, Innovation & Competition, University of Pennsylvania Law School.

INTRODUCTION

The federal "hacking" statute, the Computer Fraud and Abuse Act ("CFAA"), was intended to criminalize exactly that: the circumvention of technical restrictions in order to access data by a person not otherwise entitled to access it. The CFAA was not intended to criminalize breaches of contract, or misappropriation or misuse of data. But in ruling that Gilberto Valle "exceeded authorized access" to a federal database under the CFAA when he logged into a police database—one he was authorized to access—for an improper purpose, the district court turned millions of ordinary computer users into criminals and rendered an already worrisomely broad statute unconstitutionally vague.

Through accessing the New York City Police Department's Omnixx Force Mobile ("OFM") system without a valid law enforcement purpose, Mr. Valle violated a computer *use* restriction—and nothing more. Neither employers nor courts can contravene Congress's intent to target hacking—not violations of contractual use restrictions—by styling a use restriction as an "access" restriction. Indeed, many courts, including the Fourth and Ninth Circuits—the two most recent circuit courts to address the issue—have rejected the very conclusion the district court reached here, finding instead that individuals, including employees, are *not* liable under the CFAA for violations of computer use restrictions. *See, e.g., WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *United*

States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc). The facts presented here are no different from the "disloyal employee" cases cited by the district court, and the district court's attempt to distinguish them rings hollow. *See United States v. Valle*, 301 F.R.D. 53, 115 (S.D.N.Y. 2014).

This Court must therefore reverse the district court's order denying Mr. Valle's motion for acquittal of the CFAA charges.

ARGUMENT

I. THE COMPUTER FRAUD AND ABUSE ACT DOES NOT PROHIBIT VIOLATIONS OF COMPUTER USE RESTRICTIONS.

Section 1030(a)(2) of the CFAA prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any department or agency of the United States[.]" 18 U.S.C. § 1030(a)(2)(B). The term "exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."[3] 18 U.S.C. § 1030(e)(6).

[3] "Entitle" is defined as "[t]o furnish with a right or claim to something." *See* "entitle," The American Heritage Dictionary (5th ed.), *available at* https://www.ahdictionary.com/word/search.html?q=entitle (last visited Mar. 5, 2015). As noted by the Ninth Circuit, for the purposes of the CFAA, "[a]n equally or more sensible reading of 'entitled' is as a synonym for 'authorized.'" *Nosal*, 676 F.3d at 857. "So read, 'exceeds authorized access' would refer to data or files on a computer that one is not authorized to access." *Id.*

The CFAA's prohibition against accessing a protected computer "without authorization" covers outsiders who have no rights to the computer system. But the prohibition against "exceed[ing] authorized access" is aimed at insiders who "ha[ve] permission to access the computer, but access[] information on the computer that the[y] [are] not entitled to access." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). An individual thus "exceeds authorized access" only when he accesses information he is not otherwise permitted to access, regardless of the purpose for which he accesses the information. *See WEC Carolina*, 687 F.3d at 206 ("exceeds authorized access" only applies when individual "obtains or alters information on a computer beyond that which he is authorized to access").

The question before this Court, then, is whether Mr. Valle—an NYPD employee—"exceed[ed] authorized access" by accessing information that he was otherwise entitled to access but for a purpose not permitted by NYPD's computer use policy. The answer is no.

The legislative history is clear that the CFAA was designed to criminalize "hacking," not violations of computer use policies. Despite the district court's holding to the contrary, the case at issue involves nothing more than a violation of an employer's computer use policy. Indeed, there is no question that Mr. Valle was authorized to access information in the police database and that he did not have to

circumvent any technological access barriers in order to access the data in question. The fact that the NYPD instituted a policy restricting use of the database for valid law enforcement purposes did not alter the scope of Mr. Valle's authorization—regardless of how the restriction was labeled—and is thus irrelevant for assessing whether Mr. Valle "exceeded his authorized access" to the database under the CFAA.

