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 OPENING 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

Attorneys for Defendant-Appellant Andrew Auernheimer

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

Statutes

New Jersey Statutes

Other State Statutes

Rules

Treatises

Legislative Materials

Law Review Articles

Other Authorities

STATEMENT REGARDING ORAL ARGUMENT

This case raises five novel issues of law that are matters of first impression in this Circuit. Appellant Andrew Auernheimer (pronounced "OUR-en-heim-er") believes oral argument will be helpful to assist the Court in resolving the complex issues raised by this appeal. For that reason, he requests oral argument in this case.

STATEMENT OF JURISDICTION

Auernheimer was convicted and sentenced of federal crimes in the United States District Court for the District of New Jersey. The district court had jurisdiction under 18 U.S.C. § 3231 and this Court has jurisdiction under 28 U.S.C. §§ 1291 and 1294(1). The district court entered final judgment on March 19, 2013, and the notice of appeal was timely filed on March 21, 2013. DCR 91-93, App.1 1, 30-36.[1] Auernheimer is currently serving a forty-one-month prison sentence at Allenwood Low Federal Correctional Institute. According to the Bureau of Prison's website, his projected release date is January 26, 2016.[2]

ISSUES PRESENTED FOR REVIEW

This is an appeal from a remarkable and unprecedented criminal conviction. The government charged Auernheimer with felony computer hacking under the Computer Fraud and Abuse Act ("CFAA") for visiting an unprotected AT&T

[1] "DCR" refers to the district court record. "App1." refers to Volume 1 of the Appendix attached to the end of this brief. "App2." refers to Volume 2 of the Appendix, filed separately in connection with this opening brief.

[2] *See* Federal Bureau of Prisons Inmate Locator, http://www.bop.gov/iloc2/LocateInmate.jsp(last visited June 27, 2013).

website and collecting e-mail addresses that AT&T had posted on the World Wide Web. The government also charged Auernheimer with identity theft for sharing those addresses with a reporter. This prosecution was brought in New Jersey even though neither Auernheimer, his alleged co-conspirator Daniel Spitler, nor any computer or communications were actually located in or passed through New Jersey. Finally, Auernheimer was sentenced to a forty-one-month prison term based in large part on AT&T's decision to spend approximately $73,000 to supplement e-mail notification to customers with a postal letter informing them that their privacy was not breached.

This case raises five legal issues:

1. Did Auernheimer and Spitler access a computer "without authorization" under 18 U.S.C. § 1030(a)(2)(C)?

Where Issue Was Raised: Auernheimer challenged the sufficiency of the superseding indictment pre-trial and moved for acquittal under Federal Rule of Criminal Procedure Rule 29 both at the close of the government's case and after the jury's verdict. DCR 51, 88, App2. 66-70, 339, 729-31.

Standard of Review: Sufficiency of evidence claims are reviewed *de novo*. *United States v. Pavulak*, 700 F.3d 651, 668 (3d Cir. 2012). The Court must decide whether the evidence, viewed in the light most favorable to the government,

"make[s] a strong enough case to let a jury find [the defendant] guilty beyond a reasonable doubt." *Id.* (citation omitted).

2. If Auernheimer was properly convicted of a conspiracy to violate the CFAA, was that conspiracy a misdemeanor or a felony?

Where Issue Was Raised: Auernheimer challenged whether he was properly charged with a felony pre-trial and moved for acquittal under Rule 29 both at the close of the government's case and after the jury's verdict. DCR 51, 88, App2. 70-75, 339, 729-31.

Standard of Review: Sufficiency of evidence claims are reviewed *de novo* with the Court deciding whether the evidence, viewed in the light most favorable to the government, shows that the defendant is guilty beyond a reasonable doubt. *Pavulak*, 700 F.3d at 668.

3. Did Auernheimer violate the identity theft statute, 18 U.S.C. § 1028(a)(7)?

Where Issue Was Raised: Auernheimer moved for acquittal under Rule 29 both at the close of the government's case and after the jury verdict. DCR 51, 88, App2. 339, 729-31.

Standard of Review: Sufficiency of evidence claims are reviewed *de novo* with the Court deciding whether the evidence, viewed in the light most favorable

to the government, shows that the defendant is guilty beyond a reasonable doubt. *Pavulak*, 700 F.3d at 668.

4. Was venue proper in the District of New Jersey?

Where Issue Was Raised: Auernheimer challenged venue before trial and requested a jury finding on venue that was denied by the district court. DCR 51, App2. 75-77, 574-78, 586-91.

Standard of Review: Whether venue is proper raises a question of law for which this Court exercises plenary review. *United States v. Baxter*, 884 F.2d 734, 736 (3d Cir. 1989).

5. Do AT&T's costs in mailing a letter to its customers support an eight-level upward adjustment under the United States Sentencing Guidelines?

Where Issue Was Raised: Auernheimer objected to the eight-level adjustment in both his written objections to the presentence report and during the sentencing hearing. DCR 90, App.2 748-50, 762-63.

Standard of Review: This Court reviews legal conclusions regarding the United States Sentencing Guidelines ("U.S.S.G.") *de novo*. *United States v. Blackmon*, 557 F.3d 113, 118 (3d Cir. 2009). Factual findings during sentencing, including loss calculations under U.S.S.G. § 2B1.1, are reviewed for clear error. *United States v. Dullum*, 560 F.3d 133, 137 (3d Cir. 2009).

RELATED CASES AND PROCEEDINGS

Daniel Spitler was charged in a separate criminal case in the district of New Jersey. *See United States v. Spitler*, 2:11-cr-00429-SDW-1 (D.N.J. 2011). On June 23, 2011, he pleaded guilty to a two-count information pursuant to a plea agreement. *See Spitler*, 2:11-cr-00429-SDW-1 Doc. No. 29. As of the filing of this brief, he has not yet been sentenced.

STATEMENT OF THE CASE

A sealed complaint was filed against Auernheimer and Spitler on January 13, 2011. On July 6, 2011, Auernheimer was indicted on charges of conspiracy to access a computer without authorization (in violation of 18 U.S.C. §§ 371 and 1030(a)(2)(C)) ("Count 1") and fraud in connection with personal identification (in violation of 18 U.S.C. § 1028(a)(7)) ("Count 2)."[3] DCR 1, 26, App2. 45-58. A superseding indictment was filed on August 16, 2012. DCR 46, App1. 2-17. To enhance the first charge from a misdemeanor to a felony, the government alleged the conduct was in furtherance of New Jersey's computer crime statute, New Jersey Stat. Ann. ("N.J.S.A.") § 2C:20-31(a). App1. 6.

Auernheimer filed a motion to dismiss the charges on September 21, 2012. DCR 51, App2. 59-81. He argued the CFAA charges were unconstitutionally vague because the term "without authorization" in § 1030(a)(2)(C) was undefined

[3] All further statutory references are to Title 18 of the United States Code unless otherwise noted.

and AT&T's website was publicly accessible; that he was improperly charged with a felony instead of a misdemeanor because the conduct underlying the CFAA charge was also the basis of the New Jersey state crime; and that venue was improper in New Jersey. DCR 51, App2. 66-80.

The district court held a motion and evidentiary hearing on October 25 and 26, 2012, but denied the motion in a written opinion issued after the hearing. DCR 63-65, 86-87, App1. 18-29. The court ruled the CFAA charges were not vague, and that the government sufficiently alleged Spitler and Auernheimer were not authorized to access the AT&T servers. App1. 7-8, 14, 21-22. It also found the felony CFAA charge was proper because the state crime required proof of an extra element missing from the CFAA. App1. 24-25. Finally, it concluded that venue was proper in New Jersey because Auernheimer's crime was "completed" in New Jersey when he disclosed the "personal identifying information" of state residents. App1. 26.

Auernheimer's jury trial began November 13, 2012, and lasted five days. DCR 70-72, 78-79, App. 130-714. At the close of the government's case, Auernheimer moved for a judgment of acquittal under Rule 29 of the Federal Rules of Criminal Procedure on all counts, which the district court denied. App2. 339-40. On November 20, 2012, Auernheimer was convicted on both counts of the

superseding indictment. DCR 79, 85, App2. 673, 728. Auernheimer renewed his motion for acquittal on December 3, 2012. DCR 88, App2. 729-31.

On March 19, 2013, the district court denied Auernheimer's motion for a new trial. App2. 761. The court sentenced him to forty-one months imprisonment followed by three years of supervised release on each count to run concurrently. DCR 91-92, App1. 31-33, App2. 785. The court also ordered him to pay $73,167.00 in restitution to AT&T. DCR 91-92, App1. 36, App2. 786.

STATEMENT OF FACTS

A. AT&T and the iPad.

In January 2010, Apple Computer introduced the iPad portable tablet computer. The iPad allowed users to connect to the Internet through either a wireless internet connection, commonly known as "wifi," or through a cellular connection, commonly referred to at the time as "3G" service. App2. 216. The telecommunications company AT&T established an exclusive contract with Apple to provide 3G access to iPad users.[4]

AT&T created a website to allow its customers to access their AT&T accounts using the combination of an e-mail address and a password. App2. 217. The AT&T website was available at the Internet address *https://dcp2.att.com*, and

[4] *See generally* Serenity Caldwell, *AT&T Releases More Details on 3G IPad Plans*, PC World (Apr. 29, 2010), http://www.pcworld.com/article/195253/article.html.

it contained a login prompt that appeared whenever a user visited the website. App2. 252-53, 257.[5] When iPad users registered with AT&T and created an account, they also provided AT&T with an e-mail address. App2. 216-17. AT&T registered each iPad using a serial number found on the part of the iPad used to send and receive communications. App2. 153. The serial numbers were known as "integrated circuit card identifiers," or ICC-IDs. App2. 217. Each ICC-ID is a nineteen or twenty digit number. App2. 149-151, 481.

