No. 13-1816

IN THE
UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

UNITED STATES OF AMERICA

v.

ANDREW AUERNHEIMER,
Appellant.

Appeal from a Final Judgment in a Criminal Case of the United States District Court for the District of New Jersey (Crim. No. 11-470).
Sat Below: Honorable Susan D. Wigenton, U.S.D.J.

BRIEF FOR APPELLEE

PAUL J. FISHMAN
United States Attorney

GLENN J. MORAMARCO
Assistant U.S. Attorney
Camden Federal Building
401 Market Street, Fourth Floor
Camden, New Jersey 08101
(856) 968-4863

TABLE OF CONTENTS

Page

TABLE OF ABBREVIATIONS

"A"	refers to the pages of the Defendant's Appendix.
"SA"	refers to the pages of the Government's Supplemental Appendix.
"PSR"	refers to the presentence investigation report filed under seal with this Court.
"DB"	refers to the pages of the Defendant's Brief.
"DMLP"	refers to the Digital Media Law Project.
"MF"	refers to the Mozilla Foundation and its associated *amici*.
"NACDL"	refers to the National Association of Criminal Defense Lawyers.
"SR"	refers to a group of security researchers, beginning with Meredith Patterson, who filed an *amicus* brief in this case.

TABLE OF AUTHORITIES

Page

Cases Cited

Federal Statutes Cited

State Statutes Cited

Congressional Material Cited

STATEMENT OF THE ISSUES

1. Whether the Government presented sufficient evidence to permit the jury to find that the conspirators' accessing of AT&T's servers was "without authorization."

2. Whether the Government presented sufficient evidence to permit the jury to convict Auernheimer of a felony, rather than a misdemeanor, violation of the CFAA.

3. Whether the District Court plainly erred by not overturning Auernheimer's identity fraud conviction because Auernheimer allegedly did not possess or transfer the e-mail addresses "in connection with" unlawful activity.

4. Whether venue was proper in New Jersey for each count.

5. Whether the District Court properly calculated the loss amount at sentencing.

STATEMENT OF THE FACTS

On January 27, 2010, Apple Computer began selling the iPad, a touchscreen tablet computer. PSR ¶ 11. All iPads could access the internet using Wi-Fi, and some iPads could also access the internet through a 3G wireless network, for which AT&T Communications, Inc. ("AT&T") was the exclusive authorized internet service provider. PSR ¶ 11.

iPad owners who wanted to use AT&T's 3G network had to register with AT&T and purchase a monthly contract. As part of the registration process, the iPad owner provided, among other things, an e-mail address, billing information, and a password. A216-17. Each iPad, like other mobile devices, contains a Subscriber Identity Module, known as a "SIM card." Each SIM card has an Integrated Circuit Card Identifier, known as an ICC-ID, which is a unique 19 or 20 digit identifying number, more commonly known as a serial number.

A sign-in screen for access to an internet service provider's network often will consist of a username and a password. The iPad was configured to require an email address (as a type of username) and a customer-selected password. AT&T decided, for business reasons, that it wanted its iPad customers to be able to access their 3G wireless plans with minimal effort. A217-19, A226, A408-09. AT&T configured the sign-in process so that its servers would automatically recognize

each iPad through its unique 19 or 20 digit ICC-ID, and the customer needed to type in only his or her password to gain access to the 3G network. A257-58. Rather than having to enter his or her email address manually, the email address would appear automatically at the login screen. *Id.*

Goatse Security

Appellant Andrew Auernheimer was in charge of Goatse Security, A238, which sometimes purports to be a security research company. It is not, to put it mildly, a traditional security research company. The firm's name is a reference to a notoriously obscene internet shock site.[1] On its own website, Goatse Security claims it is "a wholly owned subsidiary of the GNAA," with a hyperlink to the "Gay Niggers Association of America." SA135. The website lists nine members, beginning with Auernheimer (also known as "weev"), and also includes co-conspirator Daniel Spitler, who is identified by the handle "JacksonBrown." SA135; A267. Goatse Security's corporate motto is "gaping holes exposed." SA135.

Goatse Security took credit for three "exploits," which included not only the breach of AT&T's iPad ICC-ID database, but also an "XPS attack" on Apple's Safari web browser, and a "protocol scripting exploit" of the Firefox web browser.

[1] For a more graphic description, *see* http://en.wikipedia.org/wiki/Goatse.

A239; SA135. In addition to advertising Auernheimer's technical ability with e-mail deliverability, automated trading platforms, business logic exploitation, and the like, the Goatse website listed Auernheimer as president of the GNAA, and it touted his ability to "bash" (a command processor for UNIX) "while drunk" and program in "perl" (a computer language) "while tripping." SA135.

The business interests and goals of Goatse Security were explained by Auernheimer in an email:

> At Goatse Security, we don't really care about fighting cyberterrorism or cyber crime or whatever. We are pioneering new classes of exploits, new methods of evading IDS and new ways to use computers as tools to make shit happen. Our minds won't be owned by some liar's system of ethics, but they are for rent to any God or government (or corporation or criminal organization) that will write a check of sufficient size.

A181-82; SA410-11. In reality, Goatse was not a legitimate business, but instead was a group of hackers, led by Auernheimer, A238, who would discuss computer security flaws in a private internet chat room and help each other with their exploits, A235-38.

Daniel Spitler Hacks Into The AT&T Server

When the iPad was released, AT&T began offering an unlimited 3G data plan for only $30 per month. A250. This was the best price available for an unlimited data plan, but it was limited to iPads only. A250-51. Daniel Spitler did

not own an iPad, but he wanted to take advantage of the $30 per month offer anyway, so he decided to buy a replacement SIM card for an iPad, hoping that he could substitute it into another device and trick AT&T into providing him with unlimited internet access for only $30 per month. A250-51.

Spitler purchased the iPad replacement SIM card and plugged it into his 3G modem. A251-52. Spitler discovered, however, that simply putting the iPad SIM card in his modem did not allow him to access the internet. A252. The SIM card first needed to be registered with AT&T, but Spitler needed an iPad, which he did not have, to register it. A252. Spitler could not find a website for registering his new SIM card using traditional internet search methods. A252-53. Spitler was forced to download the entire Internal Operation System ("IOS") for iPad onto his computer to try to learn how Apple conducted iPad registration. A253. After downloading the operating system, Spitler next had to find the encryption key. A253. Spitler was able to find the password to decrypt the firmware image online. A253-54.

After Spitler decrypted the operating system, he began looking through its file system to find a URL[2] that would allow him to access the iPad registration

[2] A "URL" is a uniform resource locator, more commonly known as a "web address." A255. It is a specific character string that is associated with a particular webpage.

page. A254. Eventually, Spitler found the AT&T carrier profile, which contained the information he needed to begin the registration process. A254. Spitler concluded that he could access the registration page by typing the following into the URL:

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

A254-55; A727. The string of Xs represents the unique 19 or 20 digit ICC-ID associated with an iPad SIM card.

Spitler typed his ICC-ID and all of the other required information into the URL, and when he sent the command, it still did not work. A255. Spitler then tried using an iPad simulator and a software development key to attempt to uncover the source of the problem. A255-56. Spitler concluded that he would need to change the "user agent"[3] on his web browser in order to "spoof"[4] the AT&T server. A255-57. Spitler changed the user agent to identify his computer as an iPad when communicating with the AT&T server. A257. After doing all of

---

[3] When a computer contacts a server over the internet, the "user agent" string identifies for the server the operating system of the web browser in the user's system. A256; *see also* http://en.wikipedia.org/wiki/User_agent ("In HTTP, the User-Agent string is often used for content negotiation, where the origin server selects suitable content or operating parameters for the response.").

[4] "Spoofing" is, as the name implies, providing or reporting an identity that you know is not your own. A410-11.

that, Spitler was able to register his SIM card with AT&T, and begin using his $30 per month unlimited data plan on his non-iPad devices.

Spitler Discovers A Security Flaw in AT&T's Database

After Spitler successfully registered with AT&T and purchased his data plan, he still needed to log in through the AT&T servers when he wanted to use AT&T's 3G network on his non-iPad device. Spitler noticed that when he typed his ICC-ID into the URL in order to access the iPad login page, the email address that he had registered with AT&T automatically appeared. A257-58. Spitler concluded, correctly, that this was a potential security flaw in the AT&T system that he could exploit.

When an actual iPad 3G user would go to the AT&T 3G login page, she too would see her email address appear. That is because the AT&T server had the ability to identify the unique ICC-ID associated with each particular iPad. Unlike Spitler, a true iPad user would never have to type an ICC-ID into a URL; rather, the AT&T server would: (1) automatically recognize her device as an iPad, and (2) recognize the particular iPad she was using by automatically recognizing its ICC-ID. After recognizing the user's unique ICC-ID, AT&T would pre-populate the user's login page with her email address, and ask her only for her password.

Logging in to AT&T's 3G network from an actual iPad was easy, as it was meant to be. A217, A259, A411.

Because Spitler was not using an actual iPad when he was logging in, he was not able to gain access to the AT&T 3G network in the simple and easy way that AT&T expected would be used. Spitler could gain access to the login page only by spoofing the system into thinking he was using an iPad, and then manually entering his 19 or 20 digit ICC-ID, along with various other additional information, into a long and complicated URL. Because Spitler discovered how to do all of this manually, he concluded that he could use the same method to enter other people's unique ICC-IDs, and by pretending to be them when interacting with AT&T's server, he could learn their corresponding email addresses. A257-58.

The iPad 3G Account Slurper Exploits The Security Flaw

Spitler tested his theory about accessing ATT&T's database to discover other people's email addresses by changing the ICC-ID portion of the entry he made on the URL. A258. Spitler entered the ICC-ID that was one digit higher than his, and it returned someone else's email address. A258. Spitler tried this a few times, with different ICC-ID numbers, and he discovered additional email addresses. A259-60.

Spitler discussed this security flaw in the ATT&T email database with his compatriots at Goatse Security using their chat room. A260. Spitler wrote a program, which he called an "iPad 3G Account Slurper," SA146-47, which automated the process of checking different ICC-IDs to discover more associated email addresses. A260-61. One of the steps in the program, which he labeled "Spoof as iPad," changed the user agent to mimic an iPad, without which he would not have been able to access the iPad email database in AT&T's servers. A261-62; SA146-47. Spitler's program began with a root ICC-ID, and it changed that root sequentially, both up and down, inputting new ICC-IDs into the URL, and thereby searching for new email addresses associated with each ICC-ID. A263. This is commonly known as a "brute force" attack on a server. A471.

Auernheimer Assists Spitler In Exploiting The Security Flaw

When Spitler began running his Account Slurper program, he encountered some initial problems, and he sought Auernheimer's help through Goatse Security's chat room. A266-67. Spitler told Auernheimer that "I'm in a rut. I got just under 200, but can't find any more." A267; SA148. The two conspirators discussed the problem that Spitler was having, and Auernheimer offered ideas and technical advice about how to overcome those problems. A267-70; SA148-50. With the help of Auernheimer and another Goatse Security member, Spitler was

able to overcome his technical difficulties, and from June 4, 2010, through June 8, 2010, his brute force attack on AT&T's database retrieved approximately 114,000 email addresses and their associated ICC-IDs. A267-70; A283.

Spitler knew for certain that AT&T did not want him to have the email addresses that he was gathering from its database. A264, A318. Spitler changed the user agent in his Account Slurper program in order to trick the servers into thinking that he was using an iPad. A264. He "lied to the AT&T servers" in order to get the information. A264. Spitler gathered this information without asking for permission from AT&T or from any of the iPad users that he was impersonating. A264-65. AT&T did not design its system to allow these email addresses to be made public. A218, A470-71.

Auernheimer Distributes The Stolen E-Mail Addresses

While Spitler was in the process of obtaining 114,000 email addresses from the AT&T database, he and Auernheimer traded messages about what they would do with the data they were collecting. Auernheimer urged Spitler to collect as many email addresses as he could, suggesting that they could publicize their exploit through Gawker, which is an internet news media website. A271-73. Auernheimer asked Spitler to focus on email addresses for iPad owners in the news media industry. A274. Auernheimer suggested that they could generate great

publicity for themselves by contacting reporters and saying, in essence, "Hi, I stole your e-mail from AT&T. Want to know how?" A275; SA152.

On June 7, 2010, Auernheimer contacted numerous individuals in the media industry via email in order to publicize what he described as his theft of their identification information from AT&T. SA142-45. For example, Auernheimer sent an email to nine iPad owners at Reuters, which read as follows:

> Hello Reuters!
>
> An information leak on AT&T's network allows *severe privacy violations* to iPad 3G users. Your iPad's unique network identifiers were pulled straight out of AT&T's database.
>
> Every GSM device (including 3G iPads), has an ICC-ID on its SIM card. This ICC-ID is a unique identifier to the cellular network that is used by the carrier to route calls to your cellphone. If this ICC-ID is compromised an attacker could theoretically (thanks to recent cryptanalysis that cracked GSM's hash and stream functions) clone your SIM card to act as you on the AT&T network.
>
> * * *
>
> [B]y harvesting ICC-IDs, an attacker can build a complete list of contact information for all iPad 3G customers. All these Thomson Reuters employees were revealed in a short data harvest by my working group along with hundreds of thousands of other iPad 3G customers.
>
> If anyone in your organization would like to discuss this particular issue for publication I would be absolutely happy to describe *the method of theft* in more detail.

SA145 (emphasis added). Similar emails were sent to others in the media. *See, e.g.*, A164-75.

Some of the victims who received Auernheimer's email contacted AT&T about the security breach, which AT&T was able to close quickly. A218. On June 8, 2010, Spitler informed Auernheimer "game over, AT&T changed the site." SA158. Spitler told Auernheimer that he had collected 114,067 email/ICC-ID combinations. *Id.* In response to Auernheimer's request, Spitler sent Auernheimer the whole list of email addresses and ICC-ID combinations. SA159; A283-85.

Auernheimer informed Spitler that he was going to send the list to valleywag, which was a part of Gawker. SA159; A271, A284. Auernheimer sent the list to Ryan Tate at Gawker, A286-88, SA161, and Auernheimer informed Spitler that, "I think valleywag is gonna publish it in the near future," SA160. Auernheimer also told Spitler that he was going to inform AT&T of their security problem, but he did not. A288-89.

On June 9, 2010, Gawker published an article about the hack, which was quickly picked up by other news sources such as Google News and the Drudge Report. SA127. After reading the Gawker article, Spitler was concerned about a discrepancy in the reporting. SA163. Gawker was reporting that "Goatse Security notified AT&T of the breach," SA132, but AT&T claimed that Goatse Security

never notified them of the problem, SA163. Another Goatse Security member asked Auernheimer: "you DID call tech support [at AT&T] right?" SA164. Auernheimer replied "totally, but not really, lol [laughing out loud], I don't f**kin care, I hope they sue me." SA164.

Auernheimer knew that his failure to inform AT&T of the security problem was a breach of the code of ethics practiced by so-called "white hat" hackers. SA165. Auernheimer acknowledged that the "whitehats are angry cause i violated their precious disclosure rules by going to a dotcom gossip rag." SA165. Rather, than trying to fix a problem on the internet, Auernheimer was intent on profiting from it. A318, A390. Auernheimer wanted to use the publicity he generated from disclosing this information to "aggressively direct market" Goatse Security to other companies. SA166. *See also* A318.

Auernheimer Attempts To Cover His Tracks

On June 15, 2010, FBI agents went to Auernheimer's residence in Fayetteville, Arkansas, with a search warrant. A185. When the agents entered Auernheimer's bedroom, they found an Apple laptop computer that was open and running a command designed to erase the computer's hard drive. A188. An agent entered a command to stop that process, and the FBI confiscated the laptop. A188-89. When questioned about the attempted erasure of the data, Auernheimer told

the FBI agents that he did not want anything on his computer to implicate himself and others. A189.

STATEMENT OF THE CASE

On August 16, 2012, a grand jury sitting in Newark, New Jersey, returned a two count superseding indictment charging Auernheimer with conspiracy to access a computer without authorization in violation of 18 U.S.C. § 371, and fraud in connection with personal information in violation of 18 U.S.C. § 1028(a)(7). A2-17. On September 21, 2012, Auernheimer filed a motion to dismiss the superseding indictment. A59-81. The District Court held a hearing on October 25, 2012, SA1-44, and issued an opinion and order denying the motion the next day, A18-29. Auernheimer's jury trial commenced on November 13, 2012, and on November 20, 2012, the jury returned a guilty verdict on both counts. A42-43.

The District Court held Auernheimer's sentencing hearing on March 18, 2013. The principal point of contention at the hearing was the amount of loss sustained by AT&T. A762. The Court found that Auernheimer was responsible for a loss of $73,167, which resulted in an eight-level increase in his total offense level. A770-71, A786. With a total offense level of 20 and Criminal History Category I, Auernheimer had an advisory Sentencing Guidelines range of 33 to 41

months. A782-83. Auernheimer addressed the Court prior to sentencing, but he did not help his cause in doing so. Auernheimer did not accept responsibility for his crimes, nor did he seek the Court's mercy. Instead, he lectured and scolded Judge Wigenton:

> I don't come here today to ask for forgiveness. I'm hear to tell this Court, if it has any foresight at all, that it should be thinking about what it can do to make amends to me for the harm and the violence that has been inflicted upon my life. . . . I respectfully say that this Court's decision is wrong. And if you people understood what you were doing with the rule of law and the Constitution, you would feel shame.

A773-74.

The District Court considered the sentencing factors contained in 18 U.S.C. § 3553(a), and imposed a top of the Guidelines sentence of 41 months' imprisonment. A782-86. On March 21, 2013, Auernheimer filed his notice of appeal. A1.

SUMMARY OF ARGUMENT

The heart of Auernheimer's claim at trial was, and on appeal is, that AT&T made the email/ICC-ID pairings for its iPad subscribers "publicly available" to everyone. The jury disagreed, and rightly so. Spitler obtained the email addresses from AT&T's servers only by impersonating other authorized users. AT&T took steps that were designed to publish individual e-mail addresses only to the individual iPad user who had pre-registered that address with the company. AT&T's security was not as good as it should have been, but it was not non-existent. This information was not accessible to anyone who was not a reasonably sophisticated hacker, as Spitler was. Spitler, with Auernheimer's assistance, exploited a security flaw, and both of them knew it. Spitler readily conceded that, when he was hacking the AT&T servers, he knew that his actions were not authorized by AT&T or the iPad users he impersonated. And Auernheimer revealed his own knowledge that their appropriation of this information was unauthorized when he described it repeatedly as "theft." This was not a close case, and the jury verdict reflected the overwhelming evidence of Auernheimer's guilt.

Auernheimer's contention that he should have been convicted of, at most, a misdemeanor violation of the CFAA, rather than a felony violation, is without merit. Simply accessing a computer, without more, is a misdemeanor. But the

conspirators here did more than that. After they accessed AT&T's server and obtained information from it, they transferred that information to another person, in violation of a New Jersey privacy statute. That additional step properly turned the misdemeanor into a felony. And, contrary to Auernheimer's contention, the record amply supported the jury's implicit finding that the conspirators violated code-based restrictions when accessing AT&T's servers – Spitler changed the user agent on his computer and entered ICC-IDs that were associated with other authorized users. The felony conviction was proper.

Auernheimer argues, for the first time on appeal, that his conviction on Count Two for identity fraud must be overturned because he did not possess or transfer e-mail addresses "in connection with" another distinct and separate crime, which he claims the statute, 18 U.S.C. § 1028, requires. There was no plain error here for two reasons. First, the evidence showed that the conspirators used a means of identification – the ICC-IDs – with the intent to commit the crime of unauthorized access of a computer. That is all the statute requires. Second, even if Auernheimer is correct that the statute requires the Government to prove two different kinds of unlawfulness, it did so. The conspirators violated the CFAA through their unlawful acquisition of individuals' means of identification, and then

they violated New Jersey's privacy law by unlawfully transferring that information to another person.

Venue is proper in the District of New Jersey for both counts. Both charges had "crucial elements" whose proof concerned New Jersey. First, the Government had to prove that the conspiratorial scheme involved a violation of the New Jersey law protecting the disclosure of personal identifying information, which made the existence of New Jersey victims a crucial element of the CFAA conspiracy count. Second, the conspirators failed to obtain authorization from the more than 4,500 victims located in New Jersey before using their ICC-IDs to access the server, and obtaining access without authorization was a crucial element of both counts. Additionally, under the broader "substantial contacts" test that this Court applies, venue can be based on the location of the effects of the crime, which would include the victims' District of residence. Venue is also proper in New Jersey because both offenses continued in New Jersey, where the Gawker article that published some of the stolen personal identifying information could be and indeed was accessed. Auernheimer, who caused that publication, is responsible for its consequences. Finally, even if venue were lacking for the CFAA offense, it was still proper for the identity fraud charge because the "essential nature" of identity fraud is the improper adoption by a defendant of another person's identity, which

is a highly victim-based crime. Thousands of those victims lived in the District of New Jersey, so venue was proper there.

Finally, Auernheimer's challenge to the District Court's award of an eight-level sentencing enhancement, base on a finding of a $73,167 loss amount, is without merit. The Court properly concluded, as a matter of law, that Guidelines loss for a computer crime can include reasonable expenditures undertaken by a company to notify its customers of a security breach. And the Court was not clearly erroneous in finding that AT&T's decision here to notify the victims by mail was reasonable under the circumstances.

ARGUMENT

I. THE GOVERNMENT PRESENTED SUFFICIENT EVIDENCE TO PERMIT THE JURY TO FIND THAT THE CONSPIRATORS' ACCESSING OF AT&T'S SERVERS WAS UNAUTHORIZED.

Standard of Review: plenary review over challenges to the sufficiency of the evidence. *U.S. v. Taftsiou*, 144 F.3d 287, 290 (3d Cir. 1998).

Auernheimer argues that he did not violate the CFAA because the conspirators collected the e-mail/ICC-ID pairings by visiting what he claims were unprotected public web pages. Thus, he concludes that the conspirators' access to AT&T's server was "authorized." Auernheimer is wrong. AT&T's server was not unprotected and openly available to the public. Bad or inadequate protection is not the same as no protection. Spitler had to impersonate registered users when he accessed AT&T's database, and he knew he was not authorized to do that. Moreover, Spitler violated code-based restrictions when accessing the AT&T server by changing his "user agent" to pretend he was using an iPad in order to access the server and entering other people's ICC-IDs. What Spitler did, with Auernheimer's assistance, was "hacking" as that term is commonly understood, not merely visiting a publicly-accessible web page.

Importantly, Auernheimer has not challenged the jury instructions given by the District Court. Instead, Auernheimer has raised only a sufficiency of the

evidence claim. *See* DB2-3 (issue presented as a sufficiency claim). In *Jackson v. Virginia*, 443 U.S. 307 (1979), the Supreme Court set forth the standard for reviewing the sufficiency of the evidence in a criminal case:

> [T]he critical inquiry on review of the sufficiency of the evidence to support a criminal conviction must be . . . to determine whether the record evidence could reasonably support a finding of guilt beyond a reasonable doubt. But this inquiry does not require a court to "ask itself whether it believes that the evidence at the trial established guilt beyond a reasonable doubt." Instead, the relevant question is whether, after viewing the evidence in the light most favorable to the prosecution, <u>any</u> rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.

443 U.S. at 318-19 (emphasis by Court; citations omitted). The evidence must be "viewed in the light most favorable to the government," *Burks v. U.S.*, 437 U.S. 1, 16- 17 (1978), "draw[ing] all reasonable inferences in favor of the jury's verdict," *U.S. v. Anderskow*, 88 F.3d 245, 251 (3d Cir. 1996).

This Court should reject Auernheimer's sufficiency challenge because there was abundant evidence to support the jury's guilty verdict. The evidence demonstrated that AT&T did not design its system to make the e-mail addresses in its database available to the public at large, but instead designed it to make the e-mail addresses available only to the individual iPad user who had himself provided that information to AT&T during the registration process. AT&T's security precautions were inadequate, and Auernheimer and Spitler exploited for their own

purposes the security flaw they discovered. The jury was entitled to find, as they did, that the conspirators' accessing of the AT&T servers was unauthorized.

The Jury Instructions

The jury instructions, to which there is no objection on appeal, set out the relevant legal standards. As to Count One, the Government had to prove, among other things, that Auernheimer joined the conspiracy, knowing and intending to achieve its objective, which was "to access computers without authorization and to disclose data from that unlawful access." A697. To prove the conspiracy charged in Count One, the Government had to prove not only the essential elements of conspiracy law, A697, but also an agreement to violate the elements of 18 U.S.C. § 1030(a)(2)(C), governing unauthorized access to computers, A703-04, and N.J.S.A. 2C:20-31, governing disclosure of data from wrongful computer access, A704-06.

In regard to a § 1030(a)(2)(C) substantive offense, the District Court instructed the jury that a violation of the CFAA required, among other things, a finding that "the defendant *intentionally* accessed without authorization or exceeded authorized access to a computer." A703-04 (emphasis added). The Court defined the "authorization" component as follows:

> To access without authorization is to access a computer without approval or permission. The 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 to obtain or alter.

A704. This definition comports with the contemporary meaning of the terms and is not challenged on appeal.[5] *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir. 2009) (similarly defining "without authorization" using its ordinary common meaning).

The Court further instructed the jury that the Government had to prove that Auernheimer "engaged in the conduct of intentionally accessing a computer without authorization or in excess of authorization to assist in, promote, accomplish, advance or achieve a violation of New Jersey statute 2C:20-31." A704-05. In regard to the violation of the New Jersey disclosure statute, the Court was more specific in defining "authorization," charging as follows:

> Authorization means permission, authority or consent given by a person who possess [sic] lawful authority to grant such permission, authority or consent to another person to access, operate, use, obtain, take, copy, alter, damage, or destroy a computer, computer network, computer system, computer equipment, computer software, computer program, computer storage medium or data. This element is met if a reasonable person would know that he or she lacked authorization or exceeded authorization.

---

[5] The CFAA does not define "without authorization," but it does define "exceeds authorized access." *See* 18 U.S.C. § 1030(e)(5)

* * *

> "Access without authorization" means access *without password-based permission or code-based permission, or in violation of a code-based restriction by impersonating an authorized user*."

A705-06 (emphasis added).

Because the Government charged a conspiracy to disclose data in violation of the CFAA and New Jersey law, the Government had to prove the relevant components of both 18 U.S.C. § 1030(a)(2)(C) and N.J.S.A. § 2C:20-31. By finding Auernheimer guilty, the jury necessarily found that the conspiracy involved an agreement to violate a code-based restriction and/or impersonate an authorized user. A706.

A. The Evidence Overwhelmingly Supported A Jury Finding That The Conspirators Improperly Accessed AT&T's Computers By Impersonating Authorized Users.

The jury was entitled to find that, as part of the conspiracy, Spitler improperly accessed AT&T's computers by impersonating authorized users. Indeed, the underlying facts are largely undisputed. Auernheimer simply disagrees with the reasonable inferences that the jury could draw from the undisputed facts.

The login page for iPad access, as designed by Apple, required both an email address and a password. A405. AT&T decided that, for the convenience of its customers, it would allow iPad users to log in to its 3G network by entering a

password only. A217-19, A226, A408-09. AT&T was able to do this because authorized users of its network had pre-registered their iPads, which required the users to disclose, among other things, their e-mail addresses and billing information. A216. AT&T's system was able to automatically recognize the unique 19 to 20 digit ICC-ID of individual iPads seeking access to its servers, and AT&T opted to pre-populate the login page with the particular e-mail address associated with the particular iPad seeking access to the network. A217-19, A226, A408-09. This was done to allow users to access the 3G network quickly. A217-19, A226, A408-09. AT&T did not design its system to publish e-mail addresses to the public at large. A214, A221. Rather, it took steps that were designed to publish an e-mail address to only the particular user of the iPad whose owner had himself given that information to AT&T. A410, A470-71, A473.

Spitler impersonated 114,000 authorized users when he used the account slurper program to gather paired e-mail/ICC-ID information from AT&T's network. This impersonation was accomplished in two steps. First, by changing the "user agent," he pretended he was accessing the server from an iPad, when he was not. A471. Second, he provided the unique ICC-ID number for iPads that were not his when accessing the server. A471-72. The jury was entitled to find, based on undisputed underlying facts, that Spitler impersonated 114,000 authorized

users to obtain information about each user that AT&T had designed its system to share only with each of the 114,000 individuals he impersonated. As the jury instructions make clear, "impersonating an authorized user" is "access without authorization." A706.

Spitler admitted on the witness stand that he knew that he was not authorized by AT&T or the users to obtain this information. A264, A318. Auernheimer certainly knew this as well. When Auernheimer described the gathering of this information he called it "theft."[6] A166-75. All of Auernheimer's conversations with Spitler and others indicate that he knew they were exploiting a security flaw in AT&T's system. *See, e.g.*, SA150-52, SA158. Auernheimer helped Spitler overcome technical problems Spitler was having when Spitler tried to hack into AT&T's servers. A266-70, A283; SA148-49. When the FBI came looking for Auernheimer, he tried to delete the incriminating information on one of his hard drives. A185-89. Certainly the jury was entitled to conclude that Auernheimer knew that he and Spitler were not authorized to access AT&T's servers.

[6] The Government agrees with Auernheimer that simply calling something "theft" does not necessarily make it so. DB28. Nevertheless, Auernheimer's calling this "theft" indicates his state of mind when he was committing the crime. A violation of the CFAA requires the Government to prove intentional misconduct, and Auernheimer's own words manifested that intent.

B. The E-mail/ICC-ID Pairings On AT&T's Server Were Neither Unprotected, Nor Open To The Public.

Auernheimer asserts that the e-mail/ICC-ID pairings on AT&T's servers were unprotected and open to the general public. This was a factual contention that the jury was entitled to accept or reject, not a legal conclusion. