

NO. 13-1816

---

UNITED STATES COURT OF APPEALS  
FOR THE THIRD CIRCUIT

---

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

ANDREW AUERNHEIMER,

DEFENDANT-APPELLANT.

---

On Appeal From The United States District Court  
For The District of New Jersey  
Case No. 2:11-cr-00470-SDW-1  
Honorable Susan D. Wigenton, District Judge

---

**APPELLANT'S REPLY BRIEF**

---

Tor B. Ekeland  
Mark H. Jaffe  
TOR EKELAND, P.C.  
155 Water Street  
Brooklyn, NY 11201  
Tel.: (718) 285-9343  
Email: tor@torekeland.com

Orin S. Kerr  
2000 H Street, N.W.  
Washington, DC 20052  
Tel.: (202) 994-4775  
Email: okerr@law.gwu.edu

Marcia Hofmann  
LAW OFFICE OF MARCIA HOFMANN  
25 Taylor Street  
San Francisco, CA 94102  
Tel.: (415) 830-6664  
Email: marcia@marciahofmann.com

Hanni M. Fakhoury  
ELECTRONIC FRONTIER FOUNDATION  
815 Eddy Street  
San Francisco, CA 94109  
Tel.: (415) 436-9333  
Email: hanni@eff.org

*Counsel for Defendant-  
Appellant Andrew Auernheimer*

## **TABLE OF CONTENTS**

SUMMARY OF ARGUMENT .....	1
ARGUMENT .....	1
I.    AUERNHEIMER AND SPITLER DID NOT ACCESS AT&T’S COMPUTERS WITHOUT AUTHORIZATION.....	1
A.    The Court Cannot Defer to the Jury’s Finding That the Email Addresses Were Protected and Unavailable to the Public Because the Jury Made No Such Finding.....	1
B.    ICC-IDs are not “Passwords.” .....	3
C.    Spitler’s Program Did Not Illegally “Impersonate” iPad Owners.....	6
D.    Whether Spitler used “Expertise” To Design the Program Is Irrelevant to Whether the Program Accessed AT&T’s Computer Without Authorization.....	7
E.    Spitler’s Program Was Not Illegal Because It Set the User Agent to that of an iPad. ....	13
F.    Substantial Authority Acknowledges the Ambiguity of ‘Unauthorized Access’ Under the CFAA.....	16
II.   IF AUERNHEIMER CONSPIRED TO VIOLATE THE CFAA, THE VIOLATION WAS ONLY A MISDEMEANOR.....	17
A.    The Felony Enhancement Cannot Apply Because the Enhancement Requires Independent Conduct, not an Additional Element.....	17
B.    Auernheimer Did Not Violate N.J. Stat. Ann. § 2C:20-31(a) Both Because the Program Did Not Circumvent a Code-Based Restriction and Because New Jersey Does Not and Cannot Regulate Purely Extraterritorial Conduct. ....	19

1.	The Program Did Not Violate New Jersey Law Because It Did Not Circumvent Any Code-Based Restrictions...	19
2.	The Program Did Not Violate N.J. Stat. Ann. § 2C:20-31(a) Because New Jersey Law Does Not and Cannot Apply to Purely Extraterritorial Conduct.....	20
III.	THE GOVERNMENT CANNOT DEFEND AUERNHEIMER’S CONVICTION ON COUNT 2 BASED ON A NEW THEORY OF LIABILITY NEVER PRESENTED TO THE JURY. ....	24
IV.	VENUE WAS IMPROPER IN NEW JERSEY ON BOTH COUNTS .....	27
A.	The “Substantial Contacts” Test Cannot Establish Venue Because it is a Limitation on Venue and Not a Test to Establish It.....	27
B.	The Government Cannot Establish Venue for Count 1 by Invoking the Prosecutor’s Decision to Charge Count 1 as a Felony Using a New Jersey Statute.....	30
C.	The Government Cannot Establish Venue for Count 1 Based on a Failure to Act in New Jersey. ....	35
D.	Venue Was Not Established for Count 1 When an FBI Agent in New Jersey Read About the Alleged Offense over the Internet.....	36
E.	Assuming Venue Was Proper for Count 1, Venue Was Improper for Count 2.....	39
F.	Venue is Not Subject to Harmless Error Review. ....	41
V.	THE ALLEGED MAILING COSTS WERE NOT “LOSS” UNDER THE SENTENCING GUIDELINES.....	42
A.	The Government Failed to Prove AT&T Suffered a \$73,000 “Loss” .....	43

1.	The Standard of Review Should Be Clear Error, Not Plain Error. ....	43
2.	Nothing in the Record Supports the “Loss” Amount. ....	44
B.	Alleged Costs AT&T Spent Notifying its Customers Is Not “Actual Loss” Under U.S.S.G. § 2B1.1. ....	45
1.	The Mailing Costs Were Not “Reasonably Foreseeable Pecuniary Harm” Under U.S.S.G. § 2B1.1. ....	46
2.	The Mailing Costs Were Not Loss Under the Broader Definition of “Loss” for CFAA Convictions. ....	49
CONCLUSION .....		51

## **TABLE OF AUTHORITIES**

### **Federal Cases**

<i>American Civil Liberties Union v. Johnson</i> , 194 F.3d 1149 (10th Cir. 1999).....	23
<i>American Libraries Ass’n v. Pataki</i> , 969 F.Supp. 160 (S.D.N.Y. 1997).....	23
<i>Bouie v. City of Columbia</i> , 378 U.S. 347 (1964).....	10
<i>Center For Democracy &amp; Technology v. Pappert</i> , 337 F.Supp.2d 606 (E.D. Pa. 2004) .....	23
<i>Chiarella v. United States</i> , 445 U.S. 222 (1980).....	2, 26
<i>Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.</i> , 387 F. Supp. 2d 378 (S.D.N.Y. 2005).....	50
<i>Cola v. Reardon</i> , 787 F.2d 681 (1st Cir. 1986).....	26
<i>Communications Workers v. Beck</i> , 487 U.S. 735 (1988).....	24
<i>Concrete Pipe &amp; Prods. of Cal., Inc. v. Constr. Laborers Pension Trust for S. Cal.</i> , 508 U.S. 602 (1993) .....	43
<i>Dunn v. United States</i> , 442 U.S. 100 (1979).....	26
<i>EF Cultural Travel BV v. Explorica, Inc.</i> , 274 F.3d 577 (1st Cir. 2001).....	8, 9, 12, 16
<i>EF Cultural Travel BV v. Zefer Corp.</i> , 318 F.3d 58 (1st Cir. 2003).....	<i>passim</i>

<i>Farmers Ins. Exch. v. Auto Club Grp.</i> , 823 F. Supp. 2d 847 (N.D. Ill. 2011) .....	50
<i>Giaccio v. Pennsylvania</i> , 382 U.S. 399 (1966).....	10
<i>Healy v. Beer Institute, Inc.</i> , 491 U.S. 324 (1989).....	22
<i>In re Cmty. Bank of N. Virginia</i> , 418 F.3d 277 (3d Cir. 2005).....	49
<i>In re DoubleClick Inc. Privacy Litigation</i> , 154 F. Supp. 2d 497 (S.D.N.Y. 2001).....	50
<i>LVRC Holdings, LLC v. Brekka</i> , 581 F.3d 1127 (9th Cir. 2009).....	16, 36
<i>McBurney v. Young</i> , 133 S.Ct. 1709 (2013).....	22
<i>Miller v. French</i> , 530 U.S. 327 (2000).....	23
<i>Morales v. Trans World Airlines, Inc.</i> , 504 U.S. 374 (1992).....	49
<i>Nexans Wires S.A. v. Sark-USA, Inc.</i> , 319 F. Supp. 2d 468 (S.D.N.Y. 2004) <i>aff'd</i> , 166 Fed. App'x 559 (2d Cir. 2006) .....	50, 51
<i>PSINet, Inc. v. Chapman</i> , 362 F.3d 227 (4th Cir. 2004).....	23
<i>Travis v. United States</i> , 364 U.S. 631 (1961).....	31, 38
<i>United States v. Alvarado</i> , --- F. Supp. 2d ----, 2013 WL 3816692 (E.D.Wis. 2013) .....	30

<i>United States v. Anderson</i> , 328 U.S. 699 (1946).....	35
<i>United States v. Bin Laden</i> , 146 F. Supp. 2d 373 (S.D.N.Y. 2001).....	38
<i>United States v. Bowens</i> , 224 F.3d 302 (4th Cir. 2000).....	31, 32, 35
<i>United States v. Brennan</i> , 183 F.3d 139 (2d Cir. 1999).....	41
<i>United States v. Cabrales</i> , 524 U.S. 1 (1998).....	29, 32
<i>United States v. Cioni</i> , 649 F.3d 276 (4th Cir. 2011).....	17, 18, 19
<i>United States v. Clenney</i> , 434 F.3d 780 (5th Cir. 2005).....	30, 34, 35, 40
<i>United States v. Cofield</i> , 11 F.3d 413 (4th Cir. 1993).....	29
<i>United States v. Coplan</i> , 703 F.3d 46 (2d Cir. 2012).....	33
<i>United States v. Davis</i> , 689 F.3d 179 (2d Cir. 2012).....	28
<i>United States v. Dullum</i> , 560 F.3d 133 (3d Cir. 2009).....	43
<i>United States v. Fumo</i> , 655 F.3d 288 (3d Cir. 2011).....	45
<i>United States v. Goldberg</i> , 830 F.2d 459 (3d Cir. 1987).....	27, 28, 29

<i>United States v. Grier</i> , 475 F.3d 556 (3d Cir. 2007).....	43
<i>United States v. Hammoude</i> , 51 F.3d 288 (D.C. Cir. 1995) .....	21
<i>United States v. Hart-Williams</i> , 967 F.Supp. 73 (S.D.N.Y. 1997).....	41, 42
<i>United States v. Kane</i> , 450 F.2d 77 (5th Cir. 1971).....	7
<i>United States v. Lawson</i> , 677 F.3d 629 (4th Cir. 2012).....	3, 4
<i>United States v. Magassouba</i> , 619 F.3d 202 (2d Cir. 2010).....	39
<i>United States v. Miller</i> , 527 F.3d 54 (3d Cir. 2008).....	21, 24
<i>United States v. Mitchell</i> , 518 F.3d 230 (4th Cir. 2008).....	27
<i>United States v. Muhammad</i> , 502 F.3d 646 (7th Cir. 2007).....	28
<i>United States v. Nosal</i> , 676 F.3d 854 (9th Cir. 2012) (en banc).....	13
<i>United States v. Oceanpro Indus., Ltd.</i> , 674 F.3d 323 (4th Cir. 2012).....	31
<i>United States v. Pavulak</i> , 700 F.3d 651 (3d Cir. 2012).....	21, 24
<i>United States v. Pendleton</i> , 658 F.3d 299 (3d Cir. 2011).....	28, 37