To make it easier for iPad owners to access their AT&T accounts, AT&T programmed its website to automatically pre-populate the login prompt with the e-mail address associated with that particular iPad computer. App2. 217. From the user's perspective, an iPad owner with an AT&T account who visited the website found that the "e-mail" part of the login prompt was automatically filled in with the user's e-mail address. *Id.* This feature was designed to save users time. App. 218, 258-59. Because the e-mail address would appear automatically, the user only needed to manually enter in his password to log in to the AT&T website. App2. 217.

AT&T implemented this feature by directing the iPad to a specific Internet address. When an iPad user with an ICC-ID visited the AT&T website, it would

[5] The login prompt is presently viewable at https://dcp2.att.com/OEPNDClient/ (last visited July 1, 2013).

automatically be directed to the following website, with "X" standing for the specific ICC-ID number:

https://dcp2.att.com/OEPClient/openPage?ICCID=X&IMEI=0

App2. 726. When any computer using the correct browser setting visited that particular webpage, the AT&T website would return the e-mail address associated with that specific ICC-ID number. App2. 217. iPads registered with AT&T would visit the page associated with that address automatically. App2. 255-56. However, AT&T configured its website so that it would share an e-mail address with anyone—not just the account holder—who entered the correct website address. App2. 409, 412-13.

B. Spitler Discovers the E-mail Addresses Were Available on the Internet.

Auernheimer's co-defendant, Daniel Spitler, identified this feature when he attempted to sign up for service with AT&T using a network card he had purchased from AT&T. App2. 251. After studying the iPad operating system, Spitler realized the AT&T website was configured to include a space in the Internet address for ICC-IDs. App2. 258. When Spitler entered his own ICC-ID number in that space, he was surprised to see that the AT&T login page already had his e-mail address filled out. App2. 257.

Curious about how AT&T's website could return his e-mail address, Spitler changed the ICC-ID number of the website by one digit and the website "pre-

populated" the login page with a different e-mail address. App2. 258. Spitler realized that AT&T had stored the e-mail addresses associated with different iPads on AT&T's servers. App2. 258. He concluded that he could collect many e-mail addresses using an automated computer program that he called the "account slurper." App2. 259-61, 726-27.

Spitler configured his program so it would visit the AT&T website many times using web addresses with different ICC-ID numbers. App2. 260. When the website address contained an ICC-ID number that matched that of a registered iPad user, AT&T's website would send back that user's e-mail address. App2. 258, 515.

Spitler shared his discovery with Auernheimer, who helped Spitler brainstorm ways to improve the program. App2. 260. Ultimately, the program collected approximately 114,000 e-mail addresses before AT&T discovered its customers' e-mail addresses were public. App2. 189, 283. AT&T quickly disabled the feature that pre-populated a customer's e-mail address. App2. 259-60, 459.

During this time, Spitler was located in San Francisco, California. App2. 233. Auernheimer was in Fayetteville, Arkansas. App2. 366. The evidence suggested that AT&T's computers that hosted its website were located in Dallas, Texas and Atlanta, Georgia. App2. 436.

C. Auernheimer's Disclosure to *Gawker*.

In an effort to draw attention to the computer skills of both Spitler and himself, Auernheimer contacted various media members and reporters to persuade them to write about how the e-mails were collected. App2. 272. One of those reporters was Ryan Tate of the online publication *Gawker*. App2. 150, 349. Auernheimer explained to Tate how the e-mail addresses had been collected. App2. 273. To confirm the collection, he shared the list of e-mail addresses with Tate. App2. 211, 285.

On June 9, 2010, *Gawker* ran a story written by Tate titled "Apple's Worst Security Breach: 114,000 iPad Owners Exposed." App2. 150, 721-24.[6] The story included a thorough discussion of how the e-mail addresses were collected, and it credited Spitler and Auernheimer with their collection. The popular website *Drudge Report* prominently linked to the story. App2. 162, 717.

D. The Trial.

Trial began on November 13, 2012, and ran until November 20, 2012. The government called four witnesses. The government's first witness, Special FBI Agent Phillip Frigm, testified about his investigation of the case and the FBI raid of Auernheimer's Arkansas residence on June 15, 2010. App2. 148-212. The next witness, Sherry Ramsey, an Assistant Vice President of Public Policy at AT&T,

[6] The *Gawker* article is accessible at http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed (last visited July 1, 2013).

testified about how the company responded to the public disclosure that AT&T's publicly accessible iPad servers published e-mail addresses without requiring a password. App2. 213-33.

Daniel Spitler next testified on the government's behalf pursuant to a guilty plea. Spitler testified about his discovery that AT&T's publicly accessible servers published e-mail addresses without requiring a password, and how this led him to write a program to obtain e-mail addresses. He also testified about telling Auernheimer about his program and how Auernheimer went public with the information. App2. 234-319. Finally, Stacey Halota, Vice President of Information Security and Privacy for the Washington Post Company, testified about the Post's discovery and reaction to Spitler and Auernheimer's actions. App2. 320-31.

The defense called five witnesses. Auernheimer testified first, and he explained how he learned about Spitler's program from Spitler. Auernheimer also testified about how he went to the press with the story. App2. 341-403. Dr. Edward Amoroso, Chief Security Officer at AT&T, testified that AT&T's iPad servers were publicly accessible to anyone with an Internet connection and that the e-mail addresses were not password-protected. App2. 404-16. After Amoroso, Timothy Glantz, Senior Investigator and lead analyst with AT&T, testified about

the case notes he collected from others at AT&T regarding Spitler's program accessing AT&T's servers. App2. 429-47.

R. David Hulsey followed Glantz. Hulsey testified about his involvement in AT&T's investigation and how AT&T's iPad servers were accessible to anyone with an Internet connection and that they responded to Spitler's program exactly like they were programmed to. App2. 447-83. Finally, Professor Sergey Bratus of Dartmouth College testified as an expert in computer research and security on the functioning of Spitler's program and security norms on the Internet. App2. 492-542.

On November 20, 2012, the jury returned a verdict of guilty on both counts of the superseding indictment. DCR 79, 85, App2. 673, 728.

G. The Sentencing.

The presentence report ("PSR") determined the adjusted offense level was 20, based largely on an eight level upward adjustment under U.S.S.G. § 2B1.1(b)(1)(E) because Auernheimer caused "loss" between $70,000 and $120,000.[7] The probation office reached out to AT&T for comment and submitted an affidavit form for it to declare any losses or submit a statement pursuant to the Mandatory Victim Restitution Act. PSR at 18, ¶ 52. AT&T submitted nothing. *Id.*

[7] Four copies of the presentence report were filed with this Court under seal as required by 3d Cir. L.A.R. 30.3(c) (2008).

The government also submitted a sentencing letter that agreed with the PSR's guideline calculations and urged the Court to impose a sentence within that range. DCR 89, App2. 732-45. Although the government itself believed "AT&T customers suffered no financial losses," PSR at 19, ¶ 58, and the only loss AT&T's Shirley Ramsey testified about at trial was to AT&T's "reputation," the government claimed AT&T spent $73,167 notifying its customers of the incident. However, the government provided no evidence at trial or sentencing to support its claim. App2. 221, 734. Instead, the government instead focused the court's attention on Auernheimer's previous comments and "trolling" activity. App2. 739-42.

Auernheimer objected to the eight-level upward adjustment on account of "loss." Doc. 90, App2. 748-50, 762-63. The district court overruled the objections, finding the eight-level increase appropriate because

> [W]ithout question, it is reasonably foreseeable that the costs that were incurred would be incurred as it relates to trying to rectify or resolve what occurred after the crime occurred by Mr. Auernheimer. So the eight-level increase in the amount of— basically because it was $73,000, plus as a loss to AT&T was in fact a reasonably foreseeable loss. In addition to that, there certainly was a link to the criminal activity and the actual need to notify the iPad users. In addition to that, to say that it was unnecessary or redundant, I don't think it's unreasonable. I don't think it's an aberrant cost, and I do think that it is appropriate.

App2. 770-71. The court adopted the PSR and the government's sentencing recommendations and found the adjusted offense level was 20. Because

Auernheimer was in criminal history category I, the sentencing range was between 33 and 41 months. App2. 782. The court sentenced Auernheimer to 41 months in prison on each count to run concurrently. App2. 785. The court also ordered Auernheimer to pay restitution to AT&T in the amount of $73,167. App2. 786.

SUMMARY OF ARGUMENT

Auernheimer's convictions must be overturned on multiple and independent grounds. First, Auernheimer's conviction on Count 1 must be overturned because visiting a publicly available website is not unauthorized access under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C). AT&T chose not to employ passwords or any other protective measures to control access to the e-mail addresses of its customers. It is irrelevant that AT&T subjectively wished that outsiders would not stumble across the data or that Auernheimer hyperbolically characterized the access as a "theft." The company configured its servers to make the information available to everyone and thereby authorized the general public to view the information. Accessing the e-mail addresses through AT&T's public website was authorized under the CFAA and therefore was not a crime. *See Pulte Homes, Inc. v. Laborers' Intern. Union of North America*, 648 F.3d 295, 304 (6th Cir. 2011).