A. The CFAA Was Meant To Target "Hacking," Not Violations of Computer Use Restrictions.

The CFAA "was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives[.]'" *Brekka*, 581 F.3d at 1130–31 (quoting H.R. Rep. 98–894, at 9, reprinted in 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984)). As the Ninth Circuit has noted, citing the CFAA's legislative history, Congress' purpose in enacting the CFAA was to target "hackers" who "'intentionally trespass[ed] into someone else's computer files'" and obtained information, including information on "'how to break into that computer system.'" *Nosal*, 676 F.3d at 858 (quoting S. Rep. No. 99–432, at 9, reprinted in 1986 U.S.C.C.A.N. 2479, 2487 (September 3, 1986)).

Put simply, the CFAA's "purpose is to punish hacking—the circumvention of technological access barriers[.]" *Nosal*, 676 F.3d at 863. In other words,

Congress intended to punish those who circumvented code-based barriers to access, not those who violated written, policy-based computer use restrictions.[4] Congress sought to address a narrow problem, not create "a sweeping Internet-policing mandate." *Id*. at 858; *see also Cvent, Inc. v. Eventbrite, Inc*., 739 F. Supp. 2d 927, 932 (E.D. Va. 2010) ("The CFAA is a civil and criminal anti-hacking statute designed to prohibit the use of hacking techniques to gain unauthorized access to electronic data.").

Numerous courts—including the two most recent circuit courts to address the issue and multiple decisions from the Southern District of New York[5]—have

---

[4] The way for an employer or any other computer owner to indicate who is authorized and not authorized to access a computer system is to erect a technological, code-based access barrier—such as a username and password requirement—to allow authorized users in and keep unwanted individuals out. Without some barrier to entry, however, everyone is "authorized" to access data. *See, e.g., Pulte Homes, Inc. v. Laborer's Int'l Union of N. Am*., 648 F.3d 295, 304 (6th Cir. 2011) (public presumptively authorized to access "unprotected website"); *Craigslist, Inc. v. 3Taps, Inc*., 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013) (making information website publicly available gives everyone "authorization" to view it under the CFAA). In other words, the erection of a password barrier is what permits the employer or other computer owner to determine who has authorization to access a protected computer system or website.

[5] *See Orbit One Commc'ns, Inc. v. Numerex Corp*., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("[R]eading the phrases 'access without authorization' and 'exceeds authorized access' to encompass an employee's misuse or misappropriation of information to which the employee freely was given access and which the employee lawfully obtained would depart from the plain meaning of the statute."); *see also Scottrade, Inc. v. BroCo Investments, Inc*., 774 F. Supp. 2d 573, 584 (S.D.N.Y. 2011) ("Because Scottrade does not allege that Genesis hacked into its systems, or otherwise accessed its computers without authorization,

interpreted the phrase "exceeds authorized access" to criminalize only the actions of those users who use their authorization to access data they are not entitled to obtain at all, rather than to criminalize the actions of those who have authority to access data but who do so for a purpose that violates a contractual agreement or unilaterally-imposed use policy. *See WEC Carolina*, 687 F.3d at 199; *Nosal*, 676 F.3d at 854. Though this scenario most often comes up in civil cases involving employment situations—where an employee takes data for a purpose prohibited by his employer—the rationale of these decisions applies equally to criminal CFAA cases. Indeed, courts "must interpret [a] statute consistently, whether [it] encounter[s] its application in a criminal or noncriminal context[.]" *Leocal v. Ashcroft*, 543 U.S. 1, 11, n.8 (2004). This rule applies to the CFAA, just as any

---

Scottrade's CFAA claim against Genesis fails and must be dismissed."); *Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 383–385 (S.D.N.Y. 2010) (Computer systems administrator was authorized to access advertising company's database of customer leads and historical sales data, and thus did not violate the CFAA by allegedly using the database for an improper purpose, namely, to provide company's former employee and current competitor with confidential information); *Advanced Aerofoil Technologies, AG v. Todaro*, 2013 WL 410873, at *7 (S.D.N.Y. Jan. 30, 2013) ("This Court declines the opportunity to expand the CFAA to include situations where an employee takes confidential information, using authorization given to him and controlled by his employer[.]"); *Major, Lindsey & Africa, LLC v. Mahn*, 2010 WL 3959609, at *6 (S.D.N.Y. Sept. 7, 2010) (adopting reasoning of *Orbit One* "in view of the statute's legislative history, which reveals that Congress was endeavoring to outlaw computer hacking and electronic trespassing, not providing a new means of addressing the faithless employee situation").

other statute. *See WEC Carolina*, 687 F.3d at 204 (interpretation of the CFAA "applies uniformly" in both civil and criminal cases).

Thus, the Ninth Circuit in *Brekka*—a civil case—noted that "[n]othing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer," such as violating an employer's computer use policies. 581 F.3d at 1135. Three years later, the Ninth Circuit, sitting en banc in *Nosal*—a criminal case—affirmed a narrow construction of the phrase "exceeds authorized access" and rejected the argument that the bounds of an individual's "authorized access" turned on use restrictions imposed by an employer. *Nosal*, 676 F.3d at 857. The Ninth Circuit was explicitly concerned that interpreting the phrase "exceeds authorized access" to include violations of computer use policies "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id.* As the court noted, "[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose." *Id.*

After *Nosal*, the Fourth Circuit in *WEC Carolina* narrowly interpreted the terms "without authorization" and "exceeds authorized access" in the CFAA 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*, 687 F.3d at 206. In rejecting a broad definition of the terms, the Fourth Circuit stated that it was "unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy." *Id.* at 207.

Ultimately, *Brekka*, *Nosal*, *WEC Carolina*, and numerous other district courts narrowly interpret the CFAA not only to consistently apply Congress's intent to criminalize "hacking," but also to avoid an unconstitutionally vague interpretation of the statute that would criminalize common, innocuous behavior.[6]

---

[6] *See, e.g., Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 619 (E.D. Pa. 2013); *Scottrade, Inc.*, 774 F. Supp. 2d at 584; *Orbit One*, 692 F. Supp. 2d at 386; *Lewis-Burke Associates, LLC v. Widder*, 725 F. Supp. 2d 187, 194 (D.D.C. 2010); *Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc.*, 690 F. Supp. 2d 1267 (M.D. Ala. 2010); *Clarity Servs., Inc. v. Barney*, 698 F. Supp. 2d 1309, 1315 (M.D. Fla. 2010); *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 615 (M.D. Tenn. 2010); *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929, 934 (W.D. Tenn. 2008); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008); *Diamond Power Int'l., Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005); *see also Koch Industries, Inc. v. Does*, 2011 WL 1775765, at *8 (D. Utah May 9, 2011) (unpublished); *Nat'l City Bank, N.A. v. Republic Mortgage Home Loans, LLC*, 2010 WL 959925, at *3 (W.D. Wash. Mar. 12, 2010) (unpublished); *Jet One Grp., Inc. v. Halcyon Jet Holdings, Inc.*, 2009 WL 2524864, at *6 (E.D.N.Y. Aug. 14, 2009) (unpublished); *Brett Senior & Assocs., P.C. v. Fitzgerald*, 2007 WL 2043377, at *3 (E.D. Pa. July 13, 2007) (unpublished); *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006) (unpublished).

