

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 AMENDED 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” 2

 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 12

II. IF AUERNHEIMER CONSPIRED TO VIOLATE THE CFAA, THE VIOLATION WAS ONLY A MISDEMEANOR 15

III. THE GOVERNMENT CANNOT DEFEND AUERNHEIMER’S CONVICTION ON COUNT 2 BASED ON A NEW THEORY OF LIABILITY NEVER PRESENTED TO THE JURY 16

IV. VENUE WAS IMPROPER IN NEW JERSEY ON BOTH COUNTS..... 17

 A. The “Substantial Contacts” Test Cannot Establish Venue Because It Is a Limitation on Venue and Not a Test to Establish Venue 18

| | | |
|----|--|----|
| 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 | 19 |
| C. | The Government Cannot Establish Venue for Count 1 Based on a Failure to Act in New Jersey..... | 23 |
| D. | Venue Was Not Established for Count 1 When an FBI Agent in New Jersey Read About the Alleged Offense Over the Internet..... | 24 |
| E. | Assuming Venue Was Proper for Count 1, Venue Was Improper for Count 2 | 27 |
| F. | Venue Is Not Subject to Harmless Error Review | 28 |
| V. | THE ALLEGED MAILING COSTS WERE NOT “LOSS” UNDER THE SENTENCING GUIDELINES | 29 |
| | CONCLUSION | 30 |

TABLE OF AUTHORITIES

Federal Cases

Bouie v. City of Columbia,
378 U.S. 347 (1964) 10

Chiarella v. United States,
445 U.S. 222 (1980) 2, 17

Cola v. Reardon,
787 F.2d 681 (1st Cir. 1986) 17

Dunn v. United States,
442 U.S. 100 (1979) 17

EF Cultural Travel BV v. Explorica, Inc.,
274 F.3d 577 (1st Cir. 2001) 8, 9, 11, 12

EF Cultural Travel BV v. Zefer Corp.,
318 F.3d 58 (1st Cir. 2003) *passim*

Giaccio v. Pennsylvania,
382 U.S. 399 (1966) 10

Travis v. United States,
364 U.S. 631 (1961) 26

United States v. Anderson,
328 U.S. 699 (1946) 23

United States v. Bin Laden,
146 F.Supp.2d 373 (S.D.N.Y. 2001) 25

United States v. Bowens,
224 F.3d 302 (4th Cir. 2000) 21, 23

United States v. Brennan,
183 F.3d 139 (2d Cir. 1999) 28

| | |
|--|--------|
| <i>United States v. Cabrales</i> , 524 U.S. 1 (1998)..... | 19 |
| <i>United States v. Cioni</i> , 649 F.3d 276 (4th Cir. 2011)..... | 15, 16 |
| <i>United States v. Clenney</i> , 434 F.3d 780 (5th Cir. 2005) (per curiam)..... | 22, 23 |
| <i>United States v. Coplan</i> , 703 F.3d 46 (2d Cir. 2012)..... | 21 |
| <i>United States v. Davis</i> , 689 F.3d 179 (2d Cir. 2012)..... | 18 |
| <i>United States v. Fumo</i> , 655 F.3d 288 (3d Cir. 2011)..... | 29 |
| <i>United States v. Goldberg</i> , 830 F.2d 459 (3d Cir. 1987)..... | 18 |
| <i>United States v. Hart-Williams</i> , 967 F. Supp. 73 (S.D.N.Y. 1997)..... | 28 |
| <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 |
| <i>United States v. Magassouba</i> , 619 F.3d 202 (2d Cir. 2010)..... | 27 |
| <i>United States v. Miller</i> , 527 F.3d 54 (3d Cir. 2008)..... | 16 |
| <i>United States v. Oceanpro Indus., Ltd.</i> , 674 F.3d 323 (4th Cir. 2012)..... | 21 |
| <i>United States v. Pendleton</i> , 658 F.3d 299 (3d Cir. 2011)..... | 18, 25 |

United States v. Ramirez,
420 F.3d 134 (2d Cir. 2005)..... 26

United States v. Reed,
773 F.2d 477 (2d Cir. 1985)..... 18

United States v. Rodriguez-Moreno,
526 U.S. 275 (1999) 19, 20, 22

United States v. Rowe,
414 F.3d 271 (2d Cir. 2005)..... 26

United States v. Royer,
549 F.3d 886 (2d Cir. 2008)..... 19

United States v. Saavedra,
223 F.3d 85 (2d Cir. 2000)..... 18, 19, 28

United States v. Salinas,
373 F.3d 161 (1st Cir. 2004) 25

United States v. Strain,
396 F.3d 689 (5th Cir. 2005)..... 21

United States v. Thomas,
74 F.3d 701 (6th Cir. 1996)..... 26

United States v. Walker,
529 Fed. App’x. 256 (3d Cir. 2013)..... 16

Verizon v. Main St. Dev., Inc.,
693 F. Supp. 2d 1265 (D. Or. 2010)..... 24

Federal Statutes

18 U.S.C. § 1030 *passim*

18 U.S.C. § 1204 22

18 U.S.C. § 2701 15

18 U.S.C. § 3237 25

State Statutes

N.J.S.A. § 2C:20-31 15

Federal Rules

Federal Rule of Criminal Procedure 29 16

U.S. Sentencing Guidelines

United States Sentencing Guideline § 2B1.1 29, 30

Other Authorities

Charles Alan Wright, *et al.*, *Federal Practice and Procedure* (4th ed. 2013) 24

Daniel B. Garrie, *The Legal Status of Software*, 23 J. Marshall J. Computer & Info. L. 711 (2011) 11

Default User-Agent (UA) String Changed, Microsoft 14

Understanding User-Agent Strings, Microsoft 14

Wayne R. LaFave, *Criminal Law* (4th ed. 2003) 24

Wayne R. LaFave, *et al.*, *Criminal Procedure* (3d ed. 2012) 19, 28

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 at 1. 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 offers five arguments for why Spitler and Auernheimer conspired to violate the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(C). 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 explained 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 responds that this court should defer to the jury's factual finding that the email addresses were protected and not publicly available. *See* Br. for Appellee ("GB") 27. The government's argument is meritless because the jury was not asked to decide whether the email addresses were unprotected or publicly

available. *See Chiarella v. United States*, 445 U.S. 222, 236 (1980) (“[W]e cannot affirm a criminal conviction on the basis of a theory not presented to the jury.”).

During pre-trial motions, the government persuaded the District Court that “access without authorization” in § 1030(a)(2) simply means access without permission. App1. 21-22.¹ 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. Because the jury was not asked to decide these questions, the Court cannot defer to the jury’s finding.

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. AB22. The government

¹ “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.

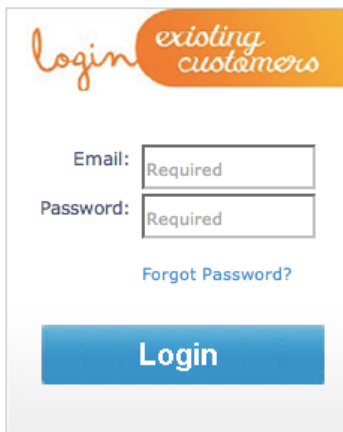
responds that the addresses were in fact protected by a kind of password. Relying on the definition of “passwords” found on the Internet website *Wikipedia*, the government contends that ICC-IDs are passwords because they are “shared secrets” between the user and the AT&T server. GB38-41.

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.” National Institute of Standards and Technology, *Electronic Authentication Guideline*, Information Security 12 (2011). Under this standard, from a source surely more authoritative than *Wikipedia*,² ICC-IDs are 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, which 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

² “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 written largely by amateurs” and is “easily vandalized,” leading many courts to reject its use. *Id.* (citing cases).

access an account. AT&T's website contained such a login prompt. App2. 252-53, 257. In its current form, it looks like this:³

A screenshot of a login form. At the top left, the word "login" is written in a cursive font. To its right, the words "existing customers" are written in a smaller, sans-serif font inside an orange rounded rectangle. Below this, there are two input fields: "Email:" followed by a box containing the word "Required", and "Password:" followed by a box containing the word "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 text.

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.

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>

³ Viewable at <https://dcp2.att.com/OEPNDClient/> (last visited Dec. 23, 2013).

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 *3502* (corresponding to recently-confirmed Judge Brian Davis).

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. GB24-26. 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.⁴ App2. 703-04.

Second, even assuming that impersonation violates the CFAA, no impersonation occurred here. To impersonate someone means to pretend to be that person.⁵ 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

⁴ "Impersonating" appeared in an instruction about New Jersey's computer crime statute, but not the CFAA. App2. 706.

⁵ See Merriam-Webster Online, <http://www.merriam-webster.com/dictionary/impersonate> (defining impersonate as "to pretend to be (another person)") (last visited Dec. 23, 2013).

anyone. It simply sent requests to a website. *Cf. United States v. Kane*, 450 F.2d 77, 85 (5th Cir. 1971) (officer who answered the defendant's phone was not "impersonating" defendant).

For the same reason, the government's claim that Spitler's program "tricked" AT&T's computer is wrong. GB42. 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. App2. 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 "computer expertise" was required to design it. GB30. The government envisions two kinds of Internet users: (1) "ordinary" users, such as "a typical judicial law clerk," and (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," GB35, 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. Spitler's program sent queries to AT&T's website that looked like this:

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

AB19; 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 here. Specifically, the district court enjoined use of the program because its 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 court 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 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 leads to prison. 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 forbids any criminal law “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,” GB35, 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 ordinary use is particularly uncertain because of how computer programs are developed. First, experts use effort and skill to create programs anyone can use. Second, ordinary

users operate the programs to perform the same steps as experts. *See* Daniel B. Garrie, *The Legal Status of Software*, 23 J. Marshall J. Computer & Info. L. 711, 713-23 (2011). Given this reality, courts cannot readily distinguish between expert and ordinary use.

The malleability of the government's standard is demonstrated by the government's 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, going into glorious and comprehensive technical detail about how Spitler designed and used the program. *See* GB5-10, 27-29.

In contrast, the government skips these steps when describing the facts of *Zefer*. The government's brief states that *Zefer* was hired, and then it jumps to the litigation that ensued after the program had been used. GB31-32. The government neglects to point out (much less elaborate on) how an insider gave *Zefer* proprietary information about the website's structure that was 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.⁶

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. GB20, 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. GB20, 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.

⁶ The government suggests that Spitler's program was illegal because it obtained information unavailable through a public search engine such as Google. GB27. 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.

An analogy based on physical trespass law explains why. Imagine 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 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 the moment he entered the store after putting on his shirt. The answer is obviously “no.” It is true that the clerk had 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, he complied with the policy and he was authorized to enter the store. 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 practices adopted by browser designers confirm this. For example, Microsoft sets the default user agent of its Internet Explorer browser 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.⁷ Microsoft does not consider itself or its users to be criminals engaging in deception by breaking into websites. User agents simply cannot act as access restrictions.

⁷ *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 Dec. 23, 2013).

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.S.A. § 2C:20-31(a), that contains a statutory element not found in 18 U.S.C. § 1030(a)(2)(C). GB52-55. The government misunderstands the law. The relevant legal question is whether the government has charged two different *acts*, not two different statutes.

The key precedent is *United States v. Cioni*, 649 F.3d 276, 278-79 (4th Cir. 2011), which rejected a felony enhancement using the unauthorized access statute found in 18 U.S.C. § 2701(a). 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 government charged and attempted to prove two crimes using the same conduct,” such that the same “facts or transactions” were used twice. *Id.* at 282-83.

The same reasoning applies here. N.J.S.A. § 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. The government is attempting to prove its case based on a single 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.

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

Contrary to the government's claim, the sufficiency of Count 2 must be reviewed *de novo*. GB63. “[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.” *United States v. Miller*, 527 F.3d 54, 62 (3d Cir. 2008). A nonspecific motion under Federal Rule of Criminal Procedure 29 preserves all sufficiency claims. *See United States v. Walker*, 529 Fed. App'x. 256, 260 (3d Cir. 2013) (unpublished). Auernheimer is challenging the sufficiency of the evidence under Count 2, and he filed a timely motion for acquittal under both Rules 29(a) and 29(c) on that count. *See App2*. 339, 729-31. His claim is therefore reviewed *de novo*.

On the merits, the government's defense of Count 2 fails because it is based on a theory of liability never presented to the jury. At trial, the government argued to the jury that Auernheimer violated Count 2 by possessing the email/ICC-ID

pairings and then transferring them to Gawker after violating the CFAA. App2. 598-99. On appeal, the government instead defends the sufficiency of Count 2 by switching to a new argument: that Auernheimer used the ICC-IDs when he entered them into Spitler's program before violating the CFAA. *See* GB64-65.

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 (citing *Dunn v. United States*, 442 U.S. 100, 106 (1979)). 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 cannot satisfy that standard. The government never argued its new theory to the jury nor provided the jury instructions needed to enable the jury to consider it. For that reason, the government's defense of Count 2 must fail.

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

Even if this Court concludes that Auernheimer was guilty of both offenses, 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 are persuasive.

A. The “Substantial Contacts” Test Cannot Establish Venue Because It Is a Limitation on Venue and Not a Test to Establish Venue.

The government first argues 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 views this test as “broader ” than the crucial elements test,⁸ and it argues that the substantial contacts test can establish venue even if no crucial elements of the offenses occurred in New Jersey. GB70-73

The government misunderstands the substantial contacts test. That 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) (“To comport with constitutional safeguards,” venue “require[s] more than ‘some activity in the situs district’; instead, there must be ‘substantial contacts’”) (quoting *Reed*, 773 F.2d at 481); *Goldberg*, 830 F.2d at 466 (describing the substantial contacts test as the test that “[t]he constitution requires”) (quoting *Reed*, 773 F.2d at 480).

It remains unclear whether this Circuit has adopted the substantial contacts test, as it was cited only in *Goldberg*. But where it has been adopted, establishing venue requires the government to satisfy *both* the statutory essential elements test

⁸ 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”).

and 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. Thus, a court cannot rely on the substantial contacts test to “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). As explained in more detail below, effects alone cannot establish venue.

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. GB75-77.

The government’s argument is incorrect. Under *United States v. Rodriguez-Moreno*, 526 U.S. 275 (1999), and *United States v. Cabrales*, 524 U.S. 1 (1998), the controlling distinction is between an “essential conduct element” that establishes venue and a “circumstance element” that does not. *Rodriguez-Moreno*, 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 a “circumstance

element” describes the circumstances that existed at the time of his act. *Rodriguez-Moreno*, 526 U.S. at 280 n.4. The felony enhancement cannot create venue in New Jersey under *Rodriguez-Moreno* and *Cabrales* because it is a circumstance element instead of 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), the part that states the maximum punishments for different offenses. Consider the language of the felony enhancement as a whole:

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. It does not describe the defendant’s prohibited act. Instead, it merely identifies various *circumstances* in which a CFAA violation can be punished as a felony instead of a misdemeanor. *Id.* The circumstances do not change the underlying act; they merely increase punishment on the basis of consequences of that act. Because they are not essential conduct elements, they cannot establish venue. *See United States v. Oceanpro Indus., Ltd.*, 674 F.3d 323,

329 (4th Cir. 2012) (noting that a statutory element that requires “proof of an antecedent crime” does not support venue); *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).

United States v. Bowens, 224 F.3d 302 (4th Cir. 2000), confirms the point. Bowens was charged with two counts of harboring a fugitive when there were a warrant out for the fugitive’s arrest. The arrest warrants had been issued in Virginia, and Bowens harbored the two fugitives in South Carolina. *Id.* at 305-07. *Bowens* held that venue was improper in Virginia even though the predicate offense arose from Virginia. Although “issuance of a federal arrest warrant” in Virginia was “an essential element” of the crime, venue was improper in Virginia because venue was “limited to the place where the essential conduct elements occur.” *Id.* at 309. 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 create

venue in Virginia, so the government's claim that the conduct violated New Jersey law cannot create venue in New Jersey.

United States v. Clenney, 434 F.3d 780 (5th Cir. 2005) (per curiam), is also on point. Clenney lived in the Southern District of Texas, and had fathered a child who lived with his mother in the Northern District of Texas. *Id.* 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 Clenney 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. Establishing intent was merely a circumstance that existed when Clenney acted, not the act itself. *Id.* at 782. As a result, intent was "plainly not an essential conduct element as required by *Rodriguez-Moreno*" and could not establish venue. *Id.* 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 effects 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 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. GB80. 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 stop a criminal act establishes venue wherever failure to stop the crime occurs. "[V]enue is limited to the place 'where the criminal act is done.'" *Bowens*, 224 F.3d at 309 (quoting *United States v. Anderson*, 328 U.S. 699, 705 (1946)). There is no precedent for the government's claim that venue additionally lies in every district where a hypothetical act could have occurred that would have prevented the offense.

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." GB80 (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.⁹

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 claims that venue was proper for Count 1 because an FBI agent in New Jersey read about the alleged crime over the Internet. GB84-89. The government's theory appears to be that the crime of Count 1 continued for a long

⁹ Venue is improper in New Jersey even accepting the government's novel "failure to act" theory. As with all trespass statutes, the right to control authorization belongs to the property owner, not its customers. *See, e.g., Verizon v. Main St. Dev., Inc.*, 693 F. Supp. 2d 1265, 1278 (D. Or. 2010). As a result, it is the location of AT&T, not its users that would matter. Even if customers could permit access, any failure to obtain permission occurs where the defendant resides, not where the customer resides.

time after the actual elements of the crime were satisfied. In the government's view, *Gawker's* subsequent reporting about the crime and the FBI agent's subsequent investigation of the crime from inside New Jersey are actually all part of the crime itself. Because the agent was in New Jersey when he was surfing the web and reader the *Gawker* story, the crime was committed in part in New Jersey and venue is proper there. *Id.* at 84-86.

The government is wrong. 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. What happened *afterwards* was not part of the offense and cannot establish venue. The

offense did not continue into New Jersey simply because the FBI agent who 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. Otherwise, investigators could establish venue over every newsworthy offense in any district simply by reading about the offense from that district. *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.”); *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 support venue here. GB84. 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 obscenity lies in any district in which

the material moves). That has no relevance here, however, as the crime charged in Count 1 was not a distribution offense.

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. GB94-95. 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)).

This argument fails on its own terms by ignoring the indictment. The government did not charge Count 1 as the underlying predicate 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. 16. 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 for the reasons explained in Auernheimer's opening brief. *See* AB49.

F. Venue Is Not Subject to Harmless Error Review.

The government concludes with the assertion that any venue error was harmless. GB97-98. This argument fails because venue is not subject to harmless error review. *See* 4 LaFave, *et al.*, *Criminal Procedure*, at §16.1(g) (“Failure of venue will not be treated as harmless error.”).

Notably, the government points to no Third Circuit case applying harmless error review to venue defects. Instead, the government relies on a district court case from another circuit. *See* GB98 (citing *United States v. Hart-Williams*, 967 F. Supp. 73, 78-81 (S.D.N.Y. 1997)). That decision is no longer good law even in its own circuit, however. *See United States v. Brennan*, 183 F.3d 139, 149 (2d Cir. 1999); *Saavedra*, 223 F.3d at 100 n.5 (Cabrane, J., dissenting) (“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 error here was not harmless. Auernheimer was hauled from Arkansas to New Jersey to face charges in a district far from home that he had never even visited. This is not a case where the defendant merely “was tried on the wrong side of the Brooklyn Bridge.” *Hart-Williams*, 967 F. Supp. at 78.

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

The government argues that plain error review should apply because Auernheimer failed to object to the loss amount. GB104. The government is wrong: Auernheimer objected to the loss amount both in his sentencing papers and at the sentencing hearing. *See 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. The sole evidence of loss mentioned in the government’s brief is a sentence in the criminal complaint, filed more than two years before the sentencing, which stated “AT&T has spent approximately \$73,000 in remedying the data breach.” *Id.* at 58. But there is no actual evidence rather than conjecture to support this claim, and thus the government’s failure to make a “prima facie case of the loss amount” makes the eight-level increase under United States Sentencing Guideline (“U.S.S.G.”) § 2B1.1(b)(1)(E) clear error. *See United States v. Fumo*, 655 F.3d 288, 310 (3d Cir. 2011).

The government claims that even if notification costs were not “loss” for purposes of Count 1, they would still qualify as loss for Count 2 because many states require breach notification. GB100-01. However, the government presented no evidence at sentencing that AT&T was obligated to notify its customers. Evidence at trial suggested that AT&T chose to notify its customers because it was

AT&T's "policy and practice," not because of a legal obligation. App2. 214. Although most states have breach notification laws, many (including New Jersey) do not include email addresses unconnected with a financial institution as the type of information that, if disclosed, triggers a disclosure requirement. *See* AB58.

Further, AT&T almost completely fulfilled any legal obligation with the email notice that reached 98% of affected customers. App2. 215, 228-29, 750. To the extent that AT&T sent the notification to assuage customer anxiety and to protect the company's reputation, App2. 221, the Guidelines specifically state that "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).

CONCLUSION

Auernheimer respectfully asks this Court to overturn his convictions and sentence.

Dated this 24th Day of December, 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 December 24, 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 6,963 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); 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: December 24, 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 December 24, 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: December 24, 2013

By: /s/ Hanni Fakhoury
Hanni M. Fakhoury

*Counsel for Defendant-
Appellant Andrew Auernheimer*