Second, should the Court find that Auernheimer is guilty of conspiracy to violate the CFAA under Count 1, the Court must vacate the felony conviction

because the offense was at most a misdemeanor. The government charged Auernheimer with a felony on the novel ground that accessing a computer without authorization under the *federal* computer crime law is a felony because it is in furtherance of an analogous *state* computer crime law, N.J.S.A. § 2C:20-31(a). The felony enhancement was improper for two reasons. First, it constitutes double-counting: the government cannot charge a defendant with committing a crime in furtherance of the crime itself. *See United States v. Cioni*, 649 F.3d 276, 283 (4th Cir. 2011), *cert. denied,* 132 S. Ct. 437 (2011). Second, Auernheimer did not violate the New Jersey computer crime law.

Third, the conviction on Count 2 must be overturned because Auernheimer did not violate the identity theft statute, 18 U.S.C. § 1028(a)(7). Auernheimer's actions were lawful for two reasons. First, the collection of e-mail addresses from a publicly accessible website does not run afoul of § 1030(a)(2)(C), so there was no predicate offense on which to anchor a § 1028(a)(7) violation. Second, even assuming that Auernheimer violated § 1030(a)(2)(C) to obtain the e-mail addresses, he did not "possess" or "transfer" them "in connection with" another distinct and separate crime, as both the plain text and legislative history of § 1028 require.

Fourth, the convictions must be vacated because venue was improper in the District of New Jersey. Venue requires a close study of the laws under which a

defendant is charged to determine the essential elements of the conduct Congress prohibited. Venue is improper under Count 1 because no computer was accessed nor information obtained in New Jersey. Venue is improper under Count 2 because no data was transferred, possessed, or used in New Jersey. This case has nothing to do with New Jersey and should not have been charged in New Jersey.

Finally, if the Court upholds the convictions on Count 1 and Count 2, the sentence must be vacated and the case remanded for resentencing because the district court improperly applied an eight-level upward adjustment under U.S.S.G. § 2B1.1. The district court applied this enhancement to account for AT&T's alleged $73,000 mailing cost to notify its affected customers. This upward adjustment was wrongly imposed for three reasons. First, the government failed to carry its burden of proof that AT&T suffered this loss. Second, mailing costs are not the type of "loss" envisioned by the CFAA. And third, the $73,000 amount was unreasonable given the absence of a legal obligation to notify its customers of the breach and the otherwise adequate email notice sent to almost all of AT&T's affected customers.

These errors require the convictions to be overturned and the sentence to be reversed.

ARGUMENT

I. AUERNHEIMER DID NOT VIOLATE THE CFAA BECAUSE VISITING AN UNPROTECTED PUBLIC WEBPAGE IS NOT UNAUTHORIZED ACCESS.

Count 1 charged a conspiracy under 18 U.S.C. § 371 to violate 18 U.S.C. § 1030(a)(2)(C). Section 1030(a)(2)(C) punishes:

> Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.

Section 1030(a)(2)(C) is part of the CFAA, a computer trespass statute that prohibits breaking into a computer much like physical trespass laws prohibit breaking into a home. *See* S. Rep. No. 99–432, at 7-12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484-90. The first issue in this case is whether visiting AT&T's website constitutes illegally breaking in to a computer: that is, whether it constitutes access "without authorization" or conduct that "exceed[ed] authorized access." 18 U.S.C. § 1030(a)(2)(C). The CFAA conviction must be overturned because the answer is no. Because the conduct was not criminal, an agreement to engage in the conduct could not be a criminal conspiracy. *See United States v. Rigas*, 605 F.3d 194, 206 n. 9 (3d Cir. 2010) (en banc).

A. Visiting AT&T's Website Was "Authorized" Under the CFAA Because AT&T's Webpages Were Unprotected and Openly Available to the Public.

This case involves the World Wide Web, a publishing platform that makes information available to the public on the Internet.[8] *See Reno v. ACLU*, 521 U.S. 844, 852 (1997). Computer users access the World Wide Web using software programs called "browsers." Popular browsers include Google Chrome, Internet Explorer, and Mozilla Firefox. When a company publishes content on the World Wide Web, anyone with an Internet connection can enter the Internet address into a browser and access the website that has published the contents.

The fundamental question in this case is whether it is a crime to visit a public website. AT&T published the e-mail addresses of its customers on a public website available at *https://dcp2.att.com*. App2. 252-53, 257, 726. AT&T programmed its website to return the e-mail addresses of users when anyone visited the correct webpage at AT&T's website. Here are a few sample website addresses visited by Spitler's program:

> *https://dcp2.att.com/OEPClient/openPage?ICCID=89014104243221019785&IMEI=0*
>
> *https://dcp2.att.com/OEPClient/openPage?ICCID=89014104243221810258&IMEI=0*

[8] For a short video introduction to how the Internet works, see *How the Internet Works in 5 Minutes*, http://www.youtube.com/watch?v=7_LPdttKXPc (last visited July 1, 2013).

https://dcp2.att.com/OEPClient/openPage?ICCID=89014104243219907967&IMEI=0

App2. 725-27.[9]

The conviction under Count 1 must be overturned because visiting these and other similar website addresses was authorized under the CFAA. Websites are open and available to the public. By publishing information on the World Wide Web, a website owner inherently authorizes others to view that information. App2. 500. A company that "places information on the information superhighway clearly subjects said information to being accessed by every conceivable interested party" unless "protective measures or devices that would have controlled access" are put in place. *United States v. Gines-Peres*, 214 F. Supp. 2d 205, 225 (D.P.R. 2002).

AT&T chose not to employ protective measures to control access to the e-mail addresses of its customers. Instead, AT&T made those e-mail addresses available to everyone without a password to make it "easier" for its customers. App2. 217. Because AT&T chose to make the information available to the public, visiting the AT&T website to collect the e-mail addresses was authorized and legal.

Pulte Homes, Inc. v. Laborers' International Union of North America, 648 F.3d 295 (6th Cir. 2011), is directly on point. The LIUNA union was engaged in a

[9] These addresses can be deduced from Spitler's explanation of how the program worked, combined with the list of ICC-ID numbers he collected. *See* App2. 263.

bitter employment dispute with builder Pulte Homes. 648 F.3d at 298. LIUNA representatives attacked the builder's computers and telephone system by "bombard[ing] Pulte's sales offices and three of its executives with thousands of phone calls and e-mails." *Id.* at 299. LIUNA's "phone and e-mail blitz" overloaded the computer's capacity and caused "havoc" by clogging access to the network. *Id*. Pulte then sued LIUNA under the CFAA, alleging that LIUNA's campaign had accessed Pulte's computers without authorization. *Id.*

The Sixth Circuit rejected the claim on the ground that LIUNA's access of the builder's telephone and e-mail systems was authorized. *Id*. at 304. To be sure, Pulte did not want the union to "bombard" its computers and wreak "havoc" on them. But LIUNA had only targeted computer systems that Pulte made available to the public. Because Pulte had configured its computers in a way that anyone could access them, LIUNA's access was inherently authorized:

> LIUNA used unprotected public communications systems, which defeats Pulte's allegation that LIUNA accessed its computers "without authorization." Pulte allows all members of the public to contact its offices and executives: it does not allege, for example, that LIUNA, or anyone else, needs a password or code to call or e-mail its business. Rather, like an unprotected website, Pulte's phone and e-mail systems were open to the public, so LIUNA was authorized to use them.

Id. at 304 (internal quotations and citations omitted).

The principle underlying *Pulte Homes* controls this case. AT&T's website was "an unprotected website" that was "open to the public, so [anyone] was

authorized to use" it. *Id*. As in *Pulte Homes*, the computer owner in this case did not approve of how someone else used its computers. But *Pulte Homes* recognizes that the owner's configuration of the computer, not its wishes as to how the computer will be used, is what determines "authorization" under the CFAA. Visiting a public website is inherently authorized, much like sending e-mails and making phone calls in *Pulte Homes*. *See also Cvent v. Eventbrite, Inc*., 739 F. Supp. 2d 927, 933-34 (E.D.Va. 2011) (holding competitor's use of a scraper to query a company's website was authorized access under the CFAA because "the entire world was given unimpeded access to [the] website").

It would be different if AT&T had protected its data with a password. Guessing someone else's password to gain access to another person's private account without permission constitutes a criminal act of access without authorization. *See United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (concluding that releasing an Internet "worm" that guessed passwords and gained access to private accounts was an access without authorization); *United States v. Phillips,* 477 F.3d 215, 220 (5th Cir. 2007) (holding that use of program that guesses passwords and then enters password-protected area of a website is an unauthorized access);[10] *Cioni*, 649 F.3d at 280, 284 (holding that unauthorized

[10] *Phillips* assumes that a user who visits a webpage with a login-prompt has not "accessed" the computer by simply visiting the webpage and seeing the prompt. Under the Fifth Circuit's approach, the "access" occurs only when the

access occurred when defendant accessed the e-mail accounts of others and "[a]ll of the accounts were password protected").

Similarly, when a person obtains permission to use someone else's password for one purpose and then accesses that password-protected account for a different purpose, the access for a different purpose in some circumstances "exceeds authorized access." *See* 18 U.S.C. § 1030(e)(6) ("[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"); *United States v. Nosal*, 676 F.3d 854, 856-64 (9th Cir. 2012) (en banc) (reviewing caselaw on "exceeds authorized access" and limiting its meaning to conduct that constitutes "hacking—the circumvention of technological access barriers"); *Cheng v. Romo*, No. 11-1007, 2012 WL 6021369 (D. Mass. Nov. 28, 2012), at *4 (D. Mass. Nov. 28, 2012) (indicating that whether use of another's password-protected account exceeded authorized access depends on extent of permission); *Wentworth–Douglass Hosp. v. Young & Novis Prof'l Ass'n*, No. 10-

---

user enters a password, bypasses the password gate, and sees the private information hidden behind it. *See id.* at 220-21 n.4. Other courts take a broader interpretation of "access" and indicate that visiting a webpage is an "access" that is authorized. *See, e.g., Southwest Airlines Co. v. BoardFirst, L.L.C.*, No. 3:06-CV-0891-B, 2007 WL 4823761 (N.D. Tex. Sept. 12, 2007) at *13 (N.D. Tex. Sept. 12, 2007); *see also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1624-28, 1646-48 (2003) (discussing broader and narrower interpretations of "access"). Either way, viewing information not protected by a password is legal—either as an authorized access or as no access at all.

cv-120-SM, 2012 WL 2522963 (D.N.H. June 29, 2012) at *4 (D.N.H. June 29, 2012) (holding that "hack[ing]" or "circumvent[ing] any technological access barrier[]" is required for unauthorized access, and therefore that use of another's password to bypass limits on account is unauthorized access).[11]

By contrast, the computer program in this case did not enter a password or bypass a password prompt. App2. 537. It did not access any private accounts. It did not break in or "hack" in to AT&T's computer. It did not infiltrate AT&T's website. App2. 219. It did not even violate any written prohibitions or Terms of Use on AT&T's website.[12] Spitler's program simply visited public webpage

---

[11] At trial, the government did not distinguish between access "without authorization" and conduct that "exceeds authorized access" under the CFAA. Instead, the government simply argued to the jury "access to AT&T servers was unauthorized." App2. 605-06. Caselaw indicates that the difference hinges on whether the person has any rights to access the computer. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). If a person has been granted no authorization at all to access a computer, breaking in to that computer would be "access without authorization." On the other hand, if the person has been granted some rights to access a computer but then enters in ways that go beyond that authorization, the conduct "exceeds authorized access." *See id.; Pulte Homes*, 648 F.3d at 304.

The difference between the two can be difficult to draw because different courts interpret "access" differently. *See* footnote 10, *supra*. However, it should not matter whether this Court looks to the access "without authorization" or "exceeds authorized access" prong because they both boil down to whether the program "circumvent[ed] technological access barriers." *Nosal*, 676 F.3d at 863. Because no technological access barriers were circumvented, any access was authorized.

[12] Other circuits have disagreed on whether use of a computer in a way contrary to written use policies "exceeds authorized access." *Compare United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010) (answering "yes") *with Nosal*,

addresses and collected the information that *AT&T itself* decided to make available without a password. App2. 527-28. Any member of the public could have done the same thing. By choosing not to protect the e-mail addresses with a password, AT&T authorized the public to view them.

B. AT&T's Hope That the Public Would Not Visit Its Website Does Not Make Such Visits Unauthorized.

At trial, the government argued that using the program was unauthorized because AT&T did not approve of what Spitler and Auernheimer did. App2. 608. "[I]f the defendant had called up AT&T" and asked for the e-mail addresses, the government argued to the jury, "[t]here's no way that they would have provided that information to the defendant." App2. 608; *see also id.* at 318.

This argument misstates the law. As *Pulte Homes* and *Cvent* make clear, the subjective hopes and wishes of the website owner are irrelevant. By posting information on the public web without a password requirement, AT&T made the information available to everyone. Although AT&T did not wish that outsiders would collect the information, the law does not criminalize visiting a website in ways that owners find dissatisfying. AT&T's act of making the information unprotected and available to the public on the information superhighway

---

676 F.3d at 856-64 (answering "no"). That disagreement is not implicated here because the government presented no evidence that such a policy existed.

authorized everyone to access it. *See Pulte Homes*, 648 F.2d at 304; *Cvent*, 739 F. Supp. 2d at 933-34.

EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003), is particularly instructive. In *EF*, a company used an automated scraper program to send thousands of queries to its competitor's website. As the First Circuit explained, a scraper is "nothing more than a computer program that accesses information contained in a succession of webpages stored on the accessed computer." *Id*. at 60. The company's goal was to collect pricing data available on the competitor's site and then to use that data to undercut its competitor's prices. *Id.*

The First Circuit held that use of the scraper was "authorized" under § 1030 even though the company that used the scraper "can have been in no doubt that [its competitors] would dislike the use of the scraper to construct a database" for other businesses to use against them. *Id.* at 63. By placing their prices on the World Wide Web, the website owner could not complain when others visited the web site even if the owner neither wanted nor expected the website to be visited by competitors in an automated way to hurt the plaintiff's business. *See id.*

The same is true here. Spitler's use of the program is closely analogous to the use of the scraper in *EF*. In both cases, the automated programs sent thousands of unwanted requests to a website. In both cases, the acts might appear selfish and

impolite. But in both cases, visiting the website was authorized under the CFAA because the information was published on the World Wide Web.

Any other rule would have disturbing implications. Most Americans surf the web every day. How are they supposed to know when visiting a webpage is legal and when visiting a webpage might land them in jail? Programs that send automated requests to websites are in common use. The web store for the Google Chrome browser offers a free scraper program that anyone can use to collect data from many different pages on a website.[13] How can users know when these programs can be used legally and when their use is illegal?

As the Eleventh Circuit has recognized:

> Through the World Wide Web, individuals can easily and readily access websites hosted throughout the world. Given the Web's ubiquitous and public nature, it becomes increasingly important in cases concerning electronic communications available through the Web for a plaintiff to demonstrate that those communications are not readily accessible. If by simply clicking a hypertext link, after ignoring an express warning, on an otherwise publicly accessible webpage, one is liable under [unauthorized access statutes], then the floodgates of litigation would open and the merely curious would be prosecuted.

Snow v. DirecTV, Inc., 450 F.3d 1314, 1321 (11th Cir. 2006) (interpreting the unauthorized access statute in 18 U.S.C. § 2701). Fortunately, that is not the law.

[13] The program can be accessed at http://goo.gl/dVQ4k (last visited July 1, 2013).

Under *Pulte Homes* and *EF*, visiting an unprotected webpage is authorized under § 1030 even if the website owner wished the visit did not occur.

C. Auernheimer's Characterization of Spitler's Act As "Theft" Does Not Make the Access Illegal.

The government also argued at trial that use of the program was unauthorized because of the words Spitler and Auernheimer chose to describe it. *See* App2. 132; 606-12. In private e-mails, Auernheimer referred to collection of the e-mail addresses as a "theft." App2. 166. In his testimony, Spitler agreed with the prosecutor's view that his program "tricked" and "lied" to the AT&T website. App2. 264. The government argued to the jury that it was these words, "first and foremost," that proved Auernheimer's guilt. App2. 132. To the extent the government's position was clear, it appeared to be that conduct characterized as a theft or a lie is necessarily unauthorized under § 1030. App2. 132, 606-11.

This argument is meritless. Auernheimer's guilt turns on whether the program accessed AT&T's website "without authorization" or "exceed[ed] authorized access." 18 U.S.C. § 1030(a)(2)(C). That depends upon how AT&T's website worked and what the program did. It does not depend on what words Auernheimer chose or thoughts he had when later describing his conduct to others. "The government cannot punish what it considers to be an immoral thought simply by linking it to otherwise innocuous acts, such as walking down the street or chewing gum." *United States v. Tykarsky*, 446 F.3d 458, 471 (3d Cir. 2006). To

be sure, a defendant's words can establish his state of mind. *See Whitney v. Horn*, 280 F.3d 240, 259 (3d Cir. 2002). But the missing element of the crime needed to convict Auernheimer is the absence of authorization, not his intent.

Auernheimer's language is irrelevant even if read to reveal his subjective belief that his conduct was illegal. A defendant's belief as to the criminality of his act is irrelevant. *See generally* Wayne R. LaFave, *Substantive Criminal Law* § 5.6 (2012). Ignorance of the law is no excuse, but neither is it an offense: A person who wrongly thinks his conduct was illegal is guilty of no offense. *See id.*

Further, the government's claim that the program tricked and deceived the AT&T computer into giving up information —implicitly rendering the access unauthorized— is false. AT&T programmed its computer to respond to *anyone* who visited the correct address; it did exactly as it was programmed to do. App2. 514-15. Visiting a website does not carry an implicit promise that the visitor is someone the website owner would like them to be. *See EF Cultural Travel*, 318 F.3d at 63. Posting data on the web posts that data for everyone. *See id.*

The government also claimed that the program tricked AT&T into divulging data because Spitler set his computer web browser's "user agent string" to appear as an iPad. App2. 264; 610. This claim misunderstands the purpose and function of user agent strings. A user agent is a browser setting that tells the website what kind of browser is making a request. App2. 510. The browser setting sends a short

string of data along with website requests that allows websites to optimize the presentation of different web pages for different browsers.[14]

Most importantly, user agents do not regulate access. App2. 514. They are merely browser settings that allow users to optimize how a webpage looks for the user's own convenience. And changing a user agent string is both very easy and very common, taking just a few clicks to allow users to pick whatever settings they want. App2. 512. In fact, most browsers have tools that allow users to change their user agent directly built into their browsers.[15] Setting the user agent string does not "lie" to a website any more than a Phillies fan lies when wearing a Mets cap.

Indeed, it has been common for browsers to be configured by their developers to change their user agent strings automatically as part of their design. *See* Nicholas C. Zakas, *History of the User-Agent String*, available at http://www.nczonline.net/blog/2010/01/12/history-of-the-user-agent-string/ ("The history of the user-agent string is marked by browsers trying to convince user-agent sniffers that they are what they are not. Internet Explorer wants to be identified as Netscape 4; Konqueror and WebKit want to be identified as Firefox;

---

[14] *See generally What's A User Agent?*, http://www.whatsmyuseragent.com/WhatsAUserAgent (last visited July 1, 2013).

[15] Directions for how to do this for Chrome and other browsers are available at http://www.howtogeek.com/113439/how-to-change-your-browsers-user-agent-without-installing-any-extensions/ (last visited July 1, 2013).

Chrome wants to be identified as Safari."); *see also* App2. 512. If changing a user agent string is a federal crime, millions of Americans may be criminals for the way they routinely surf the Web.

D. If "Authorization" is Ambiguous, the Rule of Lenity Requires It to be Narrowly Construed.

Finally, if the Court concludes that the meaning of "without authorization" or "exceeds authorized access" is ambiguous, the rule of lenity requires the court to adopt the narrower interpretation that favors the defendant. *See Rewis v. United States*, 401 U.S. 808, 812 (1971) ("[A]mbiguity concerning the ambit of criminal statutes should be resolved in favor of lenity") (citing *Bell v. United States*, 349 U.S. 81, 83 (1955)). The public would be shocked to learn that it is a federal crime to visit an unprotected website. "If Congress desires to go further" and criminalize visiting websites, "it must speak more clearly than it has." *Skilling v. United States*, 130 S.Ct. 2896, 2933 (2010) (quoting *McNally v. United States*, 483 U.S. 350, 360 (1987)).

In light of the rule of lenity, this Court should heed the guidance of a sister circuit sitting *en banc* on the need to reject broad readings of unauthorized access under the CFAA:

> The government's construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer. This would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime. While ignorance of the law is no excuse, we

> can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer.

Nosal, 676 F.3d at 859. The same skepticism is warranted here.

For these reasons, the Court should find Spitler's access to AT&T's computers was authorized under § 1030(a)(2)(C). The plan to obtain e-mail addresses from AT&T's website was not a criminal conspiracy because the object of the plan was legal. Auernheimer's conviction must therefore be reversed.

II. IF THE COURT FINDS AUERNHEIMER VIOLATED THE CFAA, THE CONVICTION SHOULD BE REDUCED TO A MISDEMEANOR.

Whether a conspiracy crime is a misdemeanor or felony depends on whether the underlying agreement involves a misdemeanor or felony. 18 U.S.C. § 371. Violations of § 1030(a)(2) are ordinarily misdemeanor offenses punishable by up to one year in jail. *See* 18 U.S.C. § 1030(c)(2)(A). However, violations can become felonies if the government proves one of the enhancements found in § 1030(c)(2)(B). *See Cioni*, 649 F.3d at 281-84. The enhancement relevant here is § 1030(c)(2)(B)(ii), which turns a misdemeanor CFAA offense into a felony if the government proves that

> 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[.]

18 U.S.C. § 1030(c)(2)(B)(ii); *see Cioni*, 649 F.3d at 281-84; App.1 6.

The government charged that the access of a computer without authorization under *federal* law was committed in furtherance of accessing a computer without authorization under a New Jersey *state* law, which provides:

> A person is guilty of a crime of the third degree if the person purposely or knowingly and without authorization, or in excess of authorization, accesses any data, data base, computer, computer storage medium, computer software, computer equipment, computer system and knowingly or recklessly discloses or causes to be disclosed any data, data base, computer software, computer programs or personal identifying information.

N.J.S.A. § 2C:20-31(a); *see also* App.1 6.

The government's felony enhancement was improper as a matter of law for two reasons. First, it constituted improper double counting. Second, Auernheimer did not violate the New Jersey computer crime law. For these reasons, any conspiracy to violate the CFAA was at most a misdemeanor rather than a felony.

A. Applying the Felony Enhancement Circumvented Congress's Careful Limits on Felony Liability by Allowing Double-Counting.

When it enacted 18 U.S.C. § 1030, Congress was careful to limit the basic § 1030(a)(2) crime to a misdemeanor. *See* S. Rep. No. 104–357 (1996) at 8 (noting Congress's decision to structure § 1030(a)(2) violations using a base misdemeanor with felony enhancements under specific conditions). The Senate Report that accompanied the enactment of this provision establishes that the enhancement in § 1030(c)(2)(B)(ii) was copied from identical language in the Wiretap Act and was "intended to have the same meaning" as it does in the

Wiretap Act. *Id*. ("The term[] . . . 'for the purpose of committing any criminal or tortious act' [is] taken from . . . the wiretap statute (18 U.S.C. § 2511(1)(d)), . . . and [is] intended to have the same meaning as in [that statute]."); *see also Cioni*, 649 F.3d at 281-82.

Courts interpreting this language in the Wiretap Act have held that an offense is committed "in furtherance of any criminal or tortious act" only when it is committed with the specific intent to further a crime or tort that is "independent of the act of [the offense] itself." *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010). In other words, the government cannot charge a defendant with committing a crime in furtherance of the crime itself. The enhancement applies only if, at the moment the defendant commits one offense (here, unauthorized access), the defendant has a subjective purpose to further a different and independent offense. *See id; see also United States v. McTiernan,* 695 F.3d 882, 889 (9th Cir. 2012) (Wiretap Act liability applies only if recording is "done for the purpose of facilitating some further impropriety" apart from the recording itself) (quotations and citations omitted).

The felony charge in this case cannot stand because New Jersey's unauthorized access statute is not independent of the federal unauthorized access statute. The two crimes are highly similar; most elements are the same. The only difference between the two statutes is a very slight one involving what happens

after the unauthorized access occurs. The CFAA requires information be obtained from the unauthorized access, while New Jersey's statute requires information be disclosed. *Compare* 18 U.S.C. § 1030(a)(2) *with* N.J.S.A. § 2C:20-31(a).

These slight differences cannot satisfy the relevant legal test to show the crimes were distinct: when Spitler's program was used, did he have a subjective intent to further a New Jersey crime other than an unauthorized access offense? *McTiernan,* 695 F.3d at 889; *Caro*, 618 F.3d at 100. He did not. Because the elements of the New Jersey's unauthorized access statute are inextricably linked to the elements of the CFAA, the government cannot use the state offense to engage in double-counting that circumvents Congress's careful limits on felony liability.

The Fourth Circuit reached a similar result in *Cioni*, 649 F.3d 276. In *Cioni*, the defendant accessed another person's email using a stolen password. *Id.* at 279-81. The government indicted her for accessing a computer with authorization in violation of § 1030(a)(2)(C). *Id.* at 281. Both charges were elevated to felonies by charging her with violating the CFAA in furtherance of a violation of § 2701(a), which punishes anyone who accesses without authorization "a facility through which an electronic communication service is provided" and "thereby obtains, alters, or prevents authorized access to a wire or electronic communication." 18 U.S.C. § 2701(a).

The Fourth Circuit vacated the felony conviction and remanded for resentencing to a misdemeanor. *Cioni*, 649 F.3d at 282-84. Although § 1030(a)(2)(C) and § 2701(a) were "two separate and distinct crimes," the enhancement was not "based on distinct conduct." *Id.* at 283. As a result, the government's theory of felony liability was premised on improper double-counting. *Id.* The same is true here. As in *Cioni*, the government is trying to use overlap among unauthorized access statutes to circumvent Congress's limits on felony liability in § 1030(a)(2)(C). Given that most states have their own unauthorized access statutes,[16] the government's theory would allow the DOJ to routinely charge all § 1030(a)(2)(C) cases as felonies instead of misdemeanors. Such double-counting is clearly contrary to Congress's intent and this Court must reject it.

B. Auernheimer Did Not Violate New Jersey's Unauthorized Access Law.

The felony CFAA charge must also be reduced to a misdemeanor because the government failed to prove Auernheimer violated N.J.S.A. § 2C:20-31(a). That is true for two reasons. First, the only published decision on New Jersey's computer access statute held that liability under N.J.S.A. § 2C:20-31(a) requires proof that the defendant breached a "code-based" barrier such as a password-gate

[16] *See generally* Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 Rich. J.L. & Tech. 28, 15 n.37 (2001).

that actually denied access to those attempting to enter. *See State v. Riley*, 988 A.2d 1252, 1267 (N.J. Super. Ct. Law Div. 2009). No such code-based barrier existed here. The website was not protected by a password and was available for anyone on the Internet to view. Thus, even if this Court deems the use of the program an unauthorized access under the CFAA, it was not an unauthorized access under New Jersey state law under *Riley*.

Second, the conduct did not violate N.J.S.A. § 2C:20-31(a) because New Jersey's unauthorized access statute does not extend to acts occurring entirely outside New Jersey. The territorial reach of New Jersey's criminal laws are normally governed by N.J.S.A. § 2C:1–3, which generally requires that at least part of the crime occur inside New Jersey. *Cf. State v. Bragg*, 295 N.J. Super. 459, 465-67 (App. Div. 1996). New Jersey's computer crime laws have an additional provision extending the state's territorial reach if the computer or "the actual damage" occurs in New Jersey. N.J.S.A. § 2C:20–34.

In this case, the conduct occurred entirely outside New Jersey. The defendants were outside New Jersey, the computers were outside New Jersey, and the information was disclosed outside New Jersey. All of the elements of the crime occurred outside New Jersey. As a result, no New Jersey crime was committed. New Jersey simply lacked criminal jurisdiction over Auernheimer and Spitler's conduct.

Indeed, under the Dormant Commerce Clause, New Jersey could not lawfully regulate the conduct. When states have enacted computer crime laws that attempt to regulate extraterritorial conduct, courts have not hesitated to invalidate them under the Dormant Commerce Clause. *See, e.g., American Booksellers Foundation v. Dean*, 342 F.3d 96, 104 (2d Cir. 2003) (striking down Vermont computer crime law that extended to conduct outside Vermont) (citing cases). New Jersey cannot extend its criminal laws to conduct all around the country or the world; it must only regulate acts in or involving New Jersey. *See id.* For these reasons, the government failed to show a violation of N.J.S.A. § 2C:20-31(a) and the felony conviction for Count 1 must be reduced to a misdemeanor.

III. THE § 1028(A)(7) CONVICTION MUST BE OVERTURNED BECAUSE AUERNHEIMER DID NOT POSSESS OR TRANSFER THE E-MAIL ADDRESSES "IN CONNECTION WITH" UNLAWFUL ACTIVITY.

Count 2 of the indictment charged Auernheimer with violating the federal identity theft statute, 18 U.S.C. § 1028(a)(7), which punishes one who:

> knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law[.]

18 U.S.C. § 1028(a)(7). The legislative history of this relatively new prohibition indicates that it was intended to punish "identity theft," such as using false or

stolen identity information to commit fraud. *See* H.R. Rep. No. 108-528 at 4-7 (2004)**,** *available at* 2004 U.S.C.C.A.N. 779, 780-82.

Auernheimer did not violate this statute for two reasons. First, as explained earlier, the act of obtaining the e-mail addresses from AT&T's unprotected website did not violate § 1030(a)(2)(C). *See supra*, p. 18-31. The government's only alleged predicate offense under § 1028(a)(7) was a violation of § 1030(a)(2)(C). App.2 16, 707. The absence of that predicate offense means that Auernheimer cannot be liable under § 1028(a)(7). *See United States v. Bonilla*, 579 F.3d 1233, 1242-43 (11th Cir. 2009) ("[U]nlawful activity in violation of federal law triggers § 1028(a)(7)"). Because that act was not unlawful, Auernheimer's possession of the e-mail addresses was not in any way related to "unlawful activity that constitutes a violation of Federal law." 18 U.S.C. § 1028(a)(7).

Count 2 must fail for a second reason. Even assuming Auernheimer violated § 1030(a)(2)(C) to obtain the e-mail addresses, he did not then possess or transfer the e-mails "in connection with" another crime. The phrase "in connection with . . . any unlawful activity" means unlawful activity other than the wrongful act of obtaining the means of identity. By that standard, it is clear that Auernheimer did not violate § 1028(a)(7).

Both the statutory text and the legislative history support the view that the "unlawful activity" must be some crime other than the unlawful means of

obtaining an identity. The statutory text makes this clear by requiring the government to prove two different kinds of unlawfulness. First, the government must prove the defendant "wrongly acquired" a means of identity "without lawful authority." H.R. Rep. No. 108-528 at 10 (2004), *reprinted in* 2004 U.S.C.C.A.N. 779, 786; 18 U.S.C. § 1028(a)(7). Second, the government must show the defendant's wrongful possession, use, or transfer was "in connection with . . . unlawful activity." 18 U.S.C. § 1028(a)(7).

The two mentions of "unlawfulness" are not surplusage. The natural reading of the text is that liability under § 1028(a)(7) requires two different kinds of unlawfulness: *first*, the lack of lawful authority to possess, use, or transfer a means of identity; and *second*, a connection between that unlawful possession, use, or transfer and some other unlawful activity such as a fraud scheme. *See Pennsylvania Dept. of Public Welfare v. Davenport*, 495 U.S. 552, 562, (1990) (expressing "a deep reluctance to interpret a statutory provision so as to render superfluous other provisions in the same enactment").

The legislative history confirms this interpretation of § 1028(a)(7). The House Report indicates that Congress aimed to punish individuals "who ha[ve] wrongly acquired another's means of identification, but ha[ve] not yet put it to use or transferred it elsewhere." *See* H.R. Rep. No. 108-528 at 10, 2004 U.S.C.C.A.N. at 786. Specifically, Congress enacted the current version of § 1028(a)(7) out of

concern that it may be difficult to prove an identity thief's specific intent to put stolen identities to criminal use. *Id.* Identity theft is generally understood as the crime of using someone's stolen identity information to commit a crime such as fraud. *See Flores-Figueroa v. United States*, 556 U.S. 646, 656 (2009) (using the example of "a defendant [who] has used another person's identification information to get access to that person's bank account" as "the classic case of identity theft"). Section 1028(a)(7) was therefore designed to hold an identity thief liable if the government can show knowledge that his acts of possession or transfer of stolen identity information *facilitate* another crime without having to show specific intent to commit that separate crime. H.R. Rep. No. 108-528 at 10, 2004 U.S.C.C.A.N. at 786.

As both the text and legislative history show, the "unlawful activity" that the possession or transfer must be "in connection with" is some unlawful act other than the wrongful act of obtaining the means of identity. *See also United States v. Villanueva-Sotelo*, 515 F.3d 1234, 1245 (D.C. Cir. 2008) ("Congress amended section 1028(a)(7) [in 2004] to ease the prosecution of identity thieves who intend to use another person's means of identification . . . to commit a felony, but have not yet actually done so.") (citing H.R. Rep. No. 108–528, at 10–11, 2004 U.S.C.C.A.N. at 786).

The government's contrary view would render the statute unconstitutionally vague. Under the government's theory, if it charges a defendant with hacking for illegally acquiring personal information, the government can always add a second count of identity theft for possessing the information just acquired. After all, possession of information will always be "in connection with" the way a person came to possess it. And when a person "obtains" information under § 1030(a)(2)(C) he necessarily then "possesses" that information under § 1028(a)(7). *See* Webster's New Universal Unabridged Dictionary at 1138 (2003) (defining "obtain" as to "come into possession of"). Under the government's theory, every misdemeanor unauthorized access involving personal information is always a felony identity theft, too.

This remarkable view of § 1028(a)(7) must be rejected. The phrase "in connection with" is notoriously vague. *See United States v. Loney*, 219 F.3d 281, 283 (3d Cir. 2000) (noting the phrase's "vagueness and pliability" and "vague, loose connective") (citations omitted). On one hand, it is possible to read the phrase breathtakingly broadly. "[A]s many a curbstone philosopher has observed, everything is related to everything else." *Cal. Div. of Labor v. Dillingham*, 519 U.S. 316, 335 (1997) (Scalia, J., concurring); *see also Bloom v. Bradford*, 480 F. Supp. 139 (E.D.N.Y. 1979) ("[I]n one sense everything is connected to everything else.").

Read very broadly, § 1028(a)(7) could have breathtaking scope. Imagine a bank robber asks the bank teller for her name in the course of the crime. After his arrest, the robber tells his lawyer that the teller gave her name as "Beth." Under the broadest reading of § 1028(a)(7), both the robber and his lawyer would be guilty of felony identity theft. After all, the robber "transfer[ed]" and his lawyer "possess[ed]" a means of identification[17] (the name Beth), all "in connection with" the crime of bank robbery.

Although such an extreme interpretation is linguistically possible, it would render § 1028(a)(7) unconstitutionally void for vagueness. *See Giaccio v. Pennsylvania*, 382 U.S. 399, 402 (1966) (noting that a criminal statute is unconstitutionally void if it is "so vague and standardless that it leaves the public uncertain as to the conduct it prohibits"). To save its constitutionally, this Court must construe the vague and standard-less language of § 1028(a)(7) in a fashion that covers only the core conduct Congress was attempting to prohibit. *See Skilling v. United States*, 130 S. Ct. 2896, 2931 (2010) (interpreting the honest services fraud statute narrowly to cover only the core conduct Congress clearly intended to prohibit in light of the vagueness concerns raised by a broader

[17] "Means of identification" is defined as a "name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any . . . name." 18 U.S.C. § 1028(d)(7)(A).

interpretation). The core conduct was possession or use "in connection with" unlawful activity other than the unlawful means of obtaining the information.

With this understanding, Count 2 was premised on an erroneous view of the law. The government argued that the only unlawfulness in Auernheimer's possession, use, or transfer of means of identity was acquisition in violation of § 1030(a)(2)(C). App.2 16, 707. The government offered no evidence whatsoever that the possession, use, or transfer was "in connection with" any *other* crime beyond the crime of coming into possession of the information in the first place. The conviction for Count 2 must fail then because there is no evidence that Auernheimer had any connection to a criminal scheme involving the information after it was unlawfully acquired.

IV. VENUE IN NEW JERSEY WAS IMPROPER BECAUSE NO AT&T COMPUTERS WERE THERE AND NO DATA WAS TRANSFERRED, POSSESSED OR USED IN THE STATE.

Even if this Court concludes that Auernheimer was guilty of both Counts, the Court must still vacate the convictions because the government failed to establish that there was venue in the District of New Jersey. A criminal defendant has a constitutional right to be tried in the district where his alleged crime was committed. *United States v. Rodriguez-Moreno*, 526 U.S. 275, 278 (1999); *United States v. Perez*, 280 F.3d 318, 329 (3d Cir. 2002) (citing U.S. Const. amend. VI and U.S. Const. art. III, § 2, cl. 3); *United States v. Pendleton*, 658 F.3d 299, 302-

03 (3d Cir. 2011) (same); *see also* Fed. R. Crim. P. 18 ("[G]overnment must prosecute an offense in a district where the offense was committed.").

The venue requirement provides a "safety net" for criminal defendants. *United States v. Salinas*, 373 F.3d 161, 164 (1st Cir. 2004). If legal limits on venue are ignored, any aggressive Assistant U.S. Attorney anywhere in the country can bring charges against an unpopular or controversial person. The venue requirement ensures that only prosecutors in districts where the crime actually occurred can bring a prosecution.

"[A]ny offense against the United States begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a). "The Government bears the burden of proving venue by a preponderance of the evidence and venue must be proper for each count of the indictment." *United States v. Root*, 585 F.3d 145, 155 (3d Cir. 2009) (citing *Perez*, 280 F.3d at 328-30).

To determine whether venue is proper, courts must apply the "*locus delicti*" test, which identifies where a crime occurred based on "the nature of the crime alleged and the location of the act or acts constituting it." *Rodriguez–Moreno*, 526 U.S. at 279 (citation omitted); *Pendleton*, 658 F.3d at 303. A "court must initially identify the conduct constituting the offense (the nature of the crime) and then

discern the location of the commission of the criminal acts)." *Rodriguez–Moreno*, 526 U.S. at 279. Venue is proper where "the crucial elements [of the crime] are performed." *Perez*, 280 F.3d at 329.

Identifying the crucial elements requires a close reading of the statutory text to identify where the crime occurred. Count 1 is a charge of conspiracy under 18 U.S.C. § 371 to violate 18 U.S.C. § 1030(a)(2)(C). That section makes it illegal to "intentionally *access* a computer without authorization or *exceed*[] authorized access, and thereby *obtain*[] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C) (emphasis added). This language makes clear that the crucial elements of the crime occur wherever the computer is accessed (that is, wherever the computer is located) or wherever the data is obtained (that is, wherever the individuals or storage devices located). The Department of Justice's own manual on prosecuting computer crimes agrees, explaining "it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access *and* where the information is obtained." Office of Legal Educ. Exec. Office for U. S. Attorneys, *Prosecuting Computer Crimes* at 118.[18]

The government indicted this case in the District of New Jersey even though no computer was accessed and no data obtained there. At all times relevant to the charges in this case, Auernheimer was in Arkansas and never visited New Jersey

[18] Available at http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (last visited July 1, 2013).

until he had to appear in court there. App.2 185, 366. Spitler was in San Francisco, California. App2. 233. The evidence at trial demonstrated the AT&T servers that Spitler accessed were located in Atlanta, Georgia and Dallas, Texas. App2. 434-35, 443-44 There was no evidence whatsoever that any data traveled through or to computers in New Jersey. App2. 442-43

Focusing on where the computer was accessed or data was taken means that this case could have been charged in Arkansas, California, Georgia, or Texas. It might also have been proper to charge this case in other districts where computer traffic traveled in the course of the conduct. But the charges could not be brought in New Jersey, where no computer was accessed, no defendant was located, and no computer traffic traveled. *See United States v. Lanoue*, 137 F.3d 656, 661 (1st Cir. 1998) (holding that the crime of being a felon in possession of a firearm can only be charged where the firearm is "actually possessed"); *United States v. Cabrales*, 524 U.S. 1, 8 (1998) (holding that venue is improper when the government charged a defendant in Missouri for money laundering in Florida using money from a Missouri narcotics operation because the defendant did not act in Missouri).

Before the district court, the government's main argument that venue was proper in New Jersey for the § 1030 charges was that the CFAA is about protecting privacy and approximately 4,500 of the e-mail addresses—4% of the 114,000—belonged to New Jersey residents. App2. 112, 221. Thus, the end result of

Auernheimer's conduct was a privacy harm presumably felt in New Jersey. App2. 110-18.

The government's argument misunderstands the applicable legal standard. Venue requires a close study of the text of the statute to see what conduct Congress prohibited, not speculation about where effects of the conduct might be felt or what happened after the crime was committed. For example, in *United States v. Passodelis*, 615 F.2d 975 (3d Cir. 1980), a defendant made improper campaign contributions in one district for a political campaign in another district. 615 F.3d at 976. The court overturned the convictions obtained in the district where the campaign was located on the ground that the crime only occurred where the contributions were made. *See id.* at 978-79. By that same reasoning, venue is only proper where the computer was accessed and information was obtained.

The government also argued that venue was proper because Count 1 charged a felony on the basis of conduct in furtherance of a New Jersey crime. App2. 110, 112. Again, this misunderstands the law. The question is what Congress prohibited when it enacted the statute, not what prosecutors decided to charge when they brought the indictment. *Rodriguez–Moreno*, 526 U.S. at 278; *Cabrales*, 524 U.S. at 6-7. Congress did not make it a federal crime to violate New Jersey law. Rather, Congress merely specified that hacking in furtherance of any crime or tort is a felony rather than a misdemeanor. *See* 18 U.S.C. § 1030(c)(2)(B)(ii). The

government's theory means venue is proper for any CFAA crime wherever there is a state law prohibiting similar conduct.

Even if the New Jersey statute is included in a search for essential elements of the crime, the government's theory fails. The New Jersey statute prohibits the knowing or reckless *disclosure* of personal identifying information that the defendant knowingly *accessed* without authorization. N.J.S.A. § 2C:20-31(a). The statute's terms describe conduct that occurred in districts other than the District of New Jersey.

Venue is lacking for Count 2 for similar reasons that it is lacking in Count 1. Count 2 charged identity theft under 18 U.S.C. § 1028(a)(7), which punishes in relevant part any person who

> knowingly *transfers*, *possesses*, or *uses*, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law

18 U.S.C. § 1028(a)(7) (emphasis added). The plain text of the statute indicates venue is proper in any district in which the means of identification were transferred, possessed, or used. Venue is not proper in New Jersey in this case because no data was transferred, possessed, or used there. *See Lanoue,* 137 F.3d at 661.

The government's novel theory that venue is proper wherever some harm may be felt is particularly troubling in a case involving Internet crimes. Given the

interconnectedness of the Internet, criminal defendants could be dragged into court in virtually any state, regardless of whether it would be foreseeable or reasonable to defend against a criminal trial there, giving every U.S. Attorney's Office the choice of bringing a case and allowing the government to cherry-pick the most advantageous jurisdictions in which to prosecute the defendant. The doctrine of venue is predicated on avoiding this prosecutorial and constitutional abuse. *See United States v. Morgan*, 393 F.3d 192, 201 (D.C. Cir. 2004).

In short, this case has nothing to do with New Jersey and should not have been charged in New Jersey. Venue was improper in New Jersey and the convictions must be reversed.[19]

[19] The government and district court relied heavily on a short unpublished decision by a Magistrate Judge in Nebraska in *United States v. Powers*, No. 09-cr-261, 2010 WL 1418172 (D.Neb. 2010). App1. 25-26, App2. 113-15. In *Powers*, an e-mail account holder in Nebraska gave the defendant her e-mail password. The defendant later used the account from Arizona for reasons beyond the account holder's permission, finding nude pictures of her, harassing her in Nebraska, and sending the nude pictures to others in Nebraska. The defendant was indicted for violating the CFAA in Nebraska and unsuccessfully challenged venue there. *See Powers,* 2010 WL 1418172, at *1-2.

But *Powers* is distinguishable on its facts. In *Powers*, the defendant actually sent messages into the jurisdiction in which the case was charged. In contrast, no communications were sent to or even through New Jersey in this case. Further, the government did not allege harassment of anyone in New Jersey or identify any specific harm felt by anyone in New Jersey. Even if *Powers* somehow lends support to the government's position, its cryptic and brief discussion is too light on legal analysis to be of much assistance. Further, an unpublished Magistrate Judge's decision from Nebraska is not binding on this Court.

V. THE SENTENCE MUST BE VACATED BECAUSE THE MAILING COSTS WERE NEITHER "REASONABLE" NOR "LOSSES."

The district court sentenced Auernheimer to a 41-month prison sentence based in large part on an eight level upward adjustment under U.S.S.G. § 2B1.1(b)(1)(E) since he caused more than $73,000 in "loss" to AT&T. App2. 771, 782. That "loss" was allegedly the costs of mailing a notice to AT&T customers notifying them of the security breach. AT&T sent the mail notice although an email notice the week before had achieved a 98% success rate according to internal AT&T documents. App2. 750. The district court found the eight-level increase appropriate because it was a "reasonably foreseeable" cost that "relates to trying to rectify or resolve what occurred after the crime occurred" and related "to the criminal activity and the actual need to notify the iPad users." App2. 770-71. It also ordered the loss amount to be repaid to AT&T as restitution. But as explained below, this upward adjustment was improperly applied and as a result, the sentence must be vacated and the case remanded for resentencing.

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

The government must prove loss by a preponderance of the evidence. *United States v. Jimenez*, 513 F.3d 62, 86 (3d Cir. 2008). The government must make out a "prima facie case of the loss amount," and only after that does the

burden of production shift to the defendant to challenge this evidence. *United States v. Fumo*, 655 F.3d 288, 310 (3d Cir. 2011).

Here, the government presented absolutely no evidence of financial loss by AT&T as a result of Auernheimer's activities. The loss amount was mentioned casually on the last page of the complaint but it references no source for that information. App1. 58. Although an AT&T's assistant vice president, Shirley Ramsey, testified at the trial, she presented no evidence of the amount of loss. App2. 212-22.

In the PSR there was no specific evidence —such as an invoice or receipt or expense report detailing what the amount of loss was to AT&T. In fact, according to the PSR, AT&T was given the opportunity by the probation department to provide a statement and to fill out an affidavit form to declare any losses under the Mandatory Victim's Restitution Act of 1996. *See* 18 U.S.C. §§ 3663, 3664. Remarkably, AT&T chose to submit nothing. *See* PSR at 18, ¶ 53.

In its sentencing memorandum, the government noted its agreement with the probation department's calculation of loss but provided no evidence at all of how this $73,000 amount was calculated. App2. 734. Despite submitting ten exhibits with its sentencing letter, not a single one of them related to AT&T's loss, let alone mentioned it. DCR 89.

By failing to present any evidence of the loss, the government failed to carry its burden of proof. Thus, it was clear error for the sentencing court to rely on the government and probation office's assertion that AT&T suffered $73,000 in loss.

B. The Mailing Costs Were Not "Loss" Under the CFAA.

Even if the government sufficiently proved AT&T spent approximately $73,000 in mailing costs to notify its customers of the disclosure of their email addresses, applying the eight level enhancement in U.S.S.G. § 2B1.1(b)(1)(E) was wrong because these mailing costs do not qualify as "loss" under the CFAA since (1) mailing costs do not qualify as "loss" under the CFAA specific definition of "loss" in U.S.S.G. § 2B1.1 and 18 U.S.C. § 1030(e)(11); and (2) the mailing costs were "unreasonable" under U.S.S.G. § 2B1.1 since electronic notice was effective.

1. Mailing Costs Do Not Count as "Loss" Under 18 U.S.C. § 1030(e)(11) or U.S.S.G. § 2B1.1 Since They Were Unrelated to a Computer.

The application notes to U.S.S.G. § 2B1.1 explain that "loss" should be the greater of "actual" or "intended" loss. U.S.S.G. § 2B1.1 app. n. (3)(A). "Actual" loss is generally defined as "the reasonably foreseeable pecuniary harm that resulted from the offense." U.S.S.G. § 2B1.1 app. n. (3)(A)(i). But the Guidelines include a broader definition of "actual" loss for CFAA convictions:

> In the case of an offense under 18 U.S.C. § 1030, actual loss 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 broader definition comes from the definition of "loss" in the CFAA itself in § 1030(e)(11). Thus, court cases analyzing the CFAA's definition of "loss" are relevant in determining what "loss" means for purposes of applying U.S.S.G. § 2B1.1 to CFAA convictions. *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)).

The definition of "loss" in §1030(e)(11) covers two things: "any reasonable cost to the victim" including the cost of "responding to the offense or otherwise restoring lost material" or "lost revenue or other damages incurred as a result of an interruption of service." *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009). Though this definition can cover economic harm, any such harm must be related to the computer systems. *Id; see also CustomGuide v. CareerBuilder, LLC*, 813 F. Supp. 2d 990, 998 (N.D. Ill. 2011) ("economic costs unrelated to computer systems do not fall within the statutory definition of [loss]").

Stated differently, "[c]osts not related to computer impairment or computer damages are 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 Von Holdt v. A-1 Tool Corp.*, 714 F. Supp. 2d 863, 875 (N.D. Ill. 2010) (CFAA "loss" must relate to "the investigation or repair of a computer or computer system following a violation that caused impairment or unavailability of data or interruption of service.") (quotations and citation omitted)); *Am. Ins. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766, 772 (N.D. Ohio 2008) ("The CFAA does not contemplate consequential damages ... unrelated to harm to the computer itself.").

So "remedial costs" incurred investigating damage and fixing that damage, as well any costs incurred "because the computer cannot function while or until repairs are made" are "loss" under the CFAA. *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)); *see also A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009).

But travel costs for senior executives of a company to conduct a damage assessment and respond to an intrusion for business purposes are insufficient to count as "loss" under the CFAA. *Nexans Wires S.A.*, 319 F. Supp. 2d at 476. The same is true of lost business revenue, and lost profits unrelated to fixing the computer. *id.* at 477-78; *Civic Ctr. Motors*, 387 F. Supp. 2d at 382. Nor do

attorneys fees or litigation costs, unrelated to the computer, count as "loss" under the CFAA either. *Wilson v. Moreau*, 440 F. Supp. 2d 81, 110 (D.R.I. 2006).

Here, the only alleged "loss" to AT&T was the mailing costs of notifying its customers of the breach. That cost was not incurred because of any damage caused to AT&T computers, let alone assessing, responding to or fixing any damage because Auernheimer caused no damage to AT&T computers at all. No data was taken, deleted or destroyed. AT&T customers could still login to AT&T's website through their iPads accounts and access their accounts. As AT&T's Shirley Ramsey testified at trial, the only technical thing AT&T did as a result of the breach was to disable the website from automatically populating a user's email address:

> So our technical folks looked at this server and were able to go in and do some technical changes so that the user, when they're trying to register their iPad to get service to work, they would have to put in both the e-mail address and the password so the e-mail wouldn't automatically be populated.

App2. 219. Because the mailing costs were unrelated to any damage caused to AT&T computers, any costs in assessing damage to or fixing AT&T computers, or costs incurred because of an interruption of service, they do not qualify as "loss" under the CFAA, and in turn U.S.S.G. § 2B1.1.

At least one district court has found that costs associated with "determining and complying with customer security breach notification obligations" do not

qualify as loss under the CFAA. *Farmers Ins. Exch. v. Auto Club Grp.*, 823 F. Supp. 2d 847, 855 (N.D. Ill. 2011). *Farmers* sued a rival insurance agency, AAA, under the CFAA after Farmers employees gave AAA employees confidential login and password information that allowed AAA agents to login to a Farmers online database and obtain confidential policyholder information about Farmers' customers. *Id.* at 850-51. The court found Farmers failed to allege "loss" and dismissed the claims under Federal Rule of Civil Procedure 12(b)(6). *Id.* at 856. The costs associated with complying with breach notification laws were not "loss" because they were not "directly attributable" to the "unauthorized computer access itself, but are instead properly attributable to the resulting disclosure of certain confidential information." *Id.* at 856.

The same is true here. AT&T's mailing costs were not attributable to the computer access itself, but rather the disclosure of the email addresses. After all, there was no "damage" to AT&T's computers and the integrity of any AT&T data was not impaired. AT&T spent no money fixing its computer architecture or attempting to retrieve lost data. These incidental mailing costs do not qualify as "loss" under the CFAA. And as a result, it was improper to apply the eight level adjustment under U.S.S.G. § 2B1.1(b)(1)(E). Rather, under U.S.S.G. § 2B1.1(b)(1)(A), he should have received no upward adjustment since the "loss" was less than $5,000, specifically $0.

2. The Mailing Costs Were Unreasonable Since Email Notice Was Effective.

The CFAA specific definition of "loss" in U.S.S.G. § 2B1.1 covers "any reasonable cost to any victim." U.S.S.G. § 2B1.1 app. n. (3)(A)(v)(III). "Reasonable" means "fair, proper, or moderate under the circumstances." Black's Law Dictionary (9th ed. 2009). But adding unnecessary mailing costs to notify customers of the breach is hardly "fair, proper, or moderate."

There was no evidence that AT&T had a legal obligation to notify its customers of the disclosure. Rather, AT&T's Shirley Ramsey testified that it was AT&T's "policy and practice" to disclose anytime there's a breach of personal information. App2. 214. And even if there was a legal obligation, all four states involved in this case—Arkansas, California, 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); N.J.S.A. § 56:8-163(d); Tex. Bus. & Com. Code Ann. § 521.053(e).[20]

[20] Most states have enacted breach notification laws requiring companies to report the disclosure of personally identifiable identification has been taken through some unauthorized access to a database. But Arkansas, California and New Jersey—the states where Auernheimer and Spitler were physically located and the state where they were charged – do not include email addresses unconnected to a financial institution in their definitions of "personal information" that trigger disclosure requirements. *See* Ark. Code Ann. § 4-110-103(7); Cal. Civ. Code §§ 1798.29(g), 1798.82(h); N.J.S.A. § 56:8-161.

Here, email notice was effective for 98% of AT&T's affected customers. *See* App2. 215, 228-29, 750. Duplicating an already unnecessary notice with an unnecessary physical mailing was not "fair, proper, or moderate" and hence unreasonable. It was especially unfair to count this additional, unnecessary cost because it played a significant role at Auernheimer's sentencing, resulting in a dramatic increase of his Guideline range.

At most, the only "reasonable" physical mailing cost would be the cost to the 2% of customers who had not received the email notification. That meant the "loss" under U.S.S.G. § 2B1.1 should have been calculated as approximately $1,460, or 2% of the alleged $73,000 mailing costs claimed by AT&T. That would result in no increase under U.S.S.G. § 2B1.1(b)(1)(A) rather than the dramatic eight-level increase the court imposed on Auernheimer.

Because the mailing costs were unnecessary and unreasonable, the sentence must be reversed.

CONCLUSION

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

Dated this 1st day of July, 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 Hofmann
LAW OFFICE OF MARCIA 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

Attorneys for Defendant-Appellant Andrew Auernheimer

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

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

1. This Appellant's Opening Brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 13,899 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

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

Dated: July 1, 2013

By: /s/ Hanni Fakhoury__

Hanni M. Fakhoury
ELECTRONIC
FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Fax: (415) 436-9993
Email: hanni@eff.org

Attorney for Defendant-
Appellant Andrew Auernheimer

CERTIFICATION OF VIRUS CHECK

I certify that a virus check was performed on the PDF file of Appellant's Opening Brief using Sophos Anti-Virus software version 8.0.15C.

Dated: July 1, 2013

By: /s/ Hanni Fakhoury__

Hanni M. Fakhoury
ELECTRONIC
FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Fax: (415) 436-9993
Email: hanni@eff.org

Attorney 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 July 1, 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: July 1, 2013

By: /s/ Hanni Fakhory__

Hanni M. Fakhoury
ELECTRONIC
FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Fax: (415) 436-9993
Email: hanni@eff.org

Attorney for Defendant-Appellant Andrew Auernheimer