As acknowledged by the district court, however, some courts have broadly interpreted "without authorization" and "exceeds authorized access" to include acts of disloyal employees who misuse their access to corporate information. *See, e.g., United States v. John*, 597 F.3d 263, 272–73 (5th Cir. 2010); *Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582–84 (1st Cir. 2001); *see also United States v. Rodriguez*, 628 F.3d 1258, 1263-64 (11th Cir. 2010). But this broad interpretation of the CFAA has been rejected by more recent decisions like *WEC Carolina* and *Nosal*. *See WEC Carolina*, 687 F.3d at 206 (rejecting *Citrin* because it had "far-reaching effects unintended by Congress"); *Nosal*, 676 F.3d at 862-63 (rejecting *John, Citrin*, and *Rodriguez* for failing to "construe ambiguous criminal statutes narrowly so as to avoid 'making criminal law in Congress's stead'") (quoting *United States v. Santos*, 553 U.S. 507, 514 (2008)). As one district court noted, the courts that broadly interpret the CFAA "wrap the intent of the employees and use of the information into the CFAA despite the fact that the statute narrowly governs access, not use" and fail "to consider the broad consequences of incorporating intent into the definition of 'authorization.'" *Dresser-Rand*, 957 F. Supp. 2d at 619.

One of the cases relied upon by the district court, *United States v. John*, highlights the logical flaws inherent in the expansive theory of CFAA liability adopted by the district court below. There, the Fifth Circuit found that "[a]n

authorized computer user has 'reason to know' that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme." 597 F.3d at 273. But John's employer had given her credentials to access the bank's system, thus authorizing her to access the information within it. Making the determination of whether access is or is not authorized dependent on what an individual *should* know based on an employment agreement hinges CFAA liability on vague expectations of what is and is not criminal. As explained in more detail below, this raises constitutional concerns since the CFAA is "a criminal statute"—not some mere use policy or handbook—and it thus "must give fair warning of the conduct that it makes a crime[.]" *Bouie v. City of Columbia*, 378 U.S. 347, 350 (1964).

Moreover, to the extent Congress intended to capture within the CFAA's reach individuals who misuse their authorization in order to engage in fraudulent activity, the CFAA does that not in the term "exceeds authorized access," but in the provision of § 1030(a)(4) that explicitly requires fraudulent intent. *See* 18 U.S.C. § 1030(a)(4) (requiring a defendant to do an act "knowingly and with intent to defraud" which "furthers the intended fraud and obtains anything of value"). A "statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant[.]" *Corley v. United States*, 556 U.S. 303, 314 (2009) (citations and internal quotations omitted).

If a user's motivation for accessing information was a determining factor for whether data was unlawfully "accessed," the fraudulent intent language of § 1030(a)(4) would be superfluous. *See Brett Senior*, 2007 WL 2043377, at *4.

In short, this Court should adopt the reasoning of the Fourth and Ninth Circuits and explicitly reject the notion that a violation of a computer use policy can result in federal criminal liability.

B. This Case Presents a Mere Use Restriction.

The district court acknowledged that many courts have concluded that employees are not liable under the CFAA for misappropriating confidential information in violation of computer use policies. *See Valle,* 301 F.R.D. at 113–14 (collecting cases). But the district court distinguished these cases by concluding that the policy here imposed an *access* restriction rather than a *use* restriction. *Id.* at 115. Namely, the district court concluded that—unlike the cited "disloyal employee" cases—Mr. Valle did not have unrestricted access to the database in question because he "was limited to circumstances in which he had a valid law enforcement purpose for querying the system." *Id.* This misconstrued the nature of the restriction, which clearly governed the *use* of data rather than whether Mr. Valle could access it at all, and was thus a mere use restriction.

Courts have recognized that a computer restriction is not necessarily a true access restriction simply because it is labeled as such. In *Craigslist Inc. v. 3Taps*

Inc., 942 F. Supp. 2d 962 (N.D. Cal. 2013), the court found a website's terms of use—which provided rules about how site visitors could use data and prohibited the use of data in ways that violated the site's terms of use—to be "use" restrictions regardless of the fact that they were "framed in terms of 'access[.]'" 942 F. Supp. 2d at 969. Because the restrictions "depend[ed] entirely on the accessor's purpose," the court concluded that the terms of use contained "only 'use' restrictions, not true 'access' restrictions[.]" *Id.*; *see also Craigslist*, 964 F. Supp. 2d at 1185 ("It is true that simply denominating limitations as 'access restrictions' does not convert what is otherwise a use policy into an access restriction. . . . Thus, purported 'de-authorizations' buried in a website's terms of service may turn out to be use restrictions in disguise.") (citations and internal quotations omitted).[7]

[7] Similarly, in *Wentworth-Douglass Hospital v. Young & Novis Professional Association*, 2012 WL 2522963 (D.N.H. June 29, 2012) (unpublished), the court rejected the plaintiff's claim that the restriction at issue was an "access" restriction. According to the court, "the [plaintiff's] policy prohibiting employees from accessing company data *for the purpose* of copying it to an external storage device is not an 'access' restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access." 2012 WL 2522963, at *4. (emphasis added). The court held that "simply denominating limitations as 'access restrictions' does not convert what is otherwise a use policy into an access restriction." *Id.* The court further noted that the employee-defendants did not "hack" computers or otherwise circumvent technological access barriers in order to access the data in question. *Id.; see also Koch Industries*, 2011 WL 1775765, at *8 ("[P]laintiff's claim was really a claim that a user with authorized access had used

Here, Mr. Valle was authorized to access the database at issue—the National Crime Information Center ("NCIC") database—via NYPD's OFM software, and pursuant to NYPD policy, the OFM software and NCIC database could be accessed only "in the course of [an officer's] official duties and responsibilities." *Valle,* 301 F.R.D. 109 (internal quotations and citations omitted). The only restriction on Mr. Valle's access cited by the district court was the purpose for which he accessed the data; no data was off limits or otherwise inaccessible to him. Like *Craigslist*, since the restriction here depends entirely on the *purpose* underlying the use of the database on any particular instance, it is a *de facto* "use" restriction regardless of the terminology employed. *See Craigslist*, 942 F. Supp. 2d at 969. Indeed, unlike a true access restriction, Mr. Valle had unlimited access to the database, albeit for a valid law enforcement purposes, and did not have to hack or otherwise circumvent any technological access barriers to access it.

The district court's distinction between the restriction at issue here and the restrictions at issue in the "disloyal employee" cases referenced above is thus nonexistent. Indeed, the facts of this case are analogous to the employee cases cited by the district court. As an NYPD employee, Mr. Valle was subject to a database use policy no different than the corporate policies intended to limit the

---

the information in an unwanted manner, not a claim of unauthorized access or of exceeding authorized access.") (citing *Cvent,* 739 F. Supp. 2d at 933).

purposes for which corporate data could be used in the "disloyal employees" cases discussed earlier. *See WEC Carolina*, 687 F.3d at 202 ("WEC instituted policies that prohibited using the information without authorization or downloading it to a personal computer."); *Nosal*, 676 F.3d at 856 & n.1 (opening screen of proprietary database included warning: "'This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only.'"). The fact that the NYPD is a government entity rather than a private employer, or that the restrictions at issue here uses different terminology than in those cases, is irrelevant to the issue of whether there is CFAA liability. This case, like the ones discussed above, all involve an employer's attempt to control the *purpose* for which an authorized user can access a protected computer or database. They are therefore restrictions on *use*, not access, and cannot be the basis of CFAA liability.

II. THE DISTRICT COURT'S BROAD READING OF THE CFAA RENDERS IT UNCONSTITUTIONALLY VAGUE.

The competing interpretations of the CFAA discussed above clearly demonstrate that the CFAA is unconstitutionally vague. A criminal statute can be void for vagueness if it either fails to provide fair notice as to what is criminal or has the potential to lead to arbitrary and discriminatory prosecutions. *Skilling v. United States*, 561 U.S. 358, 412 (2010) (citing *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)). As a result, the rule of lenity calls for ambiguous criminal statutes—

particularly those that also impose civil liability—to be interpreted narrowly in favor of the defendant. *Santos*, 553 U.S. at 514. The rule of lenity "'ensures fair warning by so resolving ambiguity in a criminal statute as to apply [] only to conduct clearly covered.'" *United States v. Velastegui*, 199 F.3d 590, 593 (2d Cir. 1999) (quoting *United States v. Shabani*, 513 U.S. 10, 17 (1994)). Critically, the "rule of lenity not only ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize." *Nosal*, 676 F.3d at 863.

These vagueness concerns have caused the Fourth and Ninth Circuits, as well as many district courts, to apply the rule of lenity to specifically prohibit CFAA liability in situations involving use, rather than access, restrictions. *See, e.g., Nosal*, 676 F.3d at 862-64; *WEC Carolina*, 687 F.3d at 204. Indeed, pursuant to the district court's approach of imposing CFAA liability based on a violation of a computer use policy, the CFAA could very well be invalidated as vague for both failing to give adequate notice and risking arbitrary enforcement. Computer use policies—which are frequently unread, generally lengthy, and largely privately created, and can be altered without notice—fail to put individuals on adequate notice of what conduct is criminally prohibited. Furthermore, giving such documents the force of criminal law would turn a vast number of individuals into criminals. Indeed, § 1030(a)(2)(C) imposes criminal penalties on anyone who

"intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer." Nothing more is required. Ultimately, "identical words used in different parts of the same statute are generally presumed to have the same meaning." *IBP, Inc. v. Alvarez*, 546 U.S. 21, 34 (2005). Thus, the district court's expansive interpretation of the CFAA opens millions of ordinary individuals to CFAA liability for innocuous and everyday behavior, enabling the government to enforce the law in an arbitrary and discriminatory manner.[8]

A. Corporate Policies Do Not Provide Sufficient Notice of What Conduct Is Prohibited.

It is axiomatic that due process requires that criminal statutes provide ample notice of what conduct is prohibited. *See Connally v. Gen. Const. Co.*, 269 U.S. 385, 390 (1926). But basing criminal liability on policies instituted by an employer—be it the NYPD or a private corporation—confers employers the power to outlaw any conduct they wish without the sufficient clarity and specificity required of criminal law. As the Ninth Circuit has stated, "[s]ignificant notice problems arise if we allow criminal liability to turn on the vagaries of private

[8] This would be true even if the district court's decision applied only to computer use restrictions styled as computer access restrictions. Indeed, if upheld, employers and website owners will simply start drafting all computer use restrictions to read as "access restrictions" to preserve CFAA liability.

polices that are lengthy, opaque, subject to change and seldom read." *Nosal*, 676 F.3d at 860.

The Ninth Circuit in *Nosal* highlighted the problems with basing CFAA liability on computer use policies. It feared that such liability permits "private parties to manipulate their computer-use and personnel policies" so as to turn employer-employee and company-consumer relationships—relationships traditionally governed by tort and contract law—"into ones policed by the criminal law." *Nosal*, 676 F.3d at 860. It thereby grants employers the power to unilaterally "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id.* But the terms of corporate computer use policies are often vague and commonly unknown, and because employees retain the right to modify their corporate policies or terms of use at any time without notice, "behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever." *Id.* at 862. And while *Nosal* dealt with a use policy of a private corporation, the same concerns apply when dealing with a use policy created by a government employer.

Imposing criminal liability for violations of a computer use policy is especially troubling because these policies are aimed not at behavior, but rather purpose and intent. While the district court's interpretation of § 1030 may have been motivated by the fact of Mr. Valle's status as a police officer, its

interpretation applies in other contexts involving private employees. *See IBP*, *Inc.*, 546 U.S. at 34. Ultimately, that makes the CFAA's essential meaning depend on the existence and clarity of employment policies that may be aimed at employees' intentions rather than actions, and which may be drafted for reasons that have nothing to do with preventing the sort of unauthorized hacking, misuse, trespass, or theft of private data that the CFAA was intended to target. This result "gives employees insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited." Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1586 (2010).

Widely available sample Internet use policies further demonstrate the notice problems inherent in premising criminal liability on corporate use policies. One sample Internet and email usage policy, for example, warns that "Internet use, on Company time, is authorized to conduct Company business only," and "[o]nly people appropriately authorized, for Company purposes, may use the Internet[.]"[9] Another sample policy vaguely states that computer use restrictions include, "but are not limited to" seven specific prohibitions, as well as "any other activities

[9] Susan M. Heathfield, Internet and Email Policy, http://humanresources.about.com /od/policiesandsamples1/a/email_policy.htm (last visited Mar. 6, 2015).

designated as prohibited by the agency."[10] As indicated above, a policy's lack of specificity is often made worse by the fact that employers may reserve the right to change policies at any time, and not necessarily with advance notice.[11] Attaching criminal punishment to breaches of these vague, boilerplate policies would make it impossible for employees to know what conduct is criminally punishable at any given time.

B. Allowing CFAA Liability For Mere Use Restrictions Turns a Vast Number of Ordinary Individuals Into Criminals.

The district court's broad interpretation of the CFAA also renders the statute unconstitutionally vague because it permits capricious enforcement by prosecutors. As the Supreme Court has stated, "if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them." *Grayned v. Rockford*, 408 U.S. 104, 108 (1972). "A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an

[10] Virginia Dep't of Human Resource Management, Use of the Internet and Electronic Communications Systems, http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf?sfvrsn=2 (last visited Mar. 6, 2015).

[11] *See, e.g.*, Employee Handbook, Policies and Procedures, http://www.hrvillage.com/PandP/all.htm (last visited Mar. 6, 2015) ("The policies stated in this handbook are subject to change at any time at the sole discretion of the Company. From time to time, you may receive updated information regarding any changes in policy."); Dartmouth College, Employment Policies and Procedures Manual, http://www.dartmouth.edu/~hrs/policy (last visited Mar. 6, 2015) ("The policies are intended as guidelines only, and they may be modified, supplemented, or revoked at any time at the College's discretion.").

ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application." *Id*. at 108–09.

Here, the district court's decision permits arbitrary and discriminatory enforcement by expanding the scope of CFAA liability to cover millions of ordinary individuals who violate computer use restrictions every day via innocuous and ordinary—indeed, routine—online behaviors such as sending personal email or checking the score of a baseball game on ESPN.com. *See Nosal*, 676 F.3d at 860. As the Ninth Circuit noted in *Nosal*, "[m]inds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights." *Id.*

Although employees are seldom disciplined for the occasional use of work computers for personal purposes, such activities are routinely prohibited by corporate computer use policies. Nevertheless, under the district court's broad interpretation of the CFAA, "such minor dalliances would become federal crimes." *Id*. As the Fourth Circuit has noted, the "deficiency" of imposing liability for mere use restrictions means "any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy" would be left "without any authorization to access his employer's computer systems." *WEC Carolina*, 687 F.3d at 206. In this way, the district court turns the CFAA on its

head by allowing employers rather than Congress to unilaterally decide what behavior is "authorized" and what behavior constitutes a serious federal crime activity—opening millions of individual employees to CFAA liability.

The district court's sweeping interpretation of the CFAA creates the potential for draconian results not only in the context of employees who momentarily stray from their work duties, but also in the context of Internet users who unknowingly violate a website's terms of use. Namely, the district court's holding that a person "exceeds authorized access" if he violates a policy regarding the use of a computer that he is otherwise authorized to access could be extended to an Internet user who accesses a website in violation of a written terms of service. The district court's expansive reading of the CFAA thus opens the door to turning millions of individual Internet users—not just millions of individual employees—into criminals for typical and routine Internet activity.

Through interpreting the CFAA to "criminalize a broad range of day-to-day activities," the district court subjects employees and Internet users alike to prosecution at the whim of prosecutors, who can pick and choose which violations they wish to penalize. *See United States v. Kozminski*, 487 U.S. 931, 949 (1988). As the Ninth Circuit noted, such broad statutory interpretation "'delegate[s] to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as

crimes' and would 'subject individuals to the risk of arbitrary or discriminatory prosecution and conviction.'" *Nosal*, 676 F.3d at 862 (citing *Kozminski*, 487 U.S. at 949). Indeed, by giving that much power to prosecutors, the district court here has "invit[ed] discriminatory and arbitrary enforcement." *Id.*

For example, many social media websites prohibit lying about or otherwise misrepresenting personal information.[12] Under the district court's holding, "[t]he difference between puffery and prosecution may depend on whether you happen to be someone an AUSA has reason to go after." *Nosal*, 676 F.3d at 862. It is this very potential for abuse that has led most courts, as explained earlier, to reject the district court's broad interpretation of "exceeds unauthorized access." Ultimately, as the Supreme Court has noted, the Constitution "does not leave us at the mercy of *noblesse oblige*" by the government. *United States v. Stevens,* 559 U.S. 460, 480 (2010); *see also Nosal*, 676 F.3d at 862. An unconstitutional interpretation of a statute should not be upheld "merely because the Government promised to use it responsibly." *Stevens*, 559 U.S. at 480.

In order to avoid fatal vagueness problems, the CFAA must be narrowly applied to only the behavior Congress clearly intended to criminalize—"hacking." Importantly, a narrow application of the CFAA does not leave employers or

[12] *See, e.g.,* Facebook's Statement of Rights and Responsibilities, 4.1 ("You will not provide any false personal information on Facebook[.]") (last revised January 30, 2015), *available at* https://www.facebook.com/legal/terms.

website owners without legal recourse; it merely limits the CFAA to its intended purpose. Employers and website owners will remain free to bring legal action against employees or Internet users in connection with beaches of contract or misappropriations of trade secrets—actions which the CFAA was never intended to address. *See Nosal*, 676 F.3d at 863 (noting that the CFAA was *not* intended to punish "misappropriation of trade secrets—a subject Congress has dealt with elsewhere" in 18 U.S.C. § 1832).

This Court must therefore reject the district court's broad construction of the CFAA and reverse the denial of Mr. Valle's motion for acquittal of his CFAA conviction. Any other outcome will leave individuals unsure of what conduct could give rise to criminal liability under the CFAA and will almost certainly result in arbitrary enforcement of an already worrisomely broad statute.

CONCLUSION

In denying Mr. Valle's motion for acquittal on his CFAA conviction, the district court ignored the fact that the restriction at issue is a clear *use* restriction—not an *access* restriction. Through effectively ruling that a use restriction can give rise to CFAA liability, the district court's holding directly conflicts with the text and purpose of the CFAA and inadvertently extends the CFAA to make criminals out of millions of ordinary Americans. The district court's denial of Mr. Valle's motion for acquittal on the CFAA count must therefore be reversed.

Dated: March 9, 2015

Respectfully submitted,

By: */s/ Hanni Fakhoury*

Hanni Fakhoury
Jamie L. Williams
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109-7701
Telephone: (415) 436-9333
hanni@eff.org

Richard D. Willstatter
Amicus Committee Vice Chair, Second Circuit
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
Green & Willstatter
200 Mamaroneck Avenue,
Suite 605
White Plains, NY 10601
(914) 948-5656
willstatter@msn.com

Harley Geiger
CENTER FOR DEMOCRACY & TECHNOLOGY
1634 I Street NW,
Suite 1100
Washington, D.C. 20006
(202) 637-9800
harley@cdt.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(a)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amici Curiae* Electronic Frontier Foundation, Center for Democracy & Technology, National Association of Criminal Defense Lawyers, and Scholars in Support of Defendant-Appellant Gilberto Valle complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,542 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: March 9, 2015

By: */s/ Hanni Fakhoury*
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on March 9, 2015, a true and correct copy of the foregoing Brief of *Amici Curiae* Electronic Frontier Foundation, Center for Democracy & Technology, National Association of Criminal Defense Lawyers, and Scholars in Support of Defendant-Appellant Gilberto Valle was served on all counsel of record in this appeal via CM/ECF pursuant to Second Circuit Rule 25.1(h)(1)-(2).

Dated: March 9, 2015

By: /s/ *Hanni Fakhoury*
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Curiae