<i>United States v. Powers</i> , No. 8:09-cr-00361, 2010 WL 1418172 (D. Neb. Mar. 4, 2010).....	39
<i>United States v. Ramirez</i> , 420 F.3d 134 (2d Cir. 2005).....	38
<i>United States v. Reed</i> , 773 F.2d 477 (2d Cir. 1985).....	27, 28, 29
<i>United States v. Rodriguez</i> , --- F.3d ---, 2013 WL 5630962 (11th Cir. Oct. 16, 2013) .....	45
<i>United States v. Rodriguez-Moreno</i> , 526 U.S. 275 (1999).....	29, 32, 34
<i>United States v. Rowe</i> , 414 F.3d 271 (2d Cir. 2005).....	38, 39
<i>United States v. Royer</i> , 549 F.3d 886 (2d Cir. 2008).....	28
<i>United States v. Saavedra</i> , 223 F.3d 85 (2d Cir. 2000).....	28, 41
<i>United States v. Salinas</i> , 373 F.3d 161 (1st Cir. 2004) .....	37
<i>United States v. Strain</i> , 396 F.3d 689 (5th Cir. 2005).....	33
<i>United States v. Thomas</i> , 74 F.3d 701 (6th Cir.1996).....	39
<i>United States v. Walker</i> , Nos. 11–2727, 11–2845, 11–3087, 11–3088, 2013 WL 3481682 (3d Cir. 2013).....	21, 24
<i>United States v. Williams</i> , 274 F.3d 1079 (6th Cir. 2001).....	29

<i>Verizon Nw., Inc. v. Main St. Dev., Inc.</i> , 693 F. Supp. 2d 1265 (D. Or. 2010) .....	36
<i>WEC Carolina Energy Solutions LLC v. Miller</i> , 687 F.3d 199 (4th Cir. 2012).....	16
<i>Wilson v. Moreau</i> , 440 F. Supp. 2d 81 (D.R.I. 2006).....	51

## State Cases

<i>State v. Gaikwad</i> , 793 A.2d 39 (N.J. App. Div. 2002).....	20
<i>State v. Riley</i> , 988 A.2d 1252 (N.J. Super. Ct. Law Div. 2009) .....	19

## Federal Statutes

18 U.S.C. § 1028 .....	24, 25, 27
18 U.S.C. § 1030 .....	<i>passim</i>
18 U.S.C. § 1071 .....	31
18 U.S.C. § 1204 .....	34
18 U.S.C. § 2701 .....	17, 18
18 U.S.C. § 3237 .....	37

## State Statutes

Ark. Code Ann. § 4-110-105(e) .....	47
Cal. Civ. Code § 1798.29 .....	47
Cal. Civ. Code § 1798.82 .....	47
Ga. Code Ann. § 10-1-911(4).....	47

Ga. Code Ann. § 10-1-912(a).....	47
N.J. Stat. Ann. § 56:8-161 .....	47
N.J. Stat. Ann. § 56:8-163(d) .....	47
N.J. Stat. Ann. § 2C:20-31(a).....	<i>passim</i>
Tex. Bus. & Com. Code Ann. § 521.053(e).....	48

### **Federal Rules**

Federal Rule of Criminal Procedure 29.....	21, 24
--	--------

### **U.S. Sentencing Guidelines**

United States Sentencing Guideline § 2B1.1 .....	<i>passim</i>
--	---------------

### **Legislative Materials**

S. Rep. No. 99–432 (1986), <i>reprinted in</i> 1986 U.S.C.C.A.N. 2479 .....	13
---	----

### **Other Authorities**

Charles Alan Wright, <i>et al.</i> , <i>Federal Practice and Procedure</i> (4th ed. 2013) .....	36
<i>Crawling &amp; Indexing, - Inside Search</i> , Google.....	12
<i>Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes</i> , 78 N.Y.U. L. Rev. 1596 (2003) .....	19, 20
Daniel B. Garrie, <i>The Legal Status of Software</i> , 23 J. Marshall J. Computer & Info. L. 711 (2011).....	11
<i>Default User-Agent (UA) String Changed</i> , Microsoft .....	15
<i>Header Field Definitions</i> , World Wide Web Consortium .....	15
Merriam-Webster Online .....	7

<i>Understanding User-Agent Strings</i> , Microsoft .....	15
Wayne R. LaFave, <i>Criminal Law</i> (4th Ed. 2003) .....	36
Wayne R. LaFave, <i>et al.</i> , <i>Criminal Procedure</i> (3d ed. 2012) .....	29, 41
William E. Burr, <i>et al.</i> , National Institute of Standards and Technology, Electronic Authentication Guideline, Information Security (2011).....	3

## **SUMMARY OF ARGUMENT**

The government has acknowledged that Auernheimer's opening brief "raises serious substantive challenges to the Government's prosecution." United States' Motion For a Word Limit Extension to 26,500 Words & A Stay of the Briefing Schedule at 1. The government has responded to those challenges by filing a 26,495-word merits brief. This reply brief explains the errors in the Government's brief in the order that they appear.

## **ARGUMENT**

### **I. AUERNHEIMER AND SPITLER DID NOT ACCESS AT&T'S COMPUTERS WITHOUT AUTHORIZATION.**

The government defends its view that Spitler and Auernheimer conspired to violate the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(C), with six different arguments. None are persuasive.

#### **A. The Court Cannot Defer to the Jury's Finding that the Email Addresses Were Protected and Unavailable to the Public Because the Jury Made No Such Finding.**

Auernheimer's opening brief argues that access to an unprotected computer available to the public on the World Wide Web does not violate 18 U.S.C. § 1030(a)(2). *See* Appellant's Opening Br. ("AB") 19-25. The government's brief appears to agree with that interpretation of the CFAA. *See* Br. for Appellee ("GB") 27. Instead, the government argues that this court should defer to the

jury's factual finding that the email addresses were protected and not publicly available. *See id.*

The government's argument is meritless because the jury was not asked to decide whether the email addresses were unprotected or publicly available. During pre-trial motions, the Government persuaded the District Court that "access without authorization" in § 1030(a)(2) simply means access without permission. App1. 21-22.<sup>1</sup> As a result, the jury was instructed that "access without authorization" in § 1030(a)(2) means "to access a computer without approval or permission." App2. 704.

Because the District Court adopted the government's proposed definition, the jury was never asked to decide whether the email addresses were unprotected or available to the public. During closing arguments, the prosecutor never mentioned whether the information was protected. He mentioned whether the information was publicly available only once in passing, and without any context or connection to the relevant legal standard. *See* App2. 611.<sup>2</sup>

A court cannot defer to a jury finding on an issue that the jury was not asked to decide. *See Chiarella v. United States*, 445 U.S. 222, 236 (1980) ("[W]e cannot

---

<sup>1</sup> "App1." refers to Volume 1 of the Appendix attached to the end of Auernheimer's opening brief. "App2." refers to Volume 2 of the Appendix, filed separately in connection with the opening brief.

<sup>2</sup> "How can it be that information is publicly available if you have to lie to get at it? It can't. The information wasn't publicly available." App2. 611.

affirm a criminal conviction on the basis of a theory not presented to the jury.”). As a result, the Government’s deference argument is without merit.

**B. ICC-IDs Are Not “Passwords.”**

Auernheimer’s opening brief explains that Spitler’s program was permitted to collect information from AT&T’s computer because the information was not protected by a password or other security measure. AB 22. The government responds that the addresses were in fact protected by a kind of password. Relying on the definition of “passwords” found on the Internet website *Wikipedia*, the government contends that ICC-IDs are passwords because they are “shared secrets” between the user and the AT&T server. GB 38-41.

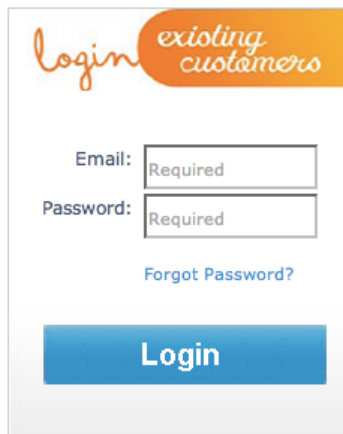
The government is wrong: ICC-IDs are not passwords. The National Institute of Standards and Technology at the U.S. Department of Commerce defines a password as a “secret that a Claimant memorizes and uses to authenticate his or her identity.” William E. Burr, *et al.*, National Institute of Standards and Technology, Electronic Authentication Guideline, Information Security 12 (2011), available at [http://www.nist.gov/customcf/get\\_pdf.cfm?pub\\_id=910006](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910006). Under this standard, from a source surely more authoritative than *Wikipedia*,<sup>3</sup> ICC-IDs are

---

<sup>3</sup> Undersigned counsel are big fans of *Wikipedia*. At the same time, the Government is wrong to rely on it for definitions of terms. “Given the open-access nature of Wikipedia, the danger in relying on a Wikipedia entry is obvious and real.” *United States v. Lawson*, 677 F.3d 629, 650 (4th Cir. 2012). *Wikipedia* “is

not passwords. AT&T customers normally would not know that ICC-IDs exist, much less what they are. Presumably none have ever memorized their ICC-IDs. ICC-IDs are just serial numbers associated with iPads. They are not secrets memorized by users that authenticate them as the correct person to access an account. For that reason, they are not passwords.

Common experience confirms the point. Every computer user is familiar with website login prompts that ask users to enter in a username and password to access an account. AT&T's website contained such a login prompt. App2. 252-53, 257. In its current form, it looks like this:<sup>4</sup>

A screenshot of a web login form. At the top, there is a header with the word "login" in a cursive font and "existing customers" in a sans-serif font, both in orange. Below this, there are two input fields. The first is labeled "Email:" and contains the text "Required". The second is labeled "Password:" and also contains the text "Required". Below the password field is a blue link that says "Forgot Password?". At the bottom of the form is a large blue button with the word "Login" in white.

It is not difficult to identify the password in this login prompt. The password is the secret code entered by the user into the box marked “Password.” Here, by contrast, ICC-IDs had nothing to do with the password box.

---

written largely by amateurs” and is “easily vandalized,” leading many courts to reject its use. *Id.* (citing cases).

<sup>4</sup> Viewable at <https://dcp2.att.com/OEPNDClient/> (last visited Oct. 22, 2013).



The fact that ICC-IDs are numbers associated with specific persons does not make them passwords. To see why, consider the website operated by the Federal Judicial Center (FJC) available at <http://www.fjc.gov>. The FJC website publishes webpages containing biographies of federal judges. Every federal judge has a biography published at a unique address using a special number for that judge. Examples include the following:

*<http://www.fjc.gov/servlet/nGetInfo?jid=1563>*  
*<http://www.fjc.gov/servlet/nGetInfo?jid=2208>*  
*<http://www.fjc.gov/servlet/nGetInfo?jid=911>*

Entering these Internet addresses into a web browser retrieves biographies of Chief Judge McKee, Judge Sloviter, and Judge Greenaway, respectively. And these are only three examples of several thousand biographies published on the FJC website. Changing the numbers at the end of the address changes the biography that visitors will see. Any Internet user who wants to collect biographies of every federal judge can start at number *1* (corresponding to Judge Matthew Abruzzo) and change the number sequentially all the way to number *3493* (corresponding to Judge Madeline Haikala, the most recently-confirmed judge with a biography at the time this brief was filed).

The FJC's website posts information on the web about specific persons using specific numbers that are difficult to guess. But the number *1563* is not Chief Judge McKee's password, just as *2208* is not Judge Sloviter's password and

911 is not Judge Greenaway's password. The numbers at the end of FJC website addresses are just numbers that enable each biography to appear at a specific Internet address.

The same is true of AT&T's website in this case. AT&T decided to post information about persons on the Internet using ICC-IDs as the suffixes of website addresses. Those suffixes are not "passwords" known to individuals whose information was posted. Instead, they are numbers that enable Internet addresses where information can be posted. Entering in those numbers is not a federal crime, regardless of whether the website belongs to the FJC or AT&T.

**C. Spitler's Program Did Not Illegally "Impersonate" iPad Owners.**

The government also argues that Spitler's program committed an unauthorized access because it "impersonated" other iPad owners. GB 24-26. The government's impersonation theory fails for two reasons. First, the CFAA punishes unauthorized access, not impersonation. Whether access to a computer amounts to an "impersonation" is not an element of the CFAA, and the jury instruction on whether an unauthorized access occurred under the CFAA did not mention impersonation.<sup>5</sup> App2. 703-04.

Second, even assuming that impersonation violates the CFAA, no impersonation occurred here. To impersonate someone means to pretend to be that

---

<sup>5</sup> "Impersonating" appeared only in an instruction about New Jersey's computer crime statute, not the CFAA. App2. 706.

person.<sup>6</sup> But Spitler's program was not designed to trick AT&T into thinking that 114,000 users had queried the website in rapid sequence. The program did not hide Spitler's Internet Protocol address. It did not send authenticating information such as personal passwords. It did not create the impression that the visits were coming from many different sources. Spitler's program did not impersonate anyone. It simply sent requests to a website. *Cf. United States v. Kane*, 450 F.2d 77, 85 (5th Cir. 1971) (noting that a police officer who answered the defendant's phone during a search of his apartment was not "impersonating" the defendant).

For the same reason, the government's claim that Spitler's program "tricked" AT&T's computer is wrong. GB 42. AT&T knew perfectly well that anyone who entered in the correct website address would obtain a user's e-mail address. AT&T made a deliberate choice to configure the website this way. App. 217-18, 258-59. No one was tricked by Spitler's program.

**D. Whether Spitler Used "Expertise" to Design the Program Is Irrelevant to Whether the Program Accessed AT&T's Computer Without Authorization.**

The government argues that Spitler's program was illegal because it required "computer expertise" to design it. GB 30. The government envisions two kinds of Internet users: (1) "ordinary" users, such as "a typical judicial law clerk," and

---

<sup>6</sup> See Merriam-Webster Online, <http://www.merriam-webster.com/dictionary/impersonate> (defining impersonate as "to pretend to be (another person)") (last visited Oct. 25, 2013).

(2) “skilled and determined” computer users, such as Spitler. *Id.* at 32-33. Basing its standard of criminal liability on “norms of behavior that are generally recognized by society” and that are apparent to a “reasonable person,” GB 35, the government argues that Spitler’s program was illegal because it exceeded expectations of what an “ordinary” computer user would obtain. *Id.* at 32, 35.

No court has ever adopted the Government’s proposed interpretation of the CFAA. Further, the First Circuit squarely rejected the Government’s interpretation in a very similar case, *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003). Zefer Corporation was a sophisticated business that used its “computer-related expertise” to help other companies. *Id.* at 60. It built “a scraper tool that could ‘scrape’ the prices” from the website of a leading travel business, EF Cultural Travel. *Id.* The scraper program was programmed to then download the collected data into an Excel spreadsheet for subsequent analysis. *Id.* Zefer designed the scraper program based on “proprietary information about the structure of the website and the tour codes” provided to it by a former employee of EF who left to work for a competitor, Explorica. *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001). The scraper program sent 30,000 queries to the EF website to build a database for Explorica. *Id.* at 579.

The queries sent by Zefer's program closely resembled the queries sent to AT&T's website in this case. Recall that Spittler's program sent queries to AT&T's website that looked like this:

*https://dcp2.att.com/OEPClient/openPage?ICCID=89014104243221  
019785&IMEI=0*

AB 19; App2. 263, 725-27. Similarly, Zefer's program sent queries to EF Cultural Travel's website that looked like this:

*http://www.eftours.com/tours/PriceResult.asp?Gate=GTF&TourID=LPM*

*Explorica*, 274 F.3d at 583 n.11. In this website address, the letters "GTF" and "LPM" were proprietary codes used by EF that apparently were only known to EF employees. *Id.* at 583.

When EF filed a civil CFAA suit, the district court applied the standard argued by the Government in this case. Specifically, the district court granted a preliminary injunction prohibiting use of the program because the program's use was "not in line with the reasonable expectations of the website owner and its users." *Id.* at 582 n.10.

On appeal, however, the First Circuit unanimously rejected the district court's "reasonable expectations" standard for CFAA liability. *Zefer*, 318 F.3d at 62-63. The First Circuit reasoned that "nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like 'reasonable expectations.'" *Id.* at 63. If EF wanted to ban access to its website in ways that the CFAA would

enforce, EF needed to do so in a way that would “giv[e] fair warning” to Internet users “and avoid[] time-consuming litigation about its private, albeit ‘reasonable,’ intentions.” *Id.* Use of Zefer’s program was authorized and legal.

The government’s proposed standard of liability is identical to that rejected by the First Circuit in *Zefer*. Mirroring the “reasonable expectations” test, the government’s “norms of behavior” standard, GB 35, is based on how a “reasonable person” would expect information to be collected from a website. This Court should reject that standard for the same reason the First Circuit did so: it puts users at the “mercy of a highly imprecise” and ambiguous standard that cannot be defined. *Zefer*, 318 F.3d at 63.

Such ambiguity is particularly problematic in a criminal case. It is one thing to adopt a vague standard that risks excessive civil litigation; it is quite another to adopt a vague standard that may lead to 41-month jail sentences. For that reason, the Supreme Court has emphasized that “a criminal statute must give fair warning of the conduct that it makes a crime[.]” *Bouie v. City of Columbia*, 378 U.S. 347, 350 (1964). The Constitution does not allow a criminal law to be “so vague and standardless that it leaves the public uncertain as to the conduct it prohibits or leaves judges and jurors free to decide, without any legally fixed standards, what is prohibited and what is not in each particular case.” *Giaccio v. Pennsylvania*, 382 U.S. 399, 402-03 (1966). The government’s vague and standardless approach,

resting on “norms of behavior that are generally recognized” by a “reasonable person,” GB 35, cannot provide the fair notice that the Constitution requires.

That is true for a common sense reason: Levels of computer expertise rapidly evolve and vary widely based on age and education. What seems complicated and shocking to an adult may seem easy and obvious to his children. The distinction between prohibited expert use and permitted novice use is particularly incoherent given how computer programs typically are developed. First, a computer expert uses effort and skill to build a program that anyone can use. Second, novices use the program to perform the same steps as the expert. *See* Daniel B. Garrie, *The Legal Status of Software*, 23 J. Marshall J. Computer & Info. L. 711, 713-23 (2011). Given this reality, courts have no way to distinguish between “purposeful action by a determined individual” that is criminal and “ordinary” action that is not. GB 29.

The malleability of the government’s standard is aptly demonstrated by the government’s dramatically different treatment of the facts of *Zefer* and the facts of this case. To distinguish *Zefer* under its proposed standard, the government must portray Spitler’s program as “sophisticated” and Zefer’s program as “ordinary.” It does so using a narrative trick. When describing the facts of this case, the government starts the story from the very beginning. The government’s brief goes

into glorious detail in its comprehensive technical description of how Spitler designed and used the program. *See* GB 5-10, 27-29.

In contrast, the government skips over all of these steps when describing the facts of *Zefer*. The government's brief states that Zefer was hired, and then it jumps immediately to the litigation that ensued after the program had been used. GB 31-32. The government neglects to point out (much less elaborate on) how an insider gave Zefer proprietary information about the website's structure needed to build the program, and how Zefer used its "computer-related expertise" to design the program. *See Zefer*, 318 F.3d at 60; *Explorica*, 274 F.3d at 583. The government's portrayal of one case as technologically complex and the other case as technologically simple merely reflects the government's choice to dwell on the technological details in one case but not the other. The difference is storytelling, not law. Criminal liability cannot rest on that standard.<sup>7</sup>

---

<sup>7</sup> The government suggests in passing that use of Spitler's program was illegal because it obtained information not available through a public search engine such as Google. GB 27. This suggestion misfires because the information collected by the scraper in *Zefer* would not have been available through a search engine, either. *See Zefer*, 318 F.3d at 60; *Explorica*, 274 F.3d at 583.

The government also fails to note that search engines such as Google themselves collect information by sending programs out to scrape data from websites on the Internet. *See Crawling & Indexing, - Inside Search*, Google, [http://www.google.com/intl/en\\_us/insidesearch/howsearchworks/crawling-indexing.html](http://www.google.com/intl/en_us/insidesearch/howsearchworks/crawling-indexing.html) (last visited Oct. 25, 2013). Under the government's approach, Google may be committing serious federal crimes by scraping data to create its search databases. Finally, whether Google or another search engine happens to make information available is largely a question of the policy followed by each



**E. Spitler's Program Was Not Illegal Because It Set the User Agent to that of an iPad.**

The government also argues that Spitler's program accessed the AT&T computer without authorization because it applied a user agent setting that matched that of an iPad. GB 20, 25, 28. The government acknowledges that user agents generally do not limit access. *Id.* at 56. But the government argues that this case is different because Spitler set the user agent to that of an iPad to obtain the email addresses. *Id.* at 20, 25. In the government's view, the user agent setting was a block on access, the circumvention of which violates the CFAA. GB 20, 55.

This argument is unpersuasive because user agents cannot act as access restrictions. A user agent is simply a browser setting. Every person who surfs the Internet can set the user agent as she wishes. User agents do not identify website requests as coming from particular people. They merely reflect the setting that the user picked or the web browser happened to select as a default. App2. 256-57.

An analogy based on physical trespass law helps explain why. *See* S. Rep. No. 99-432, at 7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484-85 (analogizing "unauthorized access" in the CFAA to physical trespass law). Imagine that a convenience store has posted a sign: "No shirts, no shoes, no service." A shirtless customer tries to enter the store. Because the customer is not

---

company. "Significant notice problems arise if we allow criminal liability to turn on the vagaries of private policies." *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (en banc).

wearing a shirt, the store clerk explains the store policy and denies the customer entry. The customer happens to have a shirt in his bag, however, so he puts on his shirt and then tries to enter the store again. This time, the clerk sees the customer's shirt and permits the customer to enter.

Now consider whether the customer is criminally liable for committing a trespass when he entered the store after putting on his shirt. The answer is obviously "no." It is true that the clerk initially blocked the customer's entrance, and the customer then devised a way to circumvent the block. But no trespass occurred because no one would understand the store's policy as an effort to keep that specific customer out. The store's policy would be understood as allowing everyone to enter on the simple condition that they wear a shirt and shoes. Anyone can do that. Because the customer put on his shirt after being denied entrance, he complied with the policy and he was fully authorized to enter the store when he did so. No trespass occurred because wearing a shirt is not an access restriction.

The same reasoning applies with user agents under the CFAA. To computer users, changing a user agent is like putting on a shirt. It is easily done and it takes a few seconds. It does not require any "lying" or "trickery," as user agents are not set to tell truth or falsehoods. User agents are simply settings that can be changed just like a person might change his clothes. A website that requires users to adjust the user agent to access it electronically is no different from a store that requires

customers to put on a shirt to access it physically. Users who comply with the store's condition on entry are fully authorized. Changing the user agent does not make a person guilty of trespass, whether that trespass is a physical trespass or the cyber trespass of the CFAA.

The ubiquity of changing user agents confirms the point. For example, Microsoft's Internet Explorer browser sets the default user agent to incorrectly identify itself as a Mozilla browser. *See Understanding User-Agent Strings*, Microsoft, <http://msdn.microsoft.com/library/ms537503.aspx> (last updated July 2013) ("For historical reasons, Internet Explorer identifies itself as a Mozilla browser."). When the most recent version of Internet Explorer was released, Microsoft decided to have the browser identify itself as a Mozilla 5.0 browser instead of a Mozilla 4.0 browser.<sup>8</sup> Microsoft does not consider itself or its users to be engaging in deception, or to be breaking into websites. User agents simply do not act as access restrictions.<sup>9</sup>

---

<sup>8</sup> *Default User-Agent (UA) String Changed*, Microsoft, [http://msdn.microsoft.com/en-us/library/ie/ff986085\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ie/ff986085(v=vs.85).aspx) (last visited Oct. 25, 2013).

<sup>9</sup> The explanation of user agents promulgated by the World Wide Web Consortium confirms this point. *See Header Field Definitions*, World Wide Web Consortium, <http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.43> (last visited Oct. 25, 2013).

**F. Substantial Authority Acknowledges the Ambiguity of ‘Unauthorized Access’ Under the CFAA**

As explained in Auernheimer’s opening brief, if this Court is unsure whether “authorization” in the CFAA encompasses Spitler’s actions, it should apply the rule of lenity and adopt a narrow construction of the statute that favors the defense. AB at 31-32.

The government responds that the rule of lenity should not apply because the CFAA’s prohibition on unauthorized access is clear. GB at 45-47. Three sister circuits have disagreed. *See, e.g., WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 205-06 (4th Cir. 2012) (recognizing widespread disagreement on the meaning of unauthorized access and adopting a narrow interpretation so as to “yield to the rule of lenity”); *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1134-35 (9th Cir. 2009) (rejecting a broad interpretation of unauthorized access because “the rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government”); *Explorica*, 274 F.3d at 582 n.10 (noting that the meaning of the term “has proven to be elusive.”).

This Court should heed these decisions and find that Spitler’s conduct did not violate the CFAA.

## **II. IF AUERNHEIMER CONSPIRED TO VIOLATE THE CFAA, THE VIOLATION WAS ONLY A MISDEMEANOR.**

The government argues that any conspiracy to violate the CFAA was a felony instead of a misdemeanor because it was in furtherance of a New Jersey statute, N.J. Stat. Ann. § 2C:20-31(a). GB 52-62. The government's argument is erroneous.

### **A. The Felony Enhancement Cannot Apply Because the Enhancement Requires Independent Conduct, Not an Additional Element.**

The government first contends that the felony enhancement under 18 U.S.C. § 1030(c)(2)(B)(ii) was proper because N.J. Stat. Ann. § 2C:20-31(a) contains an element not found in 18 U.S.C. § 1030(a)(2)(C). GB 52-55. According to the government, § 1030(a)(2)(C) does not include a distribution element while the New Jersey crime does. *Id.* The government misunderstands the law. The relevant legal question is whether the government has charged two different *acts*, not whether the government can identify a difference between two *statutes*.

The key precedent is *United States v. Cioni*, 649 F.3d 276, 278-79 (4th Cir. 2011), in which the Fourth Circuit overturned a felony conviction under § 1030(c)(2)(B)(ii) because the government tried to apply a felony enhancement based on a violation of the unauthorized access statute found in 18 U.S.C. § 2701(a) to a single course of conduct. The Fourth Circuit recognized that § 2701(a) and § 1030(a)(2)(C) are “distinct and different” crimes, and that “proof

of a § 2701(a) offense requires proof of facts that are not required for a violation of § 1030.” *Id.* at 282. Nonetheless, the court ruled the felony enhancement improper because “the facts or transactions alleged to support [the misdemeanor] offense are also the same used” to enhance the CFAA charge to a felony under § 1030(c)(2)(B)(ii). *See id.*

*Cioni* overturned a felony conviction for attempting to access another person’s email account because the “conduct” underlying the § 2701(a) crime was not “distinct” from the conduct underlying the § 1030(a)(2)(c) crime. *Id.* at 283.

*Cioni* explained:

Count 4, which claims two crimes, one in furtherance of the other, is actually based on Cioni’s single unsuccessful attempt to access Patricia Freeman’s AOL electronic e-mail account. . . . If the government had proven that Cioni accessed Freeman’s e-mail inbox and then used the information from that inbox to access another person’s electronic communications, no merger problem would have arisen. But the government charged and attempted to prove two crimes using the same conduct . . . .

*Id.* at 283.

The same reasoning applies here. N.J. Stat. Ann. § 2C:20-31(a) is an unauthorized access statute that contains an element of crime that is not found in 18 U.S.C. § 1030(a)(2)(C), just like § 2701(a) is an unauthorized access statute that “requires proof of facts that are not required for a violation of § 1030.” *Id.* at 282. But just like in *Cioni*, the government’s argument must fail because the government is charging a single course of conduct. Specifically, the government is

attempting to prove its case based on a conspiracy to gather information from AT&T's website and share the information with a reporter. That is a single course of conduct, and *Cioni* forbids the felony enhancement.

**B. Auernheimer Did Not Violate N.J. Stat. Ann. § 2C:20-31(a) Both Because the Program Did Not Circumvent a Code-Based Restriction and Because New Jersey Does Not and Cannot Regulate Purely Extraterritorial Conduct.**

Even if this court concludes that the felony enhancement can apply despite *Cioni*, it does not apply in this case because the conduct proved at trial did not violate N.J. Stat. Ann. § 2C:20-31(a). That is true for two reasons. First, obtaining the information from AT&T's servers did not constitute unauthorized access under New Jersey law as construed in *State v. Riley*, 988 A.2d 1252, 1267 (N.J. Super. Ct. Law Div. 2009). And second, New Jersey's unauthorized access statute does not extend to acts occurring entirely outside New Jersey.

*1. The Program Did Not Violate New Jersey Law Because It Did Not Circumvent Any Code-Based Restrictions.*

The government first argues that the conduct violated N.J. Stat. Ann. § 2C:20-31(a) because either the conduct circumvented a code-based restriction or at least impersonated an iPad user. GB 55-57. This is incorrect. As the government appears to acknowledge, the "code-based restriction" test adopted in *Riley* comes from a law review article, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596 (2003).

*See Riley*, 988 A.2d at 1262, 1267; *see also* GB at 57. As described in *Cybercrime's Scope*, the circumvention of a code-based restriction requires the computer owner to “erect code-based barriers to unwanted access” such as a password gate. *Id.* at 1651. Here, that did not occur: AT&T published the information on the Web where anyone with a web browser could access it.

Alternatively, the Government relies on *State v. Gaikwad*, 793 A.2d 39 (N.J. App. Div. 2002) for the view that “impersonating an authorized user constitutes unauthorized access” under New Jersey law even absent circumvention of a code-based restriction. GB 57-58. This argument fails because the defendant in *Gaikwad* clearly circumvented a code-based restriction. Gaikwad hacked in to a computer network that required a username and password to access it, and he used that access to break into private accounts to specific individuals at AT&T. *Gaikwad*, 793 A.2d at 70-74.

2. *The Program Did Not Violate N.J. Stat. Ann. § 2C:20-31(a) Because New Jersey Law Does Not and Cannot Apply to Purely Extraterritorial Conduct.*

The government wrongly assumes that this Court must review the territorial scope of New Jersey law for plain error because it was not specifically argued below. *See* GB 58. Under this Court’s precedent, however, the standard of review is *de novo*. “[A] timely motion for acquittal under Federal Rule of Criminal Procedure 29(c) will preserve a sufficiency-of-the-evidence claim for review,



irrespective of whether the defendant raised the claim at trial.” *United States v. Miller*, 527 F.3d 54, 62 (3d Cir. 2008). A nonspecific motion under Rule 29 preserves all sufficiency claims. *See United States v. Walker*, Nos. 11–2727, 11–2845, 11–3087, 11–3088, 2013 WL 3481682, at \*1 (3d Cir. 2013) (citing *United States v. Hammoude*, 51 F.3d 288, 291 (D.C. Cir. 1995)). Further, a preserved sufficiency claim is reviewed *de novo*. *See United States v. Pavulak*, 700 F.3d 651, 668 (3d Cir. 2012). Auernheimer filed a timely Rule 29(c) motion as well as a timely Rule 29(a) motion, so this sufficiency claim was fully preserved and the standard of review is *de novo*. *See App2. 339, 729-731.*

On the merits, the government argues that New Jersey has jurisdiction over the offense because the disclosure of the email addresses occurred in New Jersey when a New Jersey FBI agent read the Gawker story from his office in Newark. GB 60. This claim is based on a misunderstanding of the record. Auernheimer disclosed the list of collected email addresses to Ryan Tate of *Gawker*. App2. 150, 273, 349. The record does not indicate the state in which Tate was located, but there was no evidence that Tate was in New Jersey. *See App2. 349, 359, 599-600, 602-03.* When *Gawker* ran its story, it did not publish the list of email addresses. App1. 8. As the evidence at trial showed, the *Gawker* article included only a small number of redacted email addresses, none of which were of users in New Jersey. *Id.* Contrary to the government’s claim, no disclosure of any New Jersey email

address occurred in New Jersey or was even viewable over the Internet from a New Jersey location.

The government is also wrong in claiming New Jersey can regulate purely out of state conduct under the Dormant Commerce Clause, thus permitting a statutory interpretation of New Jersey criminal law to cover transactions entirely outside New Jersey. GB 61. The government relies on *dicta* from *McBurney v. Young*, 133 S.Ct. 1709 (2013), to suggest that the Dormant Commerce Clause only protects against “protectionist measure[s].” GB 61 (citing *McBurney*, 133 S. Ct. at 1719-20). To the contrary, “a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State’s authority and is invalid regardless of whether the statute’s extraterritorial reach was intended by the legislature.” *Healy v. Beer Institute, Inc.*, 491 U.S. 324, 336 (1989) (internal quotations omitted).

In this case, the United States wants to construe New Jersey’s computer crime law to have exactly the extraterritorial control that the dormant Commerce Clause forbids. Further, the government’s statutory construction of New Jersey criminal law would not only apply to prosecutions brought under N.J. Stat. Ann. § 2C:20-31(a), but to all of New Jersey’s criminal laws, or at least all of New Jersey’s computer crime laws, which share the same territorial reach. *See* AB 37. The United States wants New Jersey law to reach out and regulate transactions

throughout the entire country – if not the entire world – whenever anyone anywhere does anything that might impact New Jersey residents. GB 60. The Dormant Commerce Clause forbids such a law. *See, e.g., PSINet, Inc. v. Chapman*, 362 F.3d 227, 240-41 (4th Cir. 2004) (enjoining Virginia Internet regulation); *American Civil Liberties Union v. Johnson*, 194 F.3d 1149, 1160-61 (10th Cir. 1999) (enjoining a New Mexico Internet regulation); *Center For Democracy & Technology v. Pappert*, 337 F.Supp.2d 606, 662 (E.D. Pa. 2004) (striking down Pennsylvania law on Internet filtering that regulated all websites viewable from Pennsylvania because the law “has the practical effect of exporting Pennsylvania’s domestic policies” nationwide); *American Libraries Ass’n v. Pataki*, 969 F.Supp. 160, 173-75 (S.D.N.Y. 1997).

There is no New Jersey precedent interpreting the territorial scope of its computer crime statutes. The language of the territorial limit is vague, leaving uncertain whether the New Jersey legislature intended it to have extraterritorial effect. This Court should reject the government’s novel and unprecedented interpretation by construing the New Jersey statute to not extend to purely extraterritorial offenses in light of constitutional concerns. *See Miller v. French*, 530 U.S. 327, 335 (2000) (“[C]onstitutionally doubtful constructions should be avoided where ‘fairly possible.’”) (citing *Communications Workers v. Beck*, 487

U.S. 735, 762 (1988)). So construed, the conduct of Auernheimer and Spitler did not violate N.J. Stat. Ann. § 2C:20-31(a).

### **III. THE GOVERNMENT CANNOT DEFEND AUERNHEIMER'S CONVICTION ON COUNT 2 BASED ON A NEW THEORY OF LIABILITY NEVER PRESENTED TO THE JURY.**

The government's defense of Count 2 begins by claiming that plain error review should apply because Auernheimer's sufficiency argument was not raised in precisely the same form at trial. GB 63, n. 21. The government is wrong again. As noted earlier, "a timely motion for acquittal under Rule 29(c) will preserve a sufficiency-of-the-evidence claim for review, irrespective of whether the defendant raised the claim at trial." *Miller*, 527 F.3d at 62. Auernheimer is challenging the sufficiency of the evidence under Count 2, and he filed a timely motion for acquittal both under Rule 29(a) under Rule 29(c) on that count. *See* App2. 339, 729-31. His claim is therefore preserved for *de novo* review. *See Walker*, 2013 WL 3481682 at \*1, *Pavulak*, 700 F.3d at 668.

On the merits, the Government defends the conviction for Count 2 by introducing a theory of liability never presented to the jury. Count 2 charged Auernheimer with identity theft in violation of 18 U.S.C. § 1028(a)(7). At trial, the government argued that Auernheimer violated Count 2 by possessing the email/ICC-ID pairings and then transferring them to Gawker in relation to the prior

offense of violating the CFAA by using the program to collect the email addresses.

The prosecutor argued to the jury that it should convict on Count 2 on that basis:

So with those e-mail addresses and those ICC-IDS that the defendant possessed and transferred to Gawker, were those means of identification? The evidence is clear that they were. And how do you know? The defendant possessed and transferred e-mail addresses to Gawker. . . . We know the information the defendant possessed and transferred were means of identification.

App2. 598-99.

In response to Auernheimer's challenge to the conviction on Count 2, the government now defends the conviction on appeal by switching to an entirely different argument. For the first time, the government advances a new appellate theory that Auernheimer violated § 1028(a)(7) because he "used" the ICC-IDs by entering them into Spitler's program *before* the unauthorized access was committed in order to collect the e-mail addresses from AT&T's website. *See* GB 64-65 ("Auernheimer mistakenly focuses on his '*transfer*' of the *e-mail addresses*. But the correct focus should be on his '*use*' of the *ICC-IDs*. Auernheimer used the ICC-IDs, which qualified as a means of identification, 'with the intent to commit' the federal crime of unauthorized computer access.").

The government introduces this new theory to try to satisfy the dual criminality requirement of § 1028(a)(7) that was absent at trial. *See* AB 39-41. By switching to a new theory of liability, the Government can now articulate two offenses: First, the use of the ICC-IDs in violation of the CFAA, and second, the

disclosure of the email/ICC-ID pairings to *Gawker* in violation of New Jersey law. *See* GB 66-67. On that basis, the Government argues that the conviction in Count 2 should be affirmed. *See id.*

The government's creative reimagining of its case fails because of a bedrock principle of appellate review: An appellate court "cannot affirm a criminal conviction on the basis of a theory not presented to the jury." *Chiarella*, 445 U.S. at 236; *see also Dunn v. United States*, 442 U.S. 100, 107 (1979) ("[A]ppellate courts are not free to revise the basis on which a defendant is convicted simply because the same result would likely obtain on retrial"). For an appellate court to affirm a conviction based on the sufficiency of the evidence, the court can only consider the argument that the government actually "built its case" on as "part of a coherent theory of guilt" at trial. *Cola v. Reardon*, 787 F.2d 681, 693 (1st Cir. 1986).

The government's new argument for why Auernheimer violated Count 2 must be rejected because it was never presented to the jury. The prosecutors never argued that including the ICC-IDs in the website addresses was a prohibited "use" of those numbers. Further, recall that Count 2 was not charged as a conspiracy. *See* App1. 16. Given that Spitler was the one who "used" the ICC-IDs, not Auernheimer, the government would have needed to instruct the jury on the principles of accomplice liability to allow the jury to decide whether Auernheimer

aided and abetted Spitler’s “use.” The government never asked for an aiding and abetting instruction, however, and the jury never received one. *See* App2. 708-09. Because the government’s new theory was never presented to the jury – and the jury did not even receive the instructions needed to assess this new argument – the Court cannot affirm the conviction on that basis.<sup>10</sup>

#### **IV. VENUE WAS IMPROPER IN NEW JERSEY ON BOTH COUNTS**

Even if this Court concludes that Auernheimer was guilty of both Counts, the Court must vacate the convictions because the government failed to establish venue in the District of New Jersey. The Government presents a series of novel arguments for why venue was proper in New Jersey. None of their arguments are persuasive.

##### **A. The “Substantial Contacts” Test Cannot Establish Venue Because it is a Limitation on Venue and Not a Test to Establish It.**

The government’s first argument is that venue was established under the “substantial contacts” test referred to in *United States v. Goldberg*, 830 F.2d 459, 466 (3d Cir. 1987) (quoting *United States v. Reed*, 773 F.2d 477, 480-81 (2d Cir. 1985)). The government presents the substantial contacts test as a “broader test” than the crucial elements test found elsewhere in Third Circuit caselaw. GB 70.

---

<sup>10</sup> Such an argument would have been an uphill battle for a range of reasons, among them that ICC-IDs taken alone are not “means of identification.” *See United States v. Mitchell*, 518 F.3d 230, 235 (4th Cir. 2008) (use of another person’s name not enough in and of itself to be use of a “means of identification” for § 1028 since name may not be “sufficiently unique”).

The government then argues that venue exists under the substantial contacts test even if no crucial elements of the offenses occurred in New Jersey. *Id.* at 71-73<sup>11</sup>

The Government's argument reflects a simple misunderstanding of the substantial contacts test. The substantial contacts test is a constitutional *limitation* on venue, not a means of *establishing* venue. *See United States v. Davis*, 689 F.3d 179, 186 (2d Cir. 2012) (quoting *Reed*, 773 F.2d at 481) ("To comport with constitutional safeguards," venue "require[s] more than 'some activity in the situs district'; instead, there must be 'substantial contacts . . . .'"); *Goldberg*, 830 F.2d at 466 (describing the substantial contacts test as the test that "[t]he constitution requires"). In other words, establishing venue requires the government to satisfy *both* the statutory essential elements test and *also* the constitutional substantial contacts test. *See United States v. Royer*, 549 F.3d 886, 895 (2d Cir. 2008) (noting that "venue must not only involve some activity in the situs district but also satisfy the 'substantial contacts' test"); *Saavedra*, 223 F.3d at 93.

Further, it is unclear whether the Third Circuit has adopted the substantial contacts test. The Second Circuit established the test in *Reed* in 1985, and a few other circuits have discussed it since then. *See, e.g., United States v. Muhammad*, 502 F.3d 646, 652 (7th Cir. 2007); *United States v. Williams*, 274 F.3d 1079, 1084

---

<sup>11</sup> The "crucial elements" test is another term for the "essential conduct elements" test. *Compare United States v. Pendleton*, 658 F.3d 299, 303 (3d Cir. 2011) ("crucial element"), with *United States v. Saavedra*, 223 F.3d 85, 90 (2d Cir. 2000) ("essential conduct element").



(6th Cir. 2001); *United States v. Cofield*, 11 F.3d 413, 417 (4th Cir. 1993). However, it is uncertain whether the Third Circuit adopted the test. This Court's decision in *Goldberg* quoted from *Reed*, to be sure, but without the context or explanation needed to know if the court was adopting it as Third Circuit precedent. *See Goldberg*, 830 F.2d at 466. And the Third Circuit has not mentioned the substantial contacts test since *Goldberg* in over a quarter of a century of subsequent caselaw.

Supreme Court decisions after *Goldberg* explain why this Court has not cited the substantial contacts test since 1987. At the time of *Reed* and *Goldberg*, the precise relationship between the substantial contacts test and statutory venue requirements was uncertain. The Supreme Court's subsequent decisions in *United States v. Cabrales*, 524 U.S. 1 (1998), and *United States v. Rodriguez-Moreno*, 526 U.S. 275 (1999), established a rigorous elements-based approach to interpreting venue under statutory law. "[T]he focus in those cases on the actual elements of the crime" was "inconsistent with the substantial contacts standard insofar as it would establish venue based on an 'effect' that is not an element of the crime." 4 Wayne R. LaFare, *et al.*, *Criminal Procedure* § 16.2(e) (3d ed. 2012).

Put another way, the Supreme Court's decisions have not eliminated the "substantial contacts" test, but they have rendered the test irrelevant to whether venue exists based on effects of a crime. Because statutory venue cannot exist

based on a claimed effect that is not a statutory element of the crime, *see United States v. Clenney*, 434 F.3d 780, 782 (5th Cir. 2005) (per curiam), the constitutional substantial contacts test cannot play a role in determining venue in such cases. At most, the substantial contacts test will only provide an additional alternative basis for the conclusion that no venue existed. *See, e.g., United States v. Alvarado*, --- F.Supp.2d ----, 2013 WL 3816692 at \*4 (E.D.Wis. 2013) (finding no venue in Wisconsin where a prisoner in Oklahoma threatened to kill his probation officer located in Wisconsin under both the elements test and substantial contacts test).

For these reasons, the government's effort to establish venue based on the "substantial contacts" test cannot succeed.

**B. The Government Cannot Establish Venue for Count 1 by Invoking the Prosecutor's Decision to Charge Count 1 as a Felony Using a New Jersey Statute.**

The Government next argues that venue exists for Count 1 under the "crucial elements" test because it charged Auernheimer with a conspiracy to violate the CFAA in furtherance of a New Jersey law. In the Government's view, the prosecutor's decision to charge Count 1 using a felony enhancement based on a New Jersey law violation creates venue in New Jersey. GB at 75-77.

The government's argument is incorrect. When Congress "makes an offense dependent on proof of an antecedent crime, that language will not support venue."

*United States v. Oceanpro Indus., Ltd.*, 674 F.3d 323, 329 (4th Cir. 2012). This reflects the basic principle that Congress, not the prosecutor, decides where venue is proper. See *Travis v. United States*, 364 U.S. 631, 634 (1961) (“[V]enue provisions in Acts of Congress should not be so freely construed as to give the Government the choice of a tribunal favorable to it.”) (internal quotation marks omitted).

The Fourth Circuit’s decision in *United States v. Bowens*, 224 F.3d 302 (4th Cir. 2000), is illustrative. Bowens was charged with harboring fugitives in violation of 18 U.S.C. § 1071, which prohibits “harbor[ing] or conceal[ing] any person for whose arrest a warrant or process has been issued under the provisions of any law of the United States, so as to prevent his discovery and arrest[.]” After arrest warrants had been issued in the Eastern District of Virginia, Bowens harbored the two fugitives within the district of South Carolina. *Bowens*, 224 F.3d at 305-07.

The Fourth Circuit held that venue was improper in the Eastern District of Virginia even though the predicate crime was established by arrest warrants there. The court conceded that “issuance of a federal arrest warrant” in Virginia was “an essential element of the government’s case.” *Id.* at 309. Nonetheless, venue was improper in Virginia because venue was “limited to the place where the essential *conduct* elements occur, without regard to the place where other essential elements

of the crime occur[.]” *Id.* (emphasis added). The government could charge the defendant with harboring fugitives only in South Carolina, where the essential conduct of harboring the fugitives took place. *See id.*

*Bowens* explains why the government’s choice to invoke a predicate state offense in Count 1 cannot establish venue in the state where that law originates. The predicate state law violation has no impact on the “essential conduct” that Congress prohibited. Just as the Virginia warrants in *Bowens* could not establish venue in Virginia, so the government’s claim that the conduct also violated New Jersey law cannot establish venue in New Jersey. A prosecutor’s decision to pick a New Jersey law as a possible felony enhancement no more creates venue in New Jersey than would picking a federal law create venue in every federal district.

The government’s reliance on *Rodriguez-Moreno* is misplaced. Under *Rodriguez-Moreno*, the key distinction is between an “essential conduct element” that establishes venue and a “circumstance element” that does not. 526 U.S. at 280 n. 4 (citing *Cabrales*, 524 U.S. at 7). An “essential conduct element” describes the act that the defendant committed, while the “circumstance element” describes the circumstances that existed at the time of his act. *Id.* The felony enhancement cannot create venue in New Jersey under *Rodriguez-Moreno* because it is a circumstance element rather than an essential conduct element.

This is clear from both the plain text of the felony enhancement and its location in 18 U.S.C. § 1030. The felony enhancement does not appear in § 1030(a), the part of the CFAA that identifies criminal conduct. Instead, it appears in § 1030(c), which states the statutory maximum punishments for different CFAA offenses. Consider the language of the felony enhancement as a whole:

(c) The punishment for an offense under subsection (a) or (b) of this section is— . . . (2)(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2),. . . if— (i) the offense was committed for purposes of commercial advantage or private financial gain; (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or (iii) the value of the information obtained exceeds \$5,000[.]

18 U.S.C. § 1030(c)(2). This language does not describe “essential conduct” that Congress prohibited. Instead, it merely identifies various circumstances in which “an offense under subsection (a) or (b)” is punished as a 5-year felony instead of a misdemeanor. *Id.* The circumstances do not change the underlying offense or expand venue. They merely change the maximum statutory punishment at sentencing. Because they are only circumstance elements, they are not essential conduct elements and cannot establish venue. *See United States v. Coplan*, 703 F.3d 46, 78-79 (2d Cir. 2012); *United States v. Strain*, 396 F.3d 689, 694 n.5 (5th Cir. 2005).

*Clenney* is also on point. *Clenney* lived in the Southern District of Texas, and he had fathered a child who lived with his mother in the Northern District of Texas. *Clenney*, 434 F.3d at 781. When the child was visiting *Clenney* in the Southern District, *Clenney* kidnapped the child and took him to Belize. *Id.* *Clenney* was charged in the Northern District with removing a child from United States “with intent to obstruct the lawful exercise of parental rights” in violation of 18 U.S.C. § 1204. The government argued that venue was proper in the Northern District because he had formed the relevant intent in the Northern District and because the mother’s parental rights were affected in the Northern District. *Clenney*, 434 F.3d at 781.

The Fifth Circuit rejected the government’s argument and reversed the conviction, ruling that venue was improper in the Northern District because no essential conduct element of the crime occurred there. *Id.* at 781-82. The forming of the required intent was merely a circumstance that existed when *Clenney* acted, not the act itself. *Id.* at 782. As a result, the intent was “plainly not an essential conduct element as required by *Rodriguez-Moreno*” and could not establish venue. *Id.* (quotations omitted). The effect on parental rights in the Northern District was similarly irrelevant because it was not an essential conduct element of the crime. *Id.* The reasoning of *Clenney* is fully applicable here: Neither a circumstance

element of the crime nor alleged affects of the crime can create venue in New Jersey because no essential conduct element was committed there.

**C. The Government Cannot Establish Venue for Count 1 Based on a Failure to Act in New Jersey.**

The government next claims there was venue in New Jersey for Count 1 because Spitler and Auernheimer had a legal obligation to obtain explicit authorization from 4,500 New Jersey residents before using their ICC-ID numbers to access AT&T's servers. GB 80. The failure to do so implicitly took place in New Jersey, the government contends, making venue proper there. *Id.*

The government's argument is wrong. There is no support for the government's view that the failure of a person to take steps to nullify a criminal act establishes venue wherever that failure to nullify a criminal act occurs. "[V]enue is limited to the place 'where the criminal act is done.'" *Bowens*, 224 F.3d at 309 (quoting in part *United States v. Anderson*, 328 U.S. 699, 705 (1946)). There is no precedent for the government's claim that venue additionally lies in any district where a hypothetical act could have occurred that would have prevented the offense. *Cf. Clenney*, 434 F.3d at 782.

The government's authority is a sentence found in a treatise that "[i]f the statute makes it a crime to fail to do some act required by law, the failure takes place in, and the proper venue is, the district in which the act should have been done." GB 80 (citing 2 Charles Alan Wright, *et al.*, *Federal Practice and*

*Procedure* § 302 (4th ed. 2013)). That sentence offers no support here, however, as that that rule only applies when the law expressly mandates an act and therefore criminally punishes the omission of that act. *See* Wright, *supra*. Examples of such crimes include the failure to pay income taxes, failure to sign up for the draft, and the failure to pay child support. *Id.*; *see generally* Wayne R. LaFare, *Criminal Law* § 6.2 (4th Ed. 2003) (discussing crimes of omission).

When the government creates a criminal offense that mandates an affirmative act, the failure to act creates venue where the criminal omission occurs. *See* Wright, *supra*. But that guidance has no relevance to the CFAA, as the CFAA does not mandate any conduct. Like most criminal statutes, the CFAA permits inaction and punishes prohibited acts. It does not mandate actions and punish inaction. As a result, venue standards for crimes of omission are irrelevant.<sup>12</sup>

**D. Venue Was Not Established for Count 1 When an FBI Agent In New Jersey Read About the Alleged Offense Over the Internet.**

The Government's next argument is that venue was proper for Count 1

---

<sup>12</sup> Even if the court accepted the government's novel "failure to act" theory of venue, it would not establish venue in this case. As with all trespass statutes, the right to control authorization belongs to property owner. *See, e.g., Verizon Nw., Inc. v. Main St. Dev., Inc.*, 693 F. Supp. 2d 1265, 1278 (D. Or. 2010). A property owner may confer rights to access his property to others, but it retains the ultimate right to control its property. In the context of the CFAA, the computer owner controls access rights on the computer. *See Brekka*, 581 F.3d at 1133. If "permission" needs to be obtained to access a computer, the source of that permission is from the owner rather than the user. As a result, even under the government's theory, the venue for a CFAA offense would be where AT&T is located, not where its users are located.



because an FBI agent in New Jersey read about the alleged crime over the Internet. GB 84-89. The Government's theory appears to be that the crime of Count 1 continued for a long time after the actual elements of the crime were satisfied. After Auernheimer and Spitler conspired to violate the CFAA, as charged in Count 1, the following events occurred: First, Spitler collected the email addresses; next, Auernheimer disclosed the email addresses to *Gawker*; after that, *Gawker* published its story; and finally, when the *Gawker* story became a major news event, an FBI agent in New Jersey visited the *Gawker* website and read the story. *Id.* at 84-86. In the Government's telling, all of these acts are a part of the continuing crime, so there is venue in New Jersey where the FBI agent was sitting when he surfed the web and stumbled across the *Gawker* story. *Id.*

The Government's theory is incorrect. Under 18 U.S.C. § 3237, conduct cannot establish venue after the crime has been completed. And the crime is complete after the elements of the offense have been satisfied. For example, when Congress punishes traveling with intent to engage in illicit sexual conduct, the crime is completed "as soon as one begins to travel with the intent to engage in a sex act with a minor." *Pendleton*, 658 F.3d at 304. When Congress prohibits passport fraud, the crime is complete when the false statement is made and does not continue on to the time the application is processed. *United States v. Salinas*, 373 F.3d 161, 166 (1st Cir. 2004). When Congress prohibits making a false

statement, the crime is complete when the statement is made. *United States v. Bin Laden*, 146 F.Supp.2d 373, 377 (S.D.N.Y. 2001).

Under these principles, the crime described in Count 1 was completed when the unauthorized access occurred and the information was collected. The offense began in California, where Spitler was located. App.2 233. The crime continued in Arkansas, where Auernheimer was based. *Id.* at 185. The offense was completed when Spitler accessed AT&T's servers in Atlanta, Georgia and Dallas, Texas, and obtained the ICC-ID/email pairings. *Id.* at 434-35, 443-44.

What happened afterwards was not part of the offense charged in Count 1, and therefore what happened afterwards cannot establish venue. The offense did not continue into New Jersey simply because the FBI agent who eventually decided to investigate the crime happened to be in New Jersey. The investigation that started after the *Gawker* story was featured on the *Drudge Report* is not part of crime. *Cf., Travis*, 364 U.S. at 634 (noting that venue "should not be so freely construed" as to give the Government its choice of venue); *United States v. Ramirez*, 420 F.3d 134, 146 (2d Cir. 2005) (explaining that "provisions implicating venue are to be narrowly construed").

The government's reliance on *United States v. Rowe*, 414 F.3d 271 (2d Cir. 2005), is misplaced. The Government presents *Rowe* as a case about "venue for internet crimes," and it argues that because the court found venue where a

government agent was located in that case it must also stand for allowing venue here. GB 84. Not so. *Rowe* stands for the entirely unremarkable principle that a crime prohibiting the distribution of an illegal communication can be prosecuted wherever the communication was sent or received. *Rowe*, 414 F.3d at 279-80. Of course that is the case: The illegal communication actually travels from one district to another, creating venue in both districts. *See, e.g., United States v. Thomas*, 74 F.3d 701, 709 (6th Cir.1996) (venue for distributing illegal obscenity). That has no relevance here, however, as the crime charged in Count 1 was not a distribution offense.<sup>13</sup>

**E. Assuming Venue Was Proper for Count 1, Venue Was Improper For Count 2.**

The Government next asserts that venue for Count 2 was proper because it was proper for Count 1. GB 94-95. The government bases this conclusion on the Second Circuit's rule that venue for an identity theft crime is proper wherever venue is proper for the predicate crime. *See id.* (citing *United States v. Magassouba*, 619 F.3d 202, 203 (2d Cir. 2010)).

The Government's argument fails on its own terms by ignoring the indictment. The Government did not charge Count 1 as the underlying predicate

---

<sup>13</sup> The Government also relies on the Magistrate Judge's opinion in *United States v. Powers*, No. 8:09-cr-00361, 2010 WL 1418172 (D. Neb. Mar. 4, 2010). GB 87-89. As explained in Auernheimer's opening brief, that case is distinguishable because the defendant actually sent messages into the jurisdiction where the case was charged. *See* AB 50, n. 19.

offense of Count 2. Instead, the predicate offense charged in Count 2 was a misdemeanor violation of 18 U.S.C. § 1030(a)(2)(C) without the felony enhancement. *See* App1. 6. Because the government’s case for venue on Count 1 rests primarily on the felony enhancement that charged a violation of New Jersey law, the arguments for venue in Count 2 cannot rely on any of those arguments. Instead, venue must be established based only on the venue of the underlying predicate misdemeanor offense that had nothing to do with New Jersey. The Government cannot satisfy that standard. *See* AB 49.

The Government also argues that venue is proper for Count 2 even if it is improper for Count 1 “because identity fraud is a more personal victim-based harm than computer fraud, and the residence of the victims matters far more here than the location of the computer servers.” GB 96. This argument reflects the same erroneous effects-based approach to venue found in its discussion of Count 1 discussed above. The fact that a crime can have effects in a district does not create venue there. *See, e.g., Clenney*, 434 F.3d at 782 (finding venue improper for crime of interfering with parental rights in the district where parent resides and the effects of the crime are felt).

**F. Venue is Not Subject to Harmless Error Review.**

The government concludes its venue discussion with the assertion that if venue was improper, any error was harmless. GB 97-98. This argument must be rejected because venue is not subject to harmless error review:

If the venue issue was properly raised in the trial court and is properly before the appellate court, upon a finding that the proof of venue was insufficient (either because the prosecution pursued an incorrect legal theory in placing venue in the particular district or failed to present sufficient evidence as to alleged events that would establish venue in the district), the conviction will be reversed. Failure of venue will not be treated as harmless error.

LaFave, *et al.*, *Criminal Procedure*, 16.1(g). Notably, the government points to no Third Circuit case applying harmless error review to venue errors.

Instead, the government relies chiefly on a district court case from another circuit that applied harmless error review to a venue defect. *See* GB 98 (citing *United States v. Hart-Williams*, 967 F. Supp. 73 (S.D.N.Y. 1997)). Subsequent circuit decisions indicate that the district court decision is not good law even in that circuit. *See United States v. Brennan*, 183 F.3d 139, 149 (2d Cir. 1999); *Saavedra*, 223 F.3d at 100 n.5 (Cabranes, J., dissenting) (considering the possibility of introducing a harmless error rule for venue but noting that “absent a decision by this Court *en banc*, application of the harmless error rule to this case is foreclosed by our opinion in *Brennan*”). It is plainly not good law in the Third Circuit, which has never adopted a harmless error standard for improper venue.

Even if a harmless error rule applied, the venue error is not harmless. Auernheimer was hauled from Arkansas to New Jersey to face a criminal indictment in a district far from home that he had never even visited before. This is not a case in which the defendant merely “was tried on the wrong side of the Brooklyn Bridge.” *Hart-Williams*, 967 F. Supp. at 78.

Thus, the venue defects were not harmless error and the conviction must be reversed.

**V. THE ALLEGED MAILING COSTS WERE NOT “LOSS” UNDER THE SENTENCING GUIDELINES.**

Auernheimer argued in his opening brief that the 41-month sentence imposed upon him was improper for three reasons. AB 51-59. First the government failed to prove AT&T suffered an approximately \$73,000 “loss” for purposes of the U.S. Sentencing Guideline calculations. *Id.* at 51-53. Second, the alleged mailing costs did not qualify as “loss” for purposes of the CFAA, and in turn, United States Sentencing Guideline (“U.S.S.G.”) § 2B1.1. *Id.* at 53-57. And finally, the supposed mailing costs were unreasonable since email notice was effective. *Id.* at 58-59. None of the government’s arguments have merit.

**A. The Government Failed to Prove AT&T Suffered a \$73,000 “Loss.”**

*1. The Standard of Review Should Be Clear Error, Not Plain Error.*

The standard of review for factual findings during sentencing, including loss calculations under U.S.S.G. § 2B1.1, is clear error. *See United States v. Dullum*, 560 F.3d 133, 137 (3d Cir. 2009). A finding is “clearly erroneous” when this Court finds a “definite and firm conviction that a mistake has been committed.” *United States v. Grier*, 475 F.3d 556, 570 (3d Cir. 2007) (quoting *Concrete Pipe & Prods. of Cal., Inc. v. Constr. Laborers Pension Trust for S. Cal.*, 508 U.S. 602, 622 (1993) (quotation omitted)).

The government argues that the Court should review this claim under the much more deferential plain error standard, arguing that Auernheimer failed to raise this objection at sentencing. GB 104. The government is wrong. In his sentencing papers, Auernheimer objected that the “evidence at trial established no loss to AT&T,” and specifically noted that AT&T declined the probation office’s offer to provide a statement of its losses for inclusion in the presentence report (“PSR”). *See* App2. 748. He made the same objection at the sentencing hearing, telling the district court “there was no evidence submitted at trial as to this loss by AT&T. AT&T was given an opportunity by the Probation Department to submit an affidavit as to its damages. It did not do so.” *Id.* at 762.

Both the sentencing papers and this colloquy make clear that Auernheimer objected to the government's proof on loss. The government's position is also undermined by the fact that Auernheimer argued the total offense level should have been six under the Guidelines, a challenge to both the legal and factual conclusions underpinning the PSR's recommended sentencing range. *Id.* at 748.<sup>14</sup> The proper standard of review is clear error, not plain error.

2. *Nothing in the Record Supports the "Loss" Amount.*

Just as it failed to point to any evidence of the "loss" amount at trial and sentencing, the government can point to nothing in the record below to support the "loss" amount in its reply brief.

The sole evidence of "loss" mentioned in the government's reply brief is the last sentence of the criminal complaint, filed more than two years before the sentencing, which noted "AT&T has spent approximately \$73,000 in remedying the data breach." *Id.* at 58. But where this number came from is a mystery. Despite the fact AT&T's assistant vice president, Shirley Ramsey, testified at the trial, she presented no evidence of the amount of loss. *Id.* at 212-22. Nor did the PSR present any direct evidence – such as an invoice, receipt or expense report –

---

<sup>14</sup> Nor would Auernheimer's reference to the "\$73,167 'loss'" in his sentencing papers be a concession that he agreed that amount was proven. *See* GB at 104; App2. 750. Rather, given the fact that both the PSR and the government's sentencing papers used that amount to calculate the Guideline calculations, it would have been foolish for Auernheimer to ignore this assertion.



explaining how this amount was determined. While AT&T had the chance to explain its “losses” in the PSR, it declined to do so, as Auernheimer pointed out in his sentencing papers and before the district court. *See* PSR at 18, ¶ 53, App2. 748, 762.

The government has not and cannot provide this Court with information such as how much was spent on envelopes, printing or postage. In the absence of any actual evidence – rather than conjecture – as to how much AT&T spent, the government failed to make a “prima facie case of the loss amount,” and thus applying the eight-level increase under U.S.S.G. § 2B1.1(b)(1)(E) was clear error. *See United States v. Fumo*, 655 F.3d 288, 310 (3d Cir. 2011); *see also United States v. Rodriguez*, --- F.3d ----, 2013 WL 5630962, at \*6 (11th Cir. Oct. 16, 2013) (Bowen, J., concurring) (“The Government’s cavalier disregard for the need of further evidence, specific references to a trial transcript, or another basis upon which the district court may make sustainable [sentencing] findings is all too typical.”).

**B. Alleged Costs AT&T Spent Notifying its Customers Is Not “Actual Loss” Under U.S.S.G. § 2B1.1.**

Section 2B1.1 applies to both counts of conviction. Under U.S.S.G. § 2B1.1(b), the offense level is increased depending on the amount of “actual” or “intended” loss at issue in the case. U.S.S.G. § 2B1.1 app. n. (3)(A). There are two definitions of “actual” loss relevant here. First, in general, “actual” loss is

defined as “the reasonably foreseeable pecuniary harm that resulted from the offense.” *Id.* at app. n. (3)(A)(i). This definition could apply to either count of conviction here. But the Guidelines also have a broader definition of “loss” specifically for CFAA convictions that would only apply to the conviction on count one for conspiracy to violate the CFAA. *Id.* at app. n. (3)(A)(v)(III).

The claimed mailing costs fail to meet either definition of “loss” under U.S.S.G. § 2B1.1 and thus the sentence must be reversed.

*1.     The Mailing Costs Were Not “Reasonably Foreseeable Pecuniary Harm” Under U.S.S.G. § 2B1.1.*

The government claims that even if notification costs are not “loss” for purposes of the CFAA, they would still qualify as loss for purposes of the identity theft conviction on count two of the superseding indictment. GB 101. “Loss” under this non-CFAA specific definition means “the reasonably foreseeable pecuniary harm that resulted from the offense.” U.S.S.G. § 2B1.1 app. n. (3)(A)(i). “Reasonably foreseeable pecuniary harm” means financial harm “that the defendant knew or, under the circumstances, reasonably should have known, was a potential result of the offense.” *Id.* at app.n. (3)(A)(iv). The government presents only one argument why the alleged mailing costs were a “reasonably foreseeable” loss: it claims many states require a company notify its customers of a security breach and thus Auernheimer should have reasonably known that AT&T would incur expenses to fulfill this obligation. GB 100.

But the government’s theory suffers from two major flaws. First, the government presented no evidence that AT&T was under a legal obligation to notify its customers. Although most states have breach notification laws, many do not include email addresses unconnected with a financial institution as the type of information that if disclosed, triggers a disclosure requirement. Most tellingly, one of those states is New Jersey, the state where the government charged Auernheimer and Spitler because of the presence of 4,500 “victims” there. *See* N.J. Stat. Ann. § 56:8-161; App2. 221.<sup>15</sup>

Second, even if the government proved AT&T had a legal obligation to notify, AT&T almost completely fulfilled that obligation with the email notice that reached 98% of affected customers. App2. 215, 228-29, 750. All the states involved in this case—Arkansas, California, Georgia, New Jersey and Texas—require a company to notify its customers of a data breach through *one* method of communication, and all permit *either* physical mailing or electronic notification. *See* Ark. Code Ann. § 4-110-105(e); Cal. Civ. Code §§ 1798.29(i), 1798.82(j); Ga. Code Ann. §§ 10-1-911(4), 10-1-912(a); N.J. Stat. Ann. § 56:8-163(d); Tex. Bus. & Com. Code Ann. § 521.053(e). Assuming Auernheimer should have reasonably

---

<sup>15</sup> Arkansas and California—the states where Auernheimer and Spitler were physically located – also did not include email addresses unconnected to a financial institution in their definitions of “personal information” that trigger disclosure requirements at the time Spitler accessed the email addresses. After the conviction, California changed its law to include all email addresses. *See* Ark. Code Ann. § 4-110-103(7); Cal. Civ. Code §§ 1798.29(g), 1798.82(h).

foreseen that AT&T was going to notify its customers of the breach, it was unforeseeable that AT&T would duplicate an effective notice by also sending a letter in the mail.

But in any event, the evidence at trial suggested AT&T chose to notify its customers because that was AT&T's "policy and practice," not because it had a legal obligation to do so. App2. 214. The government quotes some of the testimony of AT&T's Shirley Ramsey to show that AT&T considered the incident "very, very important" and explained how AT&T customers felt "frustrated," "scared" and "angry." GB 102 (quoting App2. 221). But the government omitted an important piece of Ms. Ramsey's testimony: her testimony that the incident was "harmful for our reputation." App2. 221. That omission is telling because the Guidelines specifically state "pecuniary harm does not include emotional distress, harm to reputation, or other non-economic harm." U.S.S.G. § 2B1.1 app. n. (3)(A)(iii).

In other words, in the absence of any actual proof of a legal requirement to notify its customers, AT&T's business decision to address its customer's "anger" with a duplicate physical mailing is not "reasonably foreseeable pecuniary harm" under the Guidelines. That means under both the CFAA count and the identity

theft count, the alleged mailing costs do not qualify as “loss” under U.S.S.G. § 2B1.1.<sup>16</sup>

2. *The Mailing Costs Were Not Loss Under the Broader Definition of “Loss” for CFAA Convictions.*

There is a second definition of “actual loss” in the Guidelines for CFAA convictions, which

... includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: Any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.

U.S.S.G. § 2B1.1 app. n. (3)(A)(v)(III). That definition of “loss” comes from the text of the CFAA, specifically 18 U.S.C. § 1030(e)(11), and so case law interpreting “loss” for the CFAA applies with equal force to determining loss under U.S.S.G. § 2B1.1. *See In re Cmty. Bank of N. Virginia*, 418 F.3d 277, 295-96 (3d Cir. 2005) (“When Congress borrows language from one statute and incorporates it into a second statute, the language of the two acts ordinarily should be interpreted the same way.”) (citing *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 383–84 (1992)).

---

<sup>16</sup> Even if the supposed mailing costs were deemed “reasonably foreseeable” for the 2% of customers who did not receive the email notification, “loss” would be approximately \$1,460, or 2% of the alleged \$73,000. That would trigger no increase in the offense level under U.S.S.G. § 2B1.1(b)(1)(A).

Auernheimer's opening brief explained the supposed mailing costs did not qualify as "loss" for purposes of the CFAA because they were "not related to computer impairment or computer damages" and thus "not compensable under the CFAA." *Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 382 (S.D.N.Y. 2005); *see also* AB 54-57. "Loss" under 18 U.S.C. § 1030(e)(11), and in turn U.S.S.G. § 2B1.1 in CFAA cases, is only intended to cover expenses spent to investigate and fix damage, or costs incurred "because the computer cannot function while or until repairs are made." *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004) *aff'd*, 166 Fed. App'x 559 (2d Cir. 2006) (citing *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 521-22 (S.D.N.Y. 2001)).

Here, there was no damage to AT&T computers and nothing to repair. No data was taken or destroyed and there was no interruption of service. The alleged mailing costs were not caused by the computer access – meaning money spent to fix a broken computer or restore service – but rather the disclosure of the email addresses. And as one court has held in a similar situation, costs associated with breach notification laws, assuming it was even implicated here, are not recoverable "loss" for purposes of the CFAA. *Farmers Ins. Exch. v. Auto Club Grp.*, 823 F. Supp. 2d 847, 855-56 (N.D. Ill. 2011). This is consistent with other cases finding ancillary costs unrelated to fixing or repairing a computer or restoring service do

not qualify as “loss” under the CFAA. *See, e.g., Nexans Wires S.A.*, 319 F. Supp. 2d at 476-78 (travel costs to conduct a damage assessment, lost business revenue and profits not “loss” for CFAA); *Wilson v. Moreau*, 440 F. Supp. 2d 81, 110 (D.R.I. 2006) (attorneys fees and litigation costs not “loss” under the CFAA).

The government makes no attempt to even engage with these cases. Instead, it simply asserts these cases only involve “loss” for the CFAA charge, but not the identity theft conviction. GB 101. But as explained above, the alleged mailing costs do not qualify as “loss” under the general definition in U.S.S.G. § 2B1.1 that applies to the identity theft conviction. And the supposed mailing costs similarly fail to meet the definition of “loss” under the CFAA specific definition of “loss.” As a result, the district court erred when it applied the eight level upward adjustment in U.S.S.G. § 2B1.1(b)(1)(E). As a result, the sentence must be reversed.

### **CONCLUSION**

For the reasons discussed above, Auernheimer respectfully requests this Court overturn his convictions and sentence.

Dated this 25th day of October, 2013

Respectfully submitted,

/s/ Hanni M. Fakhoury  
Hanni M. Fakhoury  
ELECTRONIC  
FRONTIER FOUNDATION  
815 Eddy Street  
San Francisco, CA 94109  
Tel.: (415) 436-9333

Orin S. Kerr  
2000 H Street, N.W.  
Washington, DC 20052  
Tel.: (202) 994-4775

Marcia C. Hofmann  
LAW OFFICE OF MARCIA C.  
HOFMANN  
25 Taylor Street  
San Francisco, CA 94102  
Tel.: (415) 830-6664

Tor B. Ekeland  
Mark H. Jaffe  
TOR EKELAND, P.C.  
155 Water Street  
Brooklyn, NY 11201  
Tel.: (718) 285-9343

*Counsel for Defendant-  
Appellant Andrew Auernheimer*



## CERTIFICATIONS

1. I certify that a virus check was performed on the PDF file of Appellant's Reply Brief using McAfee Security Scan Plus.

2. In accordance with 3rd Circuit LAR 46. 1(e), I, Hanni M. Fakhoury, certify that I am a member of the Bar of this Court.

3. I hereby certify that the electronically filed PDF and hard copies of the corrected brief filed on October 25, 2013 are identical.

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

a. This Appellant's Opening Brief does not comply with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 12,254 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). Appellant's Motion for Leave to File a Non-Compliant Brief was filed on October 14, 2013, and no ruling has been issued as of today's date; and

b. 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: October 25, 2013

By: /s/ Hanni Fakhoury  
Hanni M. Fakhoury

*Counsel for Defendant-  
Appellant Andrew Auernheimer*

## CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Third Circuit by using the appellate CM/ECF system on October 25, 2013.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: October 25, 2013

By: /s/ Hanni Fakhoury  
Hanni M. Fakhoury

*Counsel for Defendant-  
Appellant Andrew Auernheimer*