

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

X _____ X	:
UNITED STATES OF AMERICA,	:
	:
Plaintiff,	:
	:
v.	:
	:
ANDREW AUERNHEIMER,	:
	:
Defendant.	:
X _____ X	:

11-CR-470 (SDW)

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT’S MOTION TO DISMISS

Tor Ekeland, P.C.
155 Water Street
Brooklyn, NY 11201
Tel: 718.285.9343
Fax: 718.504.5417
tor@torekeland.com

Law Office of Nace Naumoski
618 Newark Avenue
Elizabeth, NJ 07208
Tel: 908.349.8462
Fax: 908.325.1646
nace@naumoski.com
Pro Bono Attorneys for Defendant Andrew Auernheimer

On the Brief: Tor Ekeland
Mark H. Jaffe
Nace Naumoski

TABLE OF CONTENTS

THE INDICTMENT 1

PRELIMINARY STATEMENT 3

ARGUMENT 4

I. THE INDICTMENT VIOLATES THE FIFTH AMENDMENT’S DUE PROCESS CLAUSE 4

A. There Was No Fair Notice Under the Fifth Amendment’s Due Process Clause That the Object of the Conspiracy in Count One Was Illegal..... 4

B. The Government’s Interpretation of the CFAA Invites Discriminatory Enforcement..... 7

II. The Rule of Lenity Requires that Count One be Dismissed..... 7

III. THE INDICTMENT VIOLATES THE FIFTH AMENDMENT’S DOUBLE JEOPARDY CLAUSE 8

A. Count One Violates Double Jeopardy Because the Object of the Conspiracy and the Felony Aggravator Require Proof of the Same Facts..... 8

B. The Federal State and State Unauthorized Access Statutes are Virtually Identical..... 9

C. The Same Conduct Underlies Count One and its Felony Aggravator 10

D. Congress Did Not Intend For Every CFAA Violation to be a Felony 11

E. There is No Violation of the New Jersey Unauthorized Access Statute as a Matter of Statutory Construction 12

IV. THE INDICTMENT VIOLATES THE U.S. CONSTITUTION AND FEDERAL RULE OF CRIMINAL PROCEDURE 18 BECAUSE IT FAILS TO SUFFICIENTLY ALLEGE VENUE IN NEW JERSEY 13

A. Venue in the District of New Jersey is Unconstitutional..... 13

B. None of the Alleged Criminal Acts Took Place in New Jersey..... 15

V. COUNT TWO MUST BE DISMISSED 16

A. The Alleged Unauthorized Access Was Over Before the Conduct Underlying Count Two Began 16

B. 18 U.S.C. § 1028(a)(7)’s “In Connection With” Language Refers to Present or Future Criminal Conduct and not Past Criminal Conduct 17

C. Count Two Violates the First Amendment 18

CONCLUSION 19

TABLE OF AUTHORITIES

CASES

Albernaz v. United States, 450 U.S. 333 (1981).....9
Cioni v. United States, 649 F.3d 276 (4th Cir. 2011).....9,10
Coates v. City of Cincinnati, 402 U.S. 611 (1971).....6
Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927 (E.D. Va. 2010)8
Giacco v. Pennsylvania, 382 U.S. 399 (1966).....6
Koch Indus., Inc. v. Does, 2011 WL 1775765 (D. Utah May 9, 2011).....8
Kolender v. Lawson, 461 U.S. 352 (1983)7
Shamrock Foods Co. v. Gast, 535 F.Supp. 2d 962 (D. Ariz. 2008)5
Shuttlesworth v. City of Birmingham, 382 U.S. 87 (1965).....7
Skilling v. United States, 130 S.Ct. 2896 (2010)5,7
U.S. v. Santos, 533 U.S. 507 (2008).....12
United States v. Birks, 656 F.Supp. 2d 454 (D.N.J. 2009) 14,15
United States v. Brassington, 2010 WL 3982036 (D.N.J. Oct. 8, 2010).....14
United States v. Davis, 689 F.3d 179 (2d Cir. 2012).....14
United States v. Drew, 259 F.R.D.449 (C.D. Cal. 2009).....5,6
United States v. Johnson, Jr., 510 F.3d 521 (4th Cir. 2007)15
United States v. Mastronardo, 849 F.2d 799 (3d Cir. 1988).....4
United States v. Miller, 527 F.3d 54 (3d Cir. 2008).....9
United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).....5,6,7
United States v. Passodelis, 615 F.2d 925 (3d Cir. 1980).....15
United States v. Perez, 280 F.3d 318 (3d Cir. 2002).....13,14
United States v. Rodriguez-Moreno, 526 U.S. 275 (1999).....14
United States v. Salinas, 373 F.3d 161 (1st Cir. 2004).....13,14,15
United States v. Santos, 533 U.S. 507(2008).....10
United States v. Schramm, 75 F.3d 156 (3d Cir. 1996).....4
United States v. Sutcliffe, 505 F.3d 944 (9th Cir. 2007).....17
United States v. Villanueva-Sotelo, 515 F.3d 1234 (D.C. Cir. 2008).....17
Whalen v. United States, 445 U.S. 684 (1980).....9

STATUTES & RULES

18 U.S.C. § 21, 2
 18 U.S.C. §§ 3711,2,8
 18 U.S.C. § 1028(a)(7)1, 2,16,17,18
 18 U.S.C. § 1030(a)(2)(C).....1,2,5,8,10,11,16
 18 U.S.C. § 1030(c)(2)(A).....12
 18 U.S.C. § 1030(c)(2)(B)(ii).....2,8
 N.J.S.A. 2C:20-31(a)2,10,11
 Fed. Rule Crim. P. 183,13

CONSTITUTIONAL PROVISIONS

U.S. Const. Article III, § 2.....13
U.S. Const. Amend. I.....18
U.S. Const. Amend. V.....3,4,9
U.S. Const. Amend. VI.....13

OTHER AUTHORITIES

Andrew T. Hernacki, A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act, 61 Am. U. L. Rev. (2012)5
Orin S. Kerr, Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes, 78 NYU L. Rev. 1596 (2003).....11
Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn. L. Rev. 1561 (2010).....5
H.R.Rep. No. 108-52818
S.Rep. No. 104-357 11,12

THE INDICTMENT

On or about August 16, 2012, a Grand Jury in the District of New Jersey returned a two count Superseding Indictment (“Indictment”) against defendant Andrew Auernheimer charging violations of 18 U.S.C. §§ 2, 371, 1030(a)(2)(C), 1028(a)(7). According to the Indictment, between the approximate dates of June 2 and June 9, 2010, Mr. Auernheimer conspired with former co-defendant Daniel Spitler to gain unauthorized access to AT&T’s iPad servers via a computer script (the “Script”) written by Mr. Spitler and Mr. Auernheimer. (*See* Indictment at ¶¶ 7-10.) Mr. Auernheimer then allegedly committed a subsequent crime by providing the list of customer I.D. numbers paired with email addresses allegedly obtained through the unauthorized access to the internet magazine Gawker. Gawker then proceeded to publish a story on the matter. (*See* Indictment at ¶ 11.) For these violations, Mr. Auernheimer faces a maximum sentence of ten years in jail and substantial fines.

The Script queried AT&T’s readily accessible servers by emulating the format of customer identification numbers (“ICC-IDs”)¹ found on subscriber identification cards contained in every iPad. (*See* Indictment at ¶ 7(m).) The Script then sequentially generated numbers in an ICC-ID format querying AT&T’s servers. (*See* Indictment at ¶¶ 6-7.) If a number query by the Script did not match an actual customer ICC-ID the servers did not respond. (*See id.* at ¶ 8(b).) But when the Script hit an actual customer ICC-ID, AT&T’s servers published the email address of the customer associated with the ICC-ID. (*See* Indictment at ¶¶ 7(n), 16.) There is no allegation that any passwords or firewalls were obtained or bypassed. After obtaining the e-mail addresses associated with the ICC-IDs, Mr. Spitler and Mr. Auernheimer allegedly provided

¹ ICC-ID stands for “Integrated Circuit Chip Identification.” (*See* Indictment at ¶ 1m.)

them to the internet magazine Gawker. Gawker then published the pairings in redacted form.

(*See id* at ¶ 11.)

Count One of the Indictment charges defendant Andrew Auernheimer with conspiracy to gain access to a protected computer in violation of the Computer Fraud and Abuse Act (the “CFAA”), 18 U.S.C. § 1030(a)(2)(C). Because Count One alleges that the conspiracy to violate the CFAA was committed in furtherance of a criminal act in violation of New Jersey’s statute prohibiting unauthorized access to a computer, what would ordinarily be a misdemeanor charge is being elevated to a felony charge. (*See* Indictment at ¶ 5.); 18 U.S.C. §§ 371, 1030(a)(2)(C), 1030(c)(2)(B)(ii); N.J.S.A. 2C:20-31(a). Count Two of the Indictment charges Mr. Auernheimer with the knowing transfer, possession, and use of means of identification (email addresses paired with ICC-IDs) in connection with the unauthorized access to a protected computer in violation of the CFAA. 18 U.S.C. § 1028(a)(7) and 18 U.S.C. § 2. Mr. Auernheimer’s jury trial is currently scheduled before this Court for October 29, 2012.

PRELIMINARY STATEMENT

Even assuming the allegations in the Indictment to be true, both counts of the Indictment must be dismissed for constitutional, statutory and procedural deficiencies that render the Indictment defective as a matter of law:

- First, Count One must be dismissed because the CFAA is void for vagueness as applied under the Fifth Amendment's Due Process Clause.
- Second, Count One violates the Fifth Amendment's Double Jeopardy Clause because proof of the illegal object of the conspiracy requires proof of the same conduct prohibited by the New Jersey unauthorized access statute that elevates Count One from a misdemeanor to a felony.
- Third, venue is improper under the United States Constitution and Federal Rule of Criminal Procedure 18 because the Indictment makes no specific allegation that any criminal conduct occurred in New Jersey.
- Fourth, Count Two must be dismissed because it cannot be in "connection with" a past crime.
- Fifth, Count Two must be dismissed because it criminalizes the transfer of information of public concern to the press in violation of the First Amendment.

ARGUMENT

I. THE INDICTMENT VIOLATES THE FIFTH AMENDMENT'S DUE PROCESS CLAUSE

The conspiracy charge must be dismissed because Mr. Auernheimer had no notice under the Fifth Amendment's Due Process Clause that the object of the conspiracy - the alleged unauthorized access - was illegal. The CFAA is unconstitutionally vague as applied. The CFAA provides no definition as to what constitutes unauthorized access to a protected computer, and the courts are conflicted as to what unauthorized access means. Simply put, there is nothing in the CFAA or the case law that gives fair notice that the charged conduct was illegal. This vagueness and ambiguity invites arbitrary and discriminatory law enforcement.

A. There Was No Fair Notice Under the Fifth Amendment's Due Process Clause That the Object of the Conspiracy in Count One Was Illegal

The object of the conspiracy alleged in Count One is the unauthorized access to AT&T's iPad servers, and disclosure of the information obtained, in violation of the CFAA. (*See* Indictment at ¶ 6.) The object of a conspiracy must be an illegal act and a criminal defendant to a conspiracy charge must know that he is agreeing to commit that illegal act. *See, e.g., United States v. Schramm*, 75 F.3d 156, 163 (3d Cir. 1996) ("In cases which involve a conspiracy charge, the illegal object of the conspiracy is an essential element of the offense and must be included in the indictment."). If the object of the conspiracy is not illegal, or a defendant had no fair notice that what he allegedly was conspiring to do was illegal, a conspiracy charge fails. *See United States v. Mastronardo*, 849 F.2d 799, 805 (3d Cir. 1988) (reversing conspiracy convictions on fair notice due process grounds because criminal statutes must be strictly

construed and must define the criminal offense “with sufficient definiteness that ordinary people can understand what conduct is prohibited.” (citations omitted)).

The CFAA fails to give fair notice in this instance because it nowhere defines what it seeks to make illegal: “intentionally access[ing] a computer without authorization or exceed[ing] authorized access” *See* 18 U.S.C. § 1030(a)(2). This lack of clarity has caused understandable consternation among the federal courts as they attempt to divine the meaning of what Congress has declined to define. *See United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Cal. 2009) (holding the CFAA constitutionally void for vagueness as applied); *Shamrock Foods Co. v. Gast*, 535 F.Supp. 2d 962, 964-65 (D. Ariz. 2008) (discussing the conflicting approaches to unauthorized access among the federal courts in civil cases); Andrew T. Hernacki, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 Am. U. L. Rev. 1543, 1554 (2012) (“[C]ourts and academics have struggled to interpret these undefined and vague provisions”); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1572 (2010) (“Exactly what is an ‘access,’ and what makes an ‘access’ unauthorized, is presently unclear.”).

There is a dearth of criminal CFAA cases and the body of case law cannot be said to provide fair notice. Indeed, both the recent major criminal CFAA cases note the vagueness of the CFAA and the federal courts’ struggle with its meaning. These cases go on to reject the government’s expansive interpretations of unauthorized access. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012); *Drew*, 259 F.R.D. 449. If the courts cannot easily define what unauthorized access is then Mr. Auernheimer cannot be on fair notice of what the CFAA prohibits. *See Skilling v. United States*, 130 S.Ct. 2896, 2938, fn. 2 (2010) (Scalia, J., concurring) (“We have previously found important to our vagueness analysis ‘the conflicting results which

have arisen from the painstaking attempts of enlightened judges in seeking to carry out [a] statute in cases brought before them.” (citation omitted)). Simply put, no one really knows what constitutes unauthorized access under the CFAA.

The question is not whether there is an ordinary, dictionary understanding of “authorization” or “access”, but whether the CFAA specifies the standard of conduct that constitutes unauthorized access. *See Coates v. City of Cincinnati*, 402 U.S. 611, 614 (1971) (“Thus, the ordinance is vague, not in the sense that it requires a person to conform his conduct to an imprecise but comprehensible normative standard, but rather in the sense that no standard of conduct is specified at all.”). The CFAA is so vague that it unconstitutionally “[leaves] judges and jurors free to decide, without any legally fixed standards, what is prohibited and what is not in each particular case.” *Giacco v. Pennsylvania*, 382 U.S. 399, 402-03 (1966).

To the extent that the Indictment alleges any theory of unauthorized access, it seems to suggest that access was unauthorized because AT&T and its subscribers subsequently disapproved. (*See* Indictment at ¶¶ 9-10.) Yet neither the CFAA, nor case law, provide any fair notice that the conduct in question here should turn on the subjective whims of persons. Courts have rejected the view that corporate or natural persons can dictate what constitutes unauthorized access to a protected computer. *See Drew*, 259 F.R.D. at 464 (“Here, the language of section 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that the CFAA has ‘criminalized breaches of contract’ in the context of website terms of service. Normally, breaches of contract are not the subject of criminal prosecution.”); *Nosal*, 676 F.3d at 860 (“Basing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.”). That there is a circuit split on the meaning of unauthorized access under the CFAA

only highlights the CFAA's vagueness and ambiguity. *See Nosal*, 676 F.3d at 862 (“We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violation of a duty of loyalty.”).

There is nothing in the statute or the case law that provides fair notice that the object of the conspiracy alleged in Count One was illegal and therefore Count One must be dismissed.

B. The Government's Interpretation of the CFAA Invites Discriminatory Enforcement

Moreover, the CFAA fails to establish minimal guidelines for law enforcement that prevent “arbitrary and discriminatory enforcement.” *See Kolender v. Lawson*, 461 U.S. 352, 357 (1983). Enforcement cannot be left to the “whim of any police officer.” *Shuttlesworth v. City of Birmingham*, 382 U.S. 87, 90 (1965). The CFAA's vagueness invites the government to pursue expansive interpretations against unpopular defendants and then wield its expansive interpretation arbitrarily. As noted in *Nosal*, “[W]e shouldn't have to live at the mercy of our local prosecutor.” *Nosal*, 676 F.3d at 862. Therefore, Count One should be dismissed, or in the least, this Court should invoke the Rule of Lenity to narrow the CFAA to mean bypassing code based restrictions such as passwords or firewalls, thereby providing a bright line rule giving fair notice to all.

II. The Rule of Lenity Requires that Count One be Dismissed

There is no allegation that Mr. Auernheimer acted in any way to bypass any computer security measures. If the CFAA is to avoid constitutional infirmity, it must be narrowly read to require the bypassing of computer security measures. The Rule of Lenity requires that “ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity.” *Skilling*, 130 S.Ct. at 2932 (citation omitted). The ambiguity at issue here should be resolved in

favor of a bright line rule requiring that unauthorized access means the bypassing of security measures. Courts have recognized this as a clear, narrow way to interpret the CFAA, and this Court should adopt it. *See, Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 933 (E.D. Va. 2010) (holding that “scraping” information from a business competitor’s non-password protected website did not constitute unauthorized access under the CFAA); *accord, Koch Indus., Inc. v. Does*, 2011 WL 1775765, *8 (D. Utah May 9, 2011) (unpublished). Narrowly reading the CFAA this way requires that Count One be dismissed because there is no allegation that AT&T had any security measures in place.

III. THE INDICTMENT VIOLATES THE FIFTH AMENDMENT’S DOUBLE JEOPARDY CLAUSE

A. Count One Violates Double Jeopardy Because the Object of the Conspiracy and the Felony Aggravator Require Proof of the Same Facts

Count One violates the Double Jeopardy Clause because it improperly aggravates a CFAA misdemeanor into a felony. Violations of the CFAA are ordinarily misdemeanors unless committed in furtherance of a violation of a federal or state statute. *See* 18 U.S.C. § 1030(c)(2)(B)(ii). The Indictment alleges that Count One’s conspiracy to violate the CFAA was in furtherance of a violation of New Jersey’s CFAA equivalent. (*See* Indictment at ¶ 5.) But proof of the object of Count One’s conspiracy is dependent on the same conduct necessary to prove the furtherance of its felony aggravator. (*See id.*); 18 U.S.C. §§ 371, 1030(a)(2)(c), 1030(c)(2)(B)(ii); N.J.S.A. 2C: 20-31(a). That the object of the conspiracy and its felony aggravator require proof of the same conduct violates the Fifth Amendment’s Double Jeopardy Clause.

The Double Jeopardy Clause prohibits this type of bootstrapping because it charges the same criminal act twice. U.S. Const. Amend. V. The Indictment also ignores the congressional intent to elevate CFAA misdemeanor violations to felonies only when a crime separate and distinct from the act of unauthorized access occurs. *See Albernaz v. United States*, 450 U.S. 333, 344 (1981) (“[T]he question of what punishments are constitutionally permissible is not different from the question of what punishments the Legislative Branch intended to be imposed.”); *Whalen v. United States*, 445 U.S. 684, 692 (1980) (“[W]here two statutory provision[s] proscribe the ‘same offense’ they are construed not to authorize cumulative punishments in the absence of a clear indication of contrary legislative intent.”); *Cioni v. United States*, 649 F.3d 276 (4th Cir. 2011) (holding that the charged CFAA violation violated double jeopardy because the CFAA charge and its felony aggravator required proof of the same facts), *cert. denied*, 132 S.Ct. 437 (Oct. 11, 2011).

The Double Jeopardy Clause prohibits multiple punishments for the same offense. U.S. Const. Amend. V. (“nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb.”). A Double Jeopardy violation exists if two statutory provisions proscribe the same offense and clarity does not exist as to whether the legislature intended multiple punishments for the offense. *See United States v. Miller*, 527 F.3d 54, 72 (3d Cir. 2008). The issue is whether the statutes are “directed to similar, rather than separate, evils.” *Id.* Here, the statutes are directed towards similar perceived evils and the same conduct is required for both proof of the object of the conspiracy and its felony aggravator.

B. The Federal and State Unauthorized Access Statutes are Virtually Identical

The CFAA prohibits a person from, in the relevant parts, “intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . .

information” 18 U.S.C. § 1030(a)(2)(C). The relevant section of New Jersey’s unauthorized access statute reads:

A person is guilty of a crime of the third degree if the person purposely or knowingly and without authorization, or in excess of authorization, accesses any data, data base, computer, computer storage medium, computer software, computer equipment, computer system and knowingly or recklessly discloses or causes to be disclosed any data, data base, computer software, computer programs or personal identifying information.
N.J.S.A. 2C:20-31(a).

The only difference between the CFAA and New Jersey’s unauthorized access statute is that New Jersey requires knowing or reckless data disclosure. This, however, does not foreclose a Double Jeopardy violation because the underlying criminal conduct necessary for proof of the Count One’s conspiracy charge is the same as that necessary to prove that the conspiracy was in furtherance of a violation of New Jersey’s unauthorized access statute.

C. The Same Conduct Underlies Count One and its Felony Aggravator

In *Cioni v. United States*, 649 F.3d 276 (4th Cir. 2011), the Fourth Circuit held that when the same conduct underlies a CFAA violation and its felony aggravator this is “tantamount” to a Double Jeopardy violation, even though the statutory elements differed. *See id.* at 282-83 (citing *United States v. Santos*, 533 U.S. 507, 527 (2008)).

The general conspiracy statute has three elements: (1) an agreement (2) to commit an illegal act, and (3) at least one overt act in furtherance of the agreement. The government may list as many overt acts as it likes but must prove at least one. *See* 18 U.S.C. § 371. However, only one overt act alleged would suffice to prove criminal conduct in furtherance of a violation of New Jersey’s unauthorized access statute. That overt act is the disclosure of the data to Gawker. (*See* Indictment at ¶ 27(d).) This is the same conduct underlying proof of knowing and

reckless disclosure of data under New Jersey's unauthorized access statute. *See* N.J.S.A. 2C:20-31(a). Therefore, Count One must be dismissed, or in the least reduced to a misdemeanor count.

D. Congress Did Not Intend For Every CFAA Violation to be a Felony

Additionally, the statutory language of the CFAA and its legislative history reflect that Congress did not intend to elevate a misdemeanor charge into a felony where no additional illegal act is proven. If the government's bootstrapping stands, a CFAA violation may always be turned into a felony because every state in the Union has an unauthorized access statute similar to the CFAA. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 NYU L. Rev. 1596, 1615 (2003); <http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx> (listing state unauthorized access statutes as of 2009). However, the CFAA clearly distinguishes between misdemeanors and felonies, and the legislative history drives this home.

When Congress enacted the 1996 amendments to 18 U.S.C. § 1030(a), Public L. No. 104-294, 110 Stat. 3488, it explicitly indicated its intent that the phrase "for the purpose of committing any criminal or tortious act" should be narrowly construed. Congress explained that amendments to section 1030(a)(2)(C) were "intended to protect against the interstate or foreign theft of information by computer," extending coverage of section 1030(a)(2) to information on federal government computers, and to computers used in interstate or foreign commerce or communications if the conduct involved an interstate or foreign communication. S. Rep. No. 104-357. The Senate Report also clarified how Congress intended such offenses to be punished. Specifically, the report explained:

The sentencing scheme for section 1030(a)(2) is part of a broader effort to ensure that sentences for section 1030 violations adequately reflect the nature of the offense. Thus, under the bill, the harshest penalties are reserved for those who obtain classified information that could be used to injure the United States or assist a foreign state. Those who improperly use computers to obtain other types of information — such as financial records, nonclassified Government information, and information of nominal value from private individuals or companies — face only misdemeanor penalties, unless the information is used for commercial advantage, private financial gain *or to commit any criminal or tortious act*.
S. Rep. No. 104-357 (emphasis added)

Thus, Congress intends a harsher punishment for a CFAA violation only if the initial breach is followed by additional behavior in violation of another federal or state statute. Congress never intended that a CFAA misdemeanor offense be elevated to a felony merely by the coincidence or convenience of the same conduct violating another statute. It is not logical that Congress intended to allow the government to turn every CFAA violation into a felony by claiming an identical violation of any given state's unauthorized access statute. To do so would abrogate Congress's clear intent to make most CFAA violations misdemeanors.

E. There Is No Violation of the New Jersey Unauthorized Access Statute as a Matter of Statutory Construction

For the same reasons detailed above, Mr. Auernheimer could not have violated New Jersey's unauthorized access statute as a matter of statutory construction. The felony enhancement requires that an additional act "in furtherance" of a distinct violation of New Jersey law occurs, but no such distinct violation is alleged. Rather, each of the "overt acts" alleged are the same facts that constitute a violation of New Jersey's unauthorized access statute, and thus cannot have been committed in furtherance of the other. (*See* Indictment ¶ 27.) Accordingly, if all the facts alleged are proven, there can be no more than a misdemeanor violation under 18 U.S.C. § 1030(c)(2)(A).

Therefore, Count One should be dismissed, or in the least the New Jersey State felony enhancement should be stricken, reducing it to a conspiracy to commit a CFAA misdemeanor.

IV. THE INDICTMENT VIOLATES THE U.S. CONSTITUTION AND FEDERAL RULE OF CRIMINAL PROCEDURE 18 BECAUSE IT FAILS TO SUFFICIENTLY ALLEGE VENUE IN NEW JERSEY

A. Venue in the District of New Jersey is Unconstitutional

The Indictment contains no alleged fact which, if ultimately proven, took place in New Jersey. Thus, the Indictment should be dismissed because it violates the constitutional guarantee that a defendant must only be tried in a state and district where a crime has been committed.

The Framers considered venue so critical to due process that they specifically protected the right in two different sections of the Constitution. *See United States v. Perez*, 280 F.3d 318, 327-28 (3d Cir. 2002); *United States v. Salinas*, 373 F.3d 161, 164 (1st Cir. 2004). Article III, § 2 of the United States Constitution dictates that all criminal trials shall be in the state where they were committed, and the Sixth Amendment further restricts criminal venue by dictating that a criminal trial be in the district where the crime was committed. Additionally, the Federal Rules of Criminal Procedure require that a criminal prosecution be limited to “a district in which the offense was committed.” Fed. R. Crim. P. 18; *see Salinas*, 373 F.3d at 164. Collectively, these guarantees provide a “safety net, which insures that a criminal defendant cannot be tried in a distant, remote, or unfriendly forum solely at the prosecutor’s whim.” *Id.* This constitutional safeguard is undermined if an indictment may be served with no notice to the defendant of why venue was chosen and how it could be established.

Not a single act in the Indictment takes place in New Jersey. The Indictment does no more than cite the threadbare and conclusory allegation that the acts described “occurred in the District of New Jersey and elsewhere.” (*See* Indictment at ¶ 5.) There is no specific allegation

that the Defendant or his alleged co-conspirator Daniel Spitler were in New Jersey at any time during the timespan of the alleged acts, that the iPad servers that published the email addresses were located in New Jersey, that any of the Internet Relay Chats (IRC) occurred anywhere in New Jersey, that any conspirator was ever in New Jersey during any point of the conspiracy, or that either of the two recipients of emails allegedly sent by Mr. Auernheimer received them in New Jersey. Thus, there is no constitutional or procedural basis for venue in this District. This defect warrants dismissal of the Indictment, as a trial in an improper venue is a waste of judicial and governmental resources, and an unconstitutional intrusion on Defendant's right to be tried where the alleged crime was committed.

The constitutional test for venue, in the absence of a statutory designation, requires the court to identify the conduct constituting the offense, and then discern the location of the criminal acts. *See United States v. Rodriguez-Moreno*, 526 U.S. 275, 279 (1999); *Salinas*, 373 F.3d at 164; *United States v. Brassington*, 2010 WL 3982036, *11 (D.N.J. Oct. 8, 2010). Venue is improper if the acts alleged in the district do not provide elements of the alleged crime. *Brassington*, 2010 WL 3982036 at *11. Where a defendant is charged with multiple crimes, venue must be satisfied for each crime. *United States v. Davis*, 689 F.3d 179, 185 (2d Cir. 2012); *see also Salinas*, 373 F.3d at 164 (“the criminal law does not recognize the concept of supplemental venue”). The burden is on the government to establish proper venue for each count by a preponderance of the evidence. *Salinas*, 373 F.3d at 164.

For a conspiracy charge, venue may lie in any district where an overt act occurred. *United States v. Birks*, 656 F.Supp. 2d 454, 460-61 (D.N.J. 2009). A court may find that, as a matter of law, venue is not established under the facts alleged. *See United States v. Perez*, 280 F.3d 318, 330 (3d Cir. 2002) (holding that a court may properly determine venue as a matter of

law without submitting issue to jury); *United States v. Passodelis*, 615 F.2d 925 (3d Cir. 1980) (finding that a court may determine if there is sufficient evidence to find that crimes were committed in the district). Thus, a defective allegation of venue in an indictment is a proper ground for dismissal.

B. None of the Alleged Criminal Acts Took Place in New Jersey

It is obvious from the text of the CFAA that Congress has not designated a district for venue. Therefore, the only relevant inquiry is whether the alleged criminal conduct took place in New Jersey. *See Salinas*, 373 F.3d at 164-65. If all the facts alleged in the Indictment are proven, there is still no basis for venue in New Jersey. *Cf. Birks*, 656 F.Supp. 2d at 461 (finding that a general allegation of venue in New Jersey accompanied by specific allegations of overt acts was sufficient to allege venue).

A conspiracy may be charged in a district where any of the overt acts occurred. *See Birks*, 656 F.Supp. 2d at 461. None of the overt acts alleged specifically implicate any conduct in New Jersey. (*See* Indictment at ¶ 27.) Nor is there any specific allegation that any acts took place in New Jersey or were realized by any person in New Jersey.

The servers are not alleged to be located in New Jersey. None of the recipients of the forwarded information are alleged to have been in New Jersey. None of the co-conspirators have been alleged to act in New Jersey. Thus, the Indictment is constitutionally defective on its face because no specifically alleged fact occurred in New Jersey and the Court may determine as a matter of law that the government cannot meet its burden as to proving venue. The Court should dismiss the Indictment as unconstitutional, or, in the alternative, order a pre-trial hearing to determine if venue in New Jersey exists. *See, e.g., United States v. Johnson, Jr.*, 510 F.3d 521 (4th Cir. 2007) (ruling on appeal of a venue determination made at pre-trial hearing).

V. COUNT TWO MUST BE DISMISSED

Count Two must be dismissed because it alleges that the proscribed conduct was committed “in connection with” a CFAA violation, even though the alleged CFAA violation was complete before the conduct underlying Count Two began. The criminal statute at issue in Count Two, 18 U.S.C. § 1028(a)(7) essentially reads:

Whoever . . . knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law . . . shall be punished as provided in subsection (b) of this section.

Count Two alleges that Mr. Auernheimer “knowingly transferred, possessed, and used, without lawful authority, means of identification of other persons . . . *in connection with* unlawful activity, specifically, the unlawful accessing of AT&T’s servers contrary to Title 18, United States Code, Section 1030(a)(2)(c).” (emphasis added). The “in connection with” element of 18 U.S.C. § 1028(a)(7) is a critical element of the statute and without it Count Two fails. Courts, in accordance with congressional intent, interpret “in connection with” to refer to present or future criminal activity, and not past criminal activity. The fact that the Indictment alleges that the unauthorized access was over before the disclosure of data to Gawker began requires dismissal of Count Two.

A. The Alleged Unauthorized Access Was Over Before the Conduct Underlying Count Two Began

There is no specific allegation in the Indictment that the alleged unauthorized access continued when the email addresses and ICC-ID numbers were disclosed to the press. In fact, the Indictment alleges that the unauthorized access to AT&T’s servers ended on or about June 9, 2010: “From on or about June 5, 2010 through on or about June 9, 2010, the Account Slurper

attacked AT&T's servers, [and] gained unauthorized access to those servers” (Indictment at ¶ 9.) The fact that the Indictment alleges that the *conspiracy* in Count One went on until June 15, 2010 is irrelevant; the unauthorized access was complete. (*See* Indictment at ¶ 5.) The Indictment further alleges that Mr. Auernheimer and Mr. Spitler obtained “approximately 120,000 ICC-ID/e-mail address pairings for iPad 3G users.” (*Id.*) The Indictment goes on to say, under a heading alleging the knowing disclosure of the ICC-ID/e-mail address pairings to Gawker, that “[o]n or about June 9, 2010, *immediately following the theft*, the hacker-authors of the Account Slurper knowingly provided stolen e-mail addresses and ICC-IDs to the website Gawker.” (Indictment at ¶ 11 (emphasis added).) Thus, when the Indictment refers to Count Two being “in connection with” a substantive CFAA violation, namely the unauthorized access to AT&T's servers, it is referring to a past crime. This is contrary to how the courts routinely interpret the “in connection with” element of 18 U.S.C. 1028(a)(7) and is contrary to congressional intent.

B. 18 U.S.C. § 1028(a)(7)'s “In Connection With” Language Refers to Present or Future Criminal Conduct and Not Past Criminal Conduct

Almost universally, the courts read the “in connection with” language of 18 U.S.C. § 1028(a)(7) to refer to present and future crimes. This is in accordance with the congressional intent expressed when the “in connection with” language was added to 18 U.S.C. § 1028(a)(7) in 2004. *See United States v. Villanueva-Sotelo*, 515 F.3d 1234, 1245 (D.C. Cir. 2008) (“Congress amended section 1028(a)(7) to ease the prosecution of identity thieves who intend to use “another person's means of identification” . . . to commit a felony, but have not yet actually done so.” (citations omitted)); *United States v. Sutcliffe*, 505 F.3d 944, 960 (9th Cir. 2007) (“In contrast, a conviction under § 1028(a)(7) is based on the defendant's unlawful action of

transferring or using another individual's means of identification with the intent to commit or to aid or abet other unlawful activity.”); H.R.Rep. No. 108-528, at 10, 2004 U.S.C.C.A.N. at 786 (“[The in connection with language] will make it easier for prosecutors to convict identity thieves by allowing for simply possessing false identity documents with the intent to commit a crime.”). That the “in connection with” language of 18 U.S.C. § 1028(a)(7) refers to present and future crimes is logical because one cannot have an intent to commit a past crime. Intent logically precedes, or coincides with, conduct. One cannot have an intent to perform a past act. The Indictment alleges that the criminal activity that is in connection with the disclosure of the ICC-ID/ e-mail address pairings was finished before the disclosure occurred, and therefore Count Two must be dismissed.

C. Count Two Violates the First Amendment

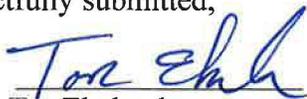
Count Two attempts to criminalize Mr. Auernheimer’s transmission of publicly available information on matters of important public concern to the press and as such violates the United States Constitution’s First Amendment. Mr. Auernheimer’s disclosure of ICC-ID numbers and email addresses to Gawker served the public by exposing AT&T’s non-existent security and cavalier disregard of its customers’ information. The First Amendment forbids criminalizing the transmission of public information of public concern to the press. Thus, Count Two must be struck down on First Amendment grounds.

CONCLUSION

For the reasons stated above, the Indictment must be dismissed.

Respectfully submitted,

By:



Tor Ekeland

Dated: September 21, 2012

Mark H. Jaffe
Tor Ekeland, P.C.
Sixth Floor Suite 2
155 Water Street
Brooklyn, NY 11201
Tel: 718.285.9343
Fax: 718.504.5417
Email: tor@torekeland.com
Pro Bono Attorneys for Defendant Andrew Auernheimer

Nace Naumoski
Law Office of Nace Naumoski
618 Newark Avenue
Elizabeth, NJ 07208
Tel: 908.349.8462
Email: nace@naumoski.com
Pro Bono Attorney for Defendant Andrew Auernheimer