United States Court of Appeals

for the

Third Circuit

Case No. 13-1816

UNITED STATES OF AMERICA

– v. –

ANDREW AUERNHEIMER

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY (WIGENTON, J.),
CRIMINAL NO. 11-CR-470 (SDW)

BRIEF OF *AMICUS CURIAE* NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF APPELLANT

STEVEN P. RAGLAND
JENNIFER A. HUBER
BEN D. ROTHSTEIN
KEKER & VAN NEST LLP
633 Battery Street
San Francisco, California 94111
Tel.: (415) 391-5400
Fax: (415) 397-7188

Attorneys for Amicus Curiae National Association of Criminal Defense Lawyers

Of Counsel:
JENNY CARROLL
Seton Hall University School of Law
Newark, New Jersey 07102

PETER GOLDBERGER
50 Rittenhouse Place
Ardmore, Pennsylvania 19003

Third Circuit Co-Vice-Chairs, National Association of Criminal Defense Lawyers Amicus Curiae Committee

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Federal Statutes

State Statutes

Federal Rules

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST OF AMICUS CURIAE[1]

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit corporation and the only national bar association working in the interest of public and private criminal defense attorneys and their clients. Founded in 1958, NACDL was established to ensure justice and due process for the accused; to foster the integrity, independence, and expertise of the criminal defense profession; and to promote the proper and fair administration of justice. NACDL has more than 13,000 members nationwide, joined by 90 local, state, and international affiliate organizations with more than 35,000 members. NACDL members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges who are committed to preserving fairness and due process in the criminal justice system. This Court has often permitted NACDL to appear as an amicus curiae in important cases, as have other Federal Circuits and the United States Supreme Court. NACDL has a significant interest in guaranteeing criminal defendants their rights under the Due Process and Venue Clauses of the United States Constitution, which are the central issues addressed in this brief. NACDL urges this Court to fortify those rights.

[1] Pursuant to Federal Rule of Appellate Procedure 29(a), this brief is filed with the consent of all parties. No counsel for a party authored this brief in whole or in part, nor did any person or entity, other than amici or their counsel, make a monetary contribution to the preparation or submission of this brief.

INTRODUCTION & SUMMARY OF ARGUMENT

The Computer Fraud and Abuse Act ("CFAA"), enacted in 1984, broadly criminalizes accessing a computer "without authorization," but does not say what that means. Today, nearly thirty years after the CFAA was enacted, Americans are routinely using computers for countless purposes—for work, school, entertainment, news, commerce, to catch up with friends, and to share ideas. We carry computers everywhere in our pockets and purses in the form of smartphones and tablets. Computers permeate our lives in ways that we could not have predicted thirty years ago. Because our computers are now interconnected through the Internet, an open public forum, America's computer crime law must provide fair notice of when accessing a computer is and is not criminal.

Amicus NACDL addresses two fundamental constitutional errors in Mr. Auernheimer's convictions. First, the district court's reading of the CFAA criminalizes routine Internet use, inviting arbitrary and discriminatory enforcement. By construing "access [to a computer] without authorization" as "access [to] a computer without approval or permission," the district court's interpretation of 18 U.S.C. § 1030(a)(2)(C) renders that provision unconstitutionally vague by permitting prosecution of Internet users merely because they view information against the wishes of a website host or computer owner—regardless of whether users have any notice of those wishes. The Fifth

Amendment's Due Process Clause and the legislative history of the CFAA compel a more narrow interpretation of "access[ing] without authorization" as computer *hacking* or, more precisely, circumventing a code-based barrier. The district court erred when it instructed the jury otherwise, and Mr. Auernheimer's charged conduct—viewing information on a publicly-available website—cannot, as a matter of law, constitute unauthorized access under the CFAA.

Second, amicus NACDL urges reversal because the district court should not have permitted this case to proceed in the District of New Jersey. Federal law, 18 U.S.C. § 3237(a), limits venue to jurisdictions in which the defendant committed a "conduct element" of the charged offense. Neither Mr. Auernheimer, nor his alleged co-conspirator, Daniel Spitler, nor the accessed AT&T computers were located in New Jersey. Nevertheless, the district court allowed the case to proceed there.

Given the interconnectedness of the Internet, the district court's misapplication of venue principles would allow prosecutors to aggressively forum shop without regard to the rights of the accused. A defendant charged with a computer crime—like any defendant—has a constitutional right to be tried in the district where his or her alleged crime was committed.

ARGUMENT FOR AMICUS CURIAE

I. THE FIFTH AMENDMENT'S DUE PROCESS CLAUSE REQUIRES A NARROW INTERPRETATION OF "WITHOUT AUTHORIZATION" UNDER THE CFAA.

The Internet's fundamental characteristics—its openness and interconnectedness—have made it a transformational technology. Young people today have never known a world without an open Internet, its endless troves of information, and the ability to use it as a platform to develop and share ideas. When an individual or entity puts information on the Internet, the information becomes publicly available unless proactive steps are taken to protect or secure it. Congress recognized this as early as 1986, when it recommended the first amendments to the CFAA, and endorsed the view that "the most effective means of preventing and deterring computer crime is *more comprehensive and effective self-protection by private business.*"[2] Computer crime laws therefore serve primarily to reinforce "security improvement programs," rather than to create independent restrictions on accessing otherwise publicly-viewable information.[3] After all, no company or individual is required to place troves of information on the Internet. Rather, persons and entities choose to do so for their own benefit and/or ends.

---

[2] S. Rep. No. 99-432, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2481 (citation and quotation marks omitted) (emphasis added).

[3] *Id.*

The district court flouted these principles in construing "access without authorization" as "access[ing] a computer without approval or permission." App2. 704.[4] This expansive reading, relying on subjective notions of approval and consent, potentially criminalizes millions of computer users for merely viewing publicly-available information on the Internet. The district court's interpretation of the CFAA requires Internet users to guess and heed the wishes of computer owners and website hosts (whether communicated to users or not), and thus renders the statute unconstitutionally vague under the Due Process Clause of the Fifth Amendment.

Revealingly, the district court's broad reading of the CFAA would criminalize Internet searches for public information that the government itself has endorsed as legal. A recently de-classified National Security Agency (NSA) "Guide to Internet Research" teaches government researchers how to construct Google Internet searches to find information "not meant to be made available to the public."[5] A government employee using this technique could, for example, search for "sensitive information about a company" by creating a complex search

[4] "App1." and "App.2" refer to Appellant Andrew Auernheimer's Appendix Volumes 1 and 2, filed July 1, 2013.

[5] [Unknown Author], *Untangling the Web: A Guide to Internet Research* 177 (2007), Addendum of Amicus Curiae NACDL in Support of Appellant (hereinafter, "Add.") 14.

string to locate Excel spreadsheets marked with the word "Confidential."[6] Commenting on the legality of this technique, the NSA states:

> [T]his is not hacking in the sense that most people use the term, i.e., gaining access to a computer or data on a computer illegally or without authorization. Nothing I am going to describe to you is illegal, nor does it in any way involve accessing unauthorized data. "Google (or search engine) hacking" ***involves using publicly available search engines to access publicly available information that almost certainly was not intended for public distribution. In short, it's using clever but legal techniques to find information that doesn't belong on the public Internet***.[7]

In other words, the government teaches its own that they need not heed the wishes of website hosts, and emphasizes that information is public if not sufficiently protected—regardless of the host's intent. Given the public nature of the Internet, and the fact that individuals and entities are free to avoid posting material online altogether, this makes sense.

Yet here, the district court's elastic reading of the CFAA would allow government prosecutors to choose to target citizens who employ the very methods endorsed in the government's manual. The district court's construction, like similar judicial efforts to construe "without authorization" based on notions of third party consent—"affords too much discretion to the police and too little notice

---

[6] *Id.*

[7] *Id.* at 175 (emphasis added), Add. 12.

to citizens[.]" *See City of Chicago v. Morales*, 527 U.S. 41, 64 (1999). So construed, the statute would be unconstitutionally vague under the Due Process Clause. *See id.* To cure this constitutional defect, the Court must adopt a construction of "access without authorization" that is objectively knowable and reasonably limited in scope. Therefore, in the context of accessing information over the Internet, amicus NACDL urges the Court to construe "access without authorization" as the intentional circumvention of code-based barriers to access—a standard that narrowly focuses the CFAA on hacking activity.

A. The Legislative History and Breadth of the CFAA Make "Authorization" the Most Important Term in Defining a § 1030(A)(2)(C) Offense.

Mr. Auernheimer was charged under 18 U.S.C. § 1030(a)(2)(C), which penalizes "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." Despite its originally narrow focus on criminalizing hacking into government computers or financial institution servers, a series of amendments have vastly expanded the CFAA to potentially criminalize everyday computer use. These amendments, and the law as a whole, must therefore be narrowly construed by the Courts to avoid constitutional infirmity.

Congress's primary motivation in enacting the first federal computer crime law in 1984 was to criminalize "the activities of so-called 'hackers' who have been

able to access (trespass into) both private and public computer systems."[8] The House Judiciary Committee, in recommending enactment of 18 U.S.C. § 1030, explained that the newfound ability of "hackers" to use personal computers to circumvent "identification code/password system[s]" had enabled a "recent flurry of electronic trespassing incidents."[9] Targeting this conduct, the Committee stated: "[T]he conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense."[10] When enacted in 1984, 18 U.S.C. § 1030 was narrowly limited to computer misuse to obtain national security secrets or personal financial records, or hacking into government computers. *Id.*

---

[8] H.R. Rep. No. 98-894, at 10 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695; *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.").

[9] 1984 U.S.C.C.A.N. at 3696 (describing the hacker threat by reference to the film WAR GAMES (1983), "show[ing] a realistic representation of the … access capabilities of the personal computer"); *see also* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 Md. L. Rev. 320, 368 (2004) (explaining that CFAA "was never intended to afford website owners with a method for obtaining absolute control over access to and use of information they have chosen to post on their publicly available Internet sites"); Mark A. Lemley, *Place and Cyberspace*, 91 Cal. L. Rev. 521, 528 (March 2003) (noting that CFAA "was designed to punish malicious hackers").

[10] 1984 U.S.C.C.A.N. at 3706.

Two years later, the Senate Judiciary Committee report recommending the 1986 amendments to the CFAA discussed the access-without-authorization provision under which the government charged Mr. Auernheimer:

> The premise of 18 U.S.C. 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions. This protection is imperative in light of the sensitive and personal financial information contained in such computer files.[11]

Since stealing this information did not require asportation—*viz.*, the physical removal of goods—the Committee intended "to make clear that 'obtaining information' in this context includes mere observation of data."[12]

In 1996, Congress dramatically expanded the CFAA by extending its reach to any "protected computer," a term that included any computer "which is used in interstate or foreign commerce or communication[.]"[13] The 1996 amendments also expanded § 1030(a)(2)—originally prohibiting only unauthorized access to obtain financial records from financial institutions, card issuers, or consumer reporting agencies[14]—to include unauthorized access to obtain *any* information of *any* kind from any "protected computer."

---

[11] S. Rep. No. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484.

[12] *Id.* at 7.

[13] 18 U.S.C. § 1030(e)(2) (Supp. II 1996).

[14] 18 U.S.C. § 1030(a)(2) (Supp. II 1996).

The purpose of these expansions was to protect additional types of "vital" private information from hacking, rather than just credit records and financial information:

> Section 1030(a)(2) currently gives special protection only to information on the computer systems of financial institutions and consumer reporting agencies, because of their significance to our country's economy and the privacy of our citizens. Yet, increasingly computer systems provide the vital backbone to many other industries, such as transportation, power supply systems, and telecommunications. [Thus, t]he bill would amend section 1030(a)(2) and extend its coverage to information held on (1) Federal Government computers and (2) computers used in interstate or foreign commerce on communications, if the conduct involved an interstate or foreign communication.[15]

Since the legislature had already interpreted "obtain[ing]" information to include simply reading it, and since nearly all Internet communications are interstate communications, the language employed by the 1996 amendments essentially extended § 1030(a)(2) to *any* unauthorized access of a computer occurring over the Internet.[16]

---

[15] S. Rep. No. 104-357, at 7 (1996), 1996 WL 492169.

[16] Courts and commentators have frequently observed that the term "protected computer" now extends to any "functioning, networked computer[.]" Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. Ill. J.L. Tech. & Pol'y 429, 433 (2009); *see also United States v. Fowler*, No. 8:10cr65, 2010 WL 4269618, at *2 (M.D. Fla. Oct. 25, 2010) (listing cases).

Combined with the ubiquitous use of computers, smartphones, tablets, or any other Internet-enabled device in today's world, the breadth of the CFAA places special importance on the meaning of "authorization." A broad construction of "authorization" potentially criminalizes an enormous amount of routine Internet activity and would render the CFAA unconstitutionally vague.

B. The District Court's Construction of "Access Without Authorization" Renders the CFAA Unconstitutionally Vague.

To satisfy due process, "a penal statute [must] define the criminal offense [1] with sufficient definiteness that ordinary people can understand what conduct is prohibited and [2] in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983); *see also United States v. Mastronardo*, 849 F.2d 799, 805 (3d Cir. 1988) (citations omitted) (recognizing that criminal statutes must be strictly construed and must define criminal offenses "with sufficient definiteness that ordinary people can understand what conduct is prohibited").

In the context of an Internet user's access to information on a public website, previous judicial efforts to construe "authorization" under § 1030(a)(2)(C) fail to provide clear guidance to courts or ordinary citizens within the CFAA's reach.[17]

[17] *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2007) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive.").

The problem is that restricting access to publicly-viewable information on the Internet based on subjective notions of consent inevitably fails to provide adequate notice to computer users, and criminalizes common Internet use.

For example, the Fifth Circuit has approached the "authorization" question by reference to whether a user's access constitutes an "intended use" of a computer owner or website host. *See United States v. Phillips*, 477 F.3d 215, 220 (5th Cir. 2007) (analyzing "scope of a user's authorization to access a protected computer on the basis of the expected norms of the intended use or the nature of the relationship established between the computer owner and the user"); *see also United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010). This approach, which prohibits accessing public websites based on the intention of the website host (whether communicated or not), has disturbing implications. The "intended use" standard would, for example, criminalize a journalist's visit to an individual's personal blog for the purpose of writing an article. Similarly, it would criminalize the use of an advanced search string—a technique expressly taught by the NSA (as discussed above)—to scan the Internet for readily-available information that a computer owner might have intended to keep private, but failed to secure. In either instance, the computer user may be visiting a website where, based on the website host's expectations, access is "without authorization." Most Americans surf the Internet every day. How are they to know the website owner's wishes? And, why

should the burden be on visitors to this vast public forum to divine the intent of a website host who chose to post information online?

Some courts have adopted a standard under which a computer user lacks authorization to access a computer if the user's access violates a website's terms of use. *See e.g., EF Cultural Travel BV v. Zefer Corp*., 318 F.3d 58, 62 (1st Cir. 2003) (noting that a lack of authorization could be established by a violation of "an explicit statement on the website restricting access"); *Register.com, Inc. v. Verio, Inc*., 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000).

Although this standard at least requires a written expression of the terms of the computer owner's approval or permission (a requirement not imposed by the district court here), it too has disturbing implications. As the United States Court of Appeals for the Ninth Circuit recently observed,

> Whenever we access a web page, commence a download, post a message on somebody's Facebook wall, shop on Amazon, bid on eBay, publish a blog, rate a movie on IMDb, read www.NYT.com, watch YouTube and do the thousands of other things we routinely do online, we are using one computer to send commands to other computers at remote locations. Our access to those remote computers is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands.

United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012). Problematically, terms of use are often vague themselves (*e.g*., a prohibition on posting "offensive content" in a chat room) and place website hosts in charge of defining criminal

conduct. *United States v. Drew*, 259 F.R.D. 449, 464-65 (C.D. Cal. 2009). Indeed, terms of use often prohibit routine Internet use, from the mundane (*e.g.*, exaggerating about oneself on a dating website) to the self-protective (*e.g.*, providing an inaccurate birth date to a website to guard against identity theft). *See, e.g.*, *Nosal*, 676 F.3d at 861-62 (listing examples of common—and commonly prohibited—Internet uses). Moreover, such a standard allows "behavior that wasn't criminal yesterday [to] become criminal today without an Act of Congress, and without any notice whatsoever." *Id.* at 862. Since there are no other textual limitations on the scope of conduct prohibited under § 1030(a)(2), the terms-of-use standard makes "section 1030(a)(2)(C) [into] a law 'that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]." *Drew*, 259 F.R.D. at 467 (citing *City of Chicago*, 527 U.S. at 64).

The *Drew* case exemplifies the potential for prosecutorial abuse when a minor terms-of-use violation presents salacious facts. The Justice Department charged Lori Drew with violating § 1030(a)(2)(C) for creating a fake profile on MySpace.com to contact thirteen-year-old Megan Meier. *Id.* at 452. After several weeks of communicating with Meier through the fake profile of "Josh Evans," Drew sent a cruel message to Meier ending the relationship. *Id.* This conduct—common insofar as it involved providing misleading information about oneself on a social networking site—attracted the government's attention when Meier

tragically committed suicide shortly after she received Drew's message. Lacking any other basis for calling Drew into federal court, the government charged her under § 1030(a)(2)(C) for violating MySpace.com's terms of service, which prohibit lying about identifying information. *Id.* at 452-53. Although the jury convicted Drew at trial, the district court overturned the verdict. The *Drew* case underscores the risk that the government will take advantage of a broad interpretation of "authorization" when it has a reason to—even if the offense has nothing to do with traditional hacking—and even if it is the wrong tool for the case.

Drew is not an outlier, and it portends prosecutors' increasing and scattershot use of the CFAA. The CFAA is same law under which Internet activist Aaron Swartz was charged for downloading academic articles from a publicly-available Massachusetts Institute of Technology computer archive. Many viewed the prosecution of Mr. Swartz as an ill-advised attempt to turn innocuous Internet mischief into a federal crime carrying a harsh penalty. Facing the prospect of a lengthy prison sentence, Swartz committed suicide in January 2013, prompting claims of prosecutorial overreach and calls to reform the law.[18]

[18] *See, e.g.,* Zoe Lofgren and Ron Wyden, *Introducing Aaron's Law, a Desperately Needed Reform of the Computer Fraud and Abuse Act*, WIRED, June 20, 2013, Add. 23-26; Tim Wu, *Fixing the Worst Law in Technology*, THE NEW YORKER, March 18, 2013, Add. 27-29.

Here, like the prosecution's theory in *Drew*, the district court's instruction construing "access without authorization" as "access[ing] a computer without approval or permission" rests on the consent of the computer owner. But in fact, the district court's instruction here was substantially *broader* because it did not require that the computer owner provide any written statement of the terms of approval or permission, nor was it based on "expected norms" of computer use; rather, it is entirely subjective. Thus, under the district court's interpretation of the CFAA, a computer user violates the law by visiting a website without the website host's permission—*regardless of whether the user has any reason to know that he or she lacks permission*.[19] This standard is patently defective under the Due Process Clause. As the *Nosal* court observed, while the government may assure us that, whatever the scope of the CFAA, it won't prosecute minor violations, "we shouldn't have to live at the mercy of our local prosecutor." *Nosal*, 676 F.3d at

[19] Should the government rely on the instruction given for the New Jersey crime, 2C:20-31(a) (disclosure of data from wrongful access, used to enhance Count 1 to a felony), to argue that the jury was in fact instructed that "access without authorization" means "access without password-based permission or code-based permission…" the argument is unavailing. *See* App2. 704-706. The New Jersey instruction required the jury to find only that Mr. Auernheimer "purposely or knowingly *and* without authorization, accesses[.]" *Id.* (emphasis added). Because the instruction did not connect *any* state-of-mind to the absence of authorization, it fails under § 1030(a)(2)(C) requiring intentionally accessing without authorization. *See* S. Rep. No. 99-432, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483 ("[I]ntentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe.").

862. Accordingly, "access without authorization" must be construed to provide Internet users with sufficient notice and impose reasonable constraints on law enforcement.

C. This Court Should Adopt a Code-Based Approach to Avoid the Vagueness Problems Inherent in the Approval- And Permission-Based Approaches.

The Third Circuit has not issued an opinion construing "access without authorization" under the CFAA. *See CollegeSource, Inc. v. AcademyOne, Inc.*, No. 10cv3542, 2012 WL 5269213, at *13 (E.D. Pa. Oct. 25, 2012).[20] In light of the legislative history of the CFAA, vagueness concerns, and the tenet that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity,"[21] amicus NACDL urges the Court to adopt the only sound interpretation of "access without authorization" articulated in CFAA decisions: the intentional circumvention of code-based barriers to access. This standard uses "code" in its ordinary sense of encryption and similar security measures, not in the computer-programming sense of the word (the language used to write a software program) or legal sense (a compilation of laws), and is intended for use in cases where the

[20] The primary Third Circuit case on the CFAA, *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504 (3d Cir. 2005), does not address the meaning of "without authorization" or "exceeds authorized access."

[21] *Skilling v. United States*, __ U.S. __, 130 S.Ct. 2896, 2932 (2010); *see also United States v. Introcaso*, 506 F.3d 260, 269-70 (3d Cir. 2007).

charged conduct involves accessing a computer remotely over the public Internet (rather than, for example, physically breaking into a facility to access a computer).

This construction has been applied by the Sixth Circuit and in several lower court decisions in remote-access cases. In *Pulte Homes, Inc. v Laborers' International Union of North America*, 648 F.3d 295 (6th Cir. 2011), the court held that a union's coordinated and partially-automated campaign to bombard an employer's phone and email systems did not violate the CFAA. The court reasoned that the employer "used unprotected public communications systems, which defeats [its] allegation that [the union] accessed its computers 'without authorization.'" 648 F.3d at 304. Citing the absence of any "password or code" requirement, the Sixth Circuit analogized the employer's communications systems to "an unprotected website" that was "open to the public," and reasoned that the union's multitudinous phone calls and emails to the employer were inherently "authorized." *Id.*

In *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 933 (E.D. Va. 2010), the court held that "scraping" information (copying large amounts of information, by use of a code-based program) from a business competitor's non-password protected website did not constitute unauthorized access under the CFAA, even though it violated the competitor's website's terms of service: "Cvent's website in fact takes no affirmative steps to screen competitors from accessing its

information. . . . [A]nyone, including competitors in the field of event planning, may access and search [Cvent's website] at will." *Id.* at 932.

Similarly, in *Southwest Airlines Co. v. BoardFirst, L.L.C.*,[22] the court noted that the plaintiff's "without authorization" theory was problematic: "BoardFirst or any other computer user obviously has the *ability* to make use of the southwest.com given the fact that it is a publicly available website which is not protected by any sort of code or password."[23] In that case, the defendant automatically checked-in Southwest passengers exactly 24 hours before their flight for a small fee, guaranteeing an advantageous position in the boarding line. While BoardFirst's efforts to profit from Southwest's website were prohibited by the southwest.com terms of use, "[i]n no sense can Boardfirst be considered an 'outside hacker[] who break[s] into a computer' given that southwest.com is a publicly available website that anyone can access and use."[24]

At least one criminal case in the Third Circuit has also suggested the code-based approach. In *United States v. Lowson*, No. 2:10cr00114 (D.N.J. Oct. 12, 2010), the defendants were charged with circumventing code-based security measures put in place by online ticket vendors (such as Ticketmaster) in order to buy large blocks of tickets to re-sell on the secondary market. Addressing

[22] No. 3:06cv0891, 2007 WL 4823761 (N.D. Tex. Sept. 12, 2007).

[23] *Id.* at 14.

[24] *Id.* (quoting S. Rep. No. 104-357, at 11 (1996), 1996 WL 492169).

"whether the scheme and conduct alleged here is merely an egregious breach of contract based on violations of the terms of service on Ticketmaster's website, or something criminal[,]" the court upheld the CFAA charges only because the government had alleged "actions taken by defendants to defeat code-based security restrictions on Ticketmaster's websites."[25]

Notably, three of the above cases are civil cases, which do not implicate the same due process principles at issue here. In a criminal case, of course, it is far more important that the Court adopt an interpretation of the CFAA that provides sufficient notice to computer users and clear guidance to law enforcement. While typical computer users cannot be expected to know in every instance whether their Internet use violates a website's terms of service or contradicts the "approval" or "permission" of a website host, a user certainly knows whether he or she has stolen a password or written a computer program to break through a security firewall. And since a code-based construction limits the CFAA's prohibitions to a discrete set of Internet activities that do not implicate visiting unprotected websites that are open to the public, it eliminates the government's carte blanche to prosecute activities akin to the "clever but legal" Internet searches urged in its own NSA manual.[26] Moreover, this construction comports with the CFAA's original purpose

[25] *See* Slip op. at 8. Add. 37.

[26] *See supra,* n.5.

as an anti-hacking statute, and thus preserves the core of the CFAA's protection. *See supra*, Section I.A. Finally, this construction is necessary from a public policy perspective because it requires website hosts who take advantage of the public Internet to take affirmative steps to protect information they wish to keep private.

II. THE DISTRICT COURT'S FINDING THAT VENUE WAS PROPER EXCEEDS CONSTITUTIONAL LIMITATIONS AND INVITES PROSECUTORIAL FORUM-SHOPPING.

As this Circuit has emphasized, "[p]roper venue in criminal trials is more than just a procedural requirement; it is a safeguard guaranteed twice by the United States Constitution itself." *United States v. Baxter*, 884 F.2d 734, 736 (3d Cir. 1989); *see also Travis v. United States*, 364 U.S. 631, 634 (1961) ("[Q]uestions of venue are more than matters of mere procedure. 'They raise deep issues of public policy in the light of which legislation must be construed.'" (quoting *United States v. Johnson*, 323 U.S. 273, 275 (1944)). Despite this long line of judicial guidance, and in violation of the constitutional rights of the accused, the district court permitted this case to proceed in a forum with no connection whatsoever to the essential conduct elements of the charged offenses. The district court justified its flawed venue ruling by reasoning that "Defendant's purported conduct—knowing disclosure of personal identifying information to the press—*affected* thousands of New Jersey residents and violated New Jersey law."[27] In so holding, the district

[27] *See* App1. 26 (emphasis added) (citing *United States v. Root*, 585 F.3d 145, 156

court adopted the government's expansive view that venue is proper in any district wherever residents are ostensibly "affected." App2. 100. This cannot be the law.

There are two fundamental flaws in the district court's approach. First, it permits a criminal trial to occur outside the jurisdiction where a defendant committed the "essential conduct elements" of the charged crime, and thus exceeds constitutional limitations on venue. *See United States v. Rodriguez-Moreno*, 526 U.S. 275, 280 (1999). Second, given the interconnected nature of the Internet, it causes extreme prejudice to the accused because it allows prosecutors to bring charges in virtually any district, and thus to cherry-pick the most advantageous forum—regardless of whether it is foreseeable or reasonable to defend against a trial there. To avoid these infirmities, venue for a § 1030(a)(2)(C) charge should be limited to jurisdictions in which the defendant either accessed a computer or obtained information—regardless of whether some individual in a distant jurisdiction may be somehow "affected." As such, New Jersey was not a proper forum for the government's charges against Mr. Auernheimer.

(3d Cir. 2009) ("The locality of a crime for the purpose of venue extends 'over the whole area through which force propelled by an offender operates.'")).

A. Venue Under § 1030(a)(2)(C) Must Be Limited Either to the District Where the Defendant Performed the Act of Accessing a Computer, or the District Where the Accessed Computer is Located.

The Constitution and the Bill of Rights guarantee a criminal defendant both the right to trial in, and the right to a jury drawn from, the state where the alleged crime "shall have been committed."[28] These limits ensure that "the accused not be subject to the hardship of being tried in a district remote from where the crime was committed[,]"[29] and they prevent the government from shopping for its "choice of 'a tribunal favorable' to it."[30] Indeed, the Supreme Court has long admonished that provisions implicating venue must be narrowly construed. *See United States v. Johnson*, 323 U.S. at 276.

Where a criminal statute includes no specific venue provision, and the charged crime occurs in more than one jurisdiction, the crime "may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a). To meet constitutional strictures, courts must limit venue under this provision to those jurisdictions where the defendant committed the "essential conduct elements" of the charged crime—that is,

---

[28] U.S. Const. art. III, § 2, cl. 3; U.S. Const. amend. VI; *see also* Fed. R. Crim. P. 18 ("Unless a statute or these rules permit otherwise, the government must prosecute an offense in a district where the offense was committed.").

[29] *United States v. Saavedra*, 223 F.3d 85, 88 (2d Cir. 2000).

[30] *Travis v. United States*, 364 U.S. 631, 634 (1961) (quoting *United States v. Johnson*, 323 U.S. at 275).

elements requiring the government to prove *conduct* by the defendant, not additional circumstances. *Rodriguez-Moreno*, 526 U.S. at 280; *see also United States v. Cabrales*, 524 U.S. 1 (1998).

The central allegation in both counts of the superseding indictment was that Mr. Auernheimer violated § 1030(a)(2)(C) of the CFAA, which penalizes "[w]hoever … (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … (C) information from any protected computer[.]"[31] With respect to Mr. Auernheimer's conduct, the government was thus required to prove that: he intentionally accessed a protected computer without authorization (or exceeded authorized access) and obtained information. Venue was therefore proper only where the protected computer was located or where the information was obtained—*i.e.*, the location of Mr. Auernheimer or his alleged co-conspirators when the information was obtained.

[31] Count 1 charged that Mr. Auernheimer conspired, under 18 U.S.C. § 371, to violate § 1030(a)(2)(C). Count 1 further charged a felony enhancement of §1030(a)(2)(C) under 18 U.S.C. § 1030(c)(2)(B)(ii), because allegedly Mr. Auernheimer violated § 1030(a)(2)(C) in furtherance of disclosing the email addresses in violation of New Jersey state law. Count 2 charged Mr. Auernheimer under 18 U.S.C. § 1028(a)(7), a provision of the federal identity theft statute prohibiting using, "without lawful authority, a means of identification of another person with the intent to commit . . . a violation of federal law." The predicate "violation of federal law" alleged in Count 2 was the § 1030(a)(2)(C) charge. Thus, the core allegation in both counts was "access without authorization" under § 1030(a)(2)(C).

No part of the essential conduct under § 1030(a)(2)(C) occurred in New Jersey. The "accessed" AT&T servers were located in Dallas, Texas and Atlanta, Georgia. App2. 434-435, 443-444. During the relevant time period, Mr. Auernheimer was located in Arkansas and his alleged co-conspirator was in California. App2. 185, 233, 366. The government offered no evidence whatsoever that Mr. Auernheimer or his alleged co-conspirator accessed any New Jersey computers, sent any data to or through New Jersey, or obtained any information from within New Jersey. App2. 442-443. In sum, the CFAA charges should not have been brought in the District of New Jersey; no computer was accessed there; no defendant was located there; and no computer traffic traveled there.

Despite this, the government brought this case in the District of New Jersey. The government's primary argument for venue under § 1030(a)(2)(C)—raised in opposition to Mr. Auernheimer's Motion to Dismiss the Superseding Indictment and accepted by the district court—was that the alleged conduct "affected" New Jersey residents. App2. 110; *see also* App1. 26. This finding was error, since "affecting" third parties is not a conduct element of an offense under § 1030(a)(2)(C).

Under controlling Supreme Court precedent, venue cannot be based on the effects of a crime unless the statutorily proscribed conduct is defined in terms of its

effects. In *Cabrales*, the Supreme Court held that venue for a money-laundering charge was improper in Missouri (where the laundered funds were generated from illegal drug transactions), because the laundering transactions (*i.e.*, the conduct prohibited by the charged statute) occurred only in Florida. 524 U.S. at 9-10. The Court specifically rejected the government's argument that venue was proper in Missouri because the charged laundering offense furthered drug-related crime affecting the Missouri community. As the Supreme Court emphasized, the case could not be brought in Missouri, despite the "interests of the community victimized by drug dealers." *Id*.

United States v. Bowens, 224 F.3d 302 (4th Cir. 2000) is also instructive. There, the Fourth Circuit held that venue for harboring or concealing a fugitive was proper only in the district where the harboring or concealing occurred—and not in the district that issued the outstanding warrant for the fugitive's arrest—even if a purpose of the harboring and concealing statute was to protect interests in the district that issued the warrant. The *Bowens* court explained that Congress can (and often does) define "an essential conduct element . . . in terms of its effects." *See id.* at 311, 313 (listing examples). But where Congress has declined to define conduct based on its effects, courts may not locate venue based on the alleged effects of the charged offense. *See id.* at 311.

In fact, the CFAA is a perfect example of a statute in which some criminal provisions require proof of effects caused by the defendant, and some do not: Sections 1030(a)(5)(B) and (C) punish anyone who "intentionally accesses a protected computer without authorization," and, under varying circumstances, cause "damage" and/or "loss." By comparison, Congress did *not* include any requirement in § 1030(a)(2)(C) that the defendant cause any effects. Thus, the district court's approach—treating the supposed indirect effects of Mr. Auernheimer's actions on New Jersey residents as conduct elements of a § 1030(a)(2)(C) offense—both violates the United States Constitution and flouts Congressional intent.

The district court's fast and loose approach would allow the government to bring criminal charges in any number of jurisdictions with an at-best tenuous connection to the charged conduct. As a result of the interconnectedness of the public Internet, extending CFAA venue to any jurisdiction where the charged conduct indirectly affects a third party effectively extends venue throughout the entire country. In the present case, for example, the government was able to proceed in New Jersey even though only a small percentage of the individuals "affected" by the disclosure of their email address were New Jersey residents—a mere 4 percent of the 114,000 email addresses allegedly disclosed. *See* App2. 106, 221. If venue in this case could lie in any jurisdiction containing "affected"

individuals, venue could lie practically anywhere in the country. Given the extreme ramifications of basing venue for alleged Internet crime on the locations of alleged indirect effects, the Court should be particularly wary of construing effects as a conduct element of § 1030(a)(2)(C).

The government also argued that venue under § 1030(a)(2)(C) was proper in New Jersey because Mr. Auernheimer "failed to obtain authorization for the taking and disclosing of personal identifying information from the residents" of that district. App2. 110. This argument also fails entirely, both as a matter of law and policy. First, the absence of authorization is a circumstance—not conduct that the government must prove—and therefore cannot serve as a basis for venue. Moreover, locating a CFAA charge in any jurisdiction where the defendant "failed to obtain authorization" essentially nullifies the protections of the constitutional and statutory limitations on venue, since individuals or entities with the ability to confer authorization may reside in any number of districts that are otherwise completely unrelated to the prohibited conduct. Additionally, the government's "without authorization" theory of venue exacerbates the vagueness problem discussed Section I, *supra*; according to the government, any of over 100,000 AT&T customers—and not just AT&T itself—was empowered to grant or deny Mr. Auernheimer, or anyone else for that matter, lawful access to the AT&T servers.

For these reasons, as well as those briefed by the Appellant himself, venue under § 1030(a)(2)(C) cannot be based anywhere third parties are affected, or where the defendant allegedly "failed to obtain authorization." Rather, proper venue is limited to only those jurisdictions in which a computer was accessed without authorization (*i.e.*, the physical location of the accessed computer) and where information was obtained (*i.e*., the physical location of the defendant). Since none of the *conduct* charged under § 1030(a)(2)(C) occurred in New Jersey, and both counts of the superseding indictment were predicated on Mr. Auernheimer's violation of § 1030(a)(2)(C), venue in New Jersey was improper for both counts.

B. The Government Cannot Evade Limitations on Venue by Linking § 1030(A)(2)(C) to Other Statutes that Do Not Add Conduct Elements.

To enhance Count 1 from a misdemeanor into a felony, the government alleged that Mr. Auernheimer violated § 1030(a)(2)(C) in furtherance of a New Jersey law criminalizing the disclosure of personal identifying information obtained from unauthorized access (N.J.S.A. 2C:20-31(a)). The government argued below that disclosure occurred in New Jersey, and that venue in New Jersey was therefore proper for Count 1. App2. 110, 112.

Again, the government's argument flouts fundamental constitutional limitations on venue. The Supreme Court has made clear that venue is based only

on the conduct prohibited by Congress when it enacts a federal criminal statute. *Rodriquez-Moreno*, 526 U.S. at 279. The relevant enhancement provision provides only that hacking in furtherance of any crime or tort is a felony rather than a misdemeanor. *See* 18 U.S.C. § 1030(c)(2)(B)(ii). Congress did not independently criminalize the commission of state-law crimes or torts, and it certainly did not incorporate the elements of such crimes or torts into the conduct elements of a §1030(a)(2)(C) offense. As a practical matter, the government's theory would extend venue to *anywhere* there is a state computer crime law prohibiting the same or similar conduct.

With respect to Count 2, the government charged Mr. Auernheimer under 18 U.S.C. § 1028(a)(7), a provision of the federal identity theft statute that prohibits "knowingly transfer[ing], possess[ing], or us[ing], "without lawful authority, a means of identification of another person with the intent to commit . . . a violation of federal law." The predicate "violation of federal law" alleged in Count 2 was the § 1030(a)(2)(C) charge. The government argued below, and the district court agreed, that venue in New Jersey was proper for Count 2 solely on the ground that venue for the predicate § 1030(a)(2)(C) offense was proper. App2. 115-116; App1. 10-11. For the reasons set forth in Section II.A above, the district court's

holding with respect to venue under § 1030(a)(2)(C) was a grave constitutional error.[32]

CONCLUSION

For the foregoing reasons, in the context of cases involving remote access over the public Internet, amicus NACDL urges this Court to limit "access without authorization" to the circumvention of code-based barriers. Amicus further urges this Court to limit venue under § 1030(a)(2)(C) to only those jurisdictions where a protected computer was "accessed," or where a defendant "obtained information."

San Francisco, California.
July 8, 2013

By: */s/ Steven P. Ragland*
STEVEN P. RAGLAND
JENNIFER A. HUBER
BEN D. ROTHSTEIN
KEKER & VAN NEST LLP
633 Battery Street
San Francisco, CA 94111-1809
Telephone: 415-391-5400
Fax: 415-397-7188

Attorneys for Amicus Curiae National Association of Criminal Defense Lawyers

[32] *See also* Appellant's Opening Brief at 49 (explaining that, even if § 1028(a)(7) contains conduct elements, "[v]enue is not proper in New Jersey [for Count 2] because no data was transferred, possessed, or used there").

Of Counsel:

JENNY CARROLL
Seton Hall Univ. School of Law
Newark, NJ 07102

PETER GOLDBERGER
50 Rittenhouse Place
Ardmore, PA 19003

Third Circuit Co-Vice-Chairs,
National Association of Criminal
Defense Lawyers Amicus Curiae
Committee

CERTIFICATION OF ADMISSION TO BAR

I, Steven P. Ragland, certify as follows:

1. I am a member in good standing of the bar of the United States Court of Appeals for the Third Circuit.

2. Pursuant to 28 U.S.C. § 1746, I certify under penalty of perjury that the foregoing is true and correct.

Dated: July 8, 2013

/s/ Steven P. Ragland
Steven P. Ragland

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF APPELLATE PROCEDURE 32(a) AND LOCAL RULE 31.1

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

This brief complies with the type-volume limitation of Rule 32(a)(7)(B) of the Federal Rules of Appellate Procedure because this brief contains 6,882 words, excluding the parts of the brief exempted by Rule 32(a)(7)(B)(iii) of the Federal Rules of Appellate Procedure.

This brief complies with the typeface requirements of Rule 32(a)(5) of the Federal Rules of Appellate Procedure and the type style requirements of Rule 32(a)(6) of the Federal Rules of Appellate Procedure because this brief has been prepared in a proportionally spaced typeface using the 2008 version of Microsoft Word in 14 point Times New Roman font.

This brief complies with the electronic filing requirements of Local Rule 31.1(c) because the text of this electronic brief is identical to the text of the paper copies, and the Vipre Virus Protection, version 3.1 has been run on the file containing the electronic version of this brief and no viruses have been detected.

Dated: July 8, 2013

/s/Steven P. Ragland
Steven P. Ragland

AFFIDAVIT OF SERVICE

DOCKET NO. 13-1816
----------X
USA
vs.

Andrew Auernheimer
----------X

I, Elissa Matias , swear under the pain and penalty of perjury, that according to law and being over the age of 18, upon my oath depose and say that:

on July 8, 2013

I served the **Brief of Amicus Curiae National Association of Criminal Defense Lawyers in Support of Appellant** within in the above captioned matter upon:

See Attached Service List

via **electronic filing and electronic service**.

Unless otherwise noted, copies have been sent to the court on the same date as above for filing via Express Mail.

Sworn to before me on July 8, 2013

/s/ Robyn Cocho
Robyn Cocho
Notary Public State of New Jersey
No. 2193491
Commission Expires January 8, 2017

/s/ Elissa Matias
Elissa Matias

Job # 248362

Service List:

Mark E. Coyne, Esq.
email: mark.coyne@usdoj.gov.
Office of United States Attorney
970 Broad Street
Room 700
Newark, NJ 07102

Tor B. Ekeland, Esq.
email: tor@torekeland.com
Tor Ekeland
155 Water Street
6th Floor, Suite 2
Brooklyn, NY 11201

Hanni M. Fakhoury, Esq.
email: hanni@eff.org
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

Marcia C. Hofmann, Esq.
email: Marcia@marciahofmann.com
25 Taylor Street
San Francisco, CA 94102

Mark H. Jaffe, Esq.
email: mark@torekeland.com
Tor Ekeland
155 Water Street
6th Floor, Suite 2
Brooklyn, NY 11201

Orin S. Kerr, Esq.
email: okerr@law.gwu.edu
George Washington University
2000 H. Street, NW
Washington, DC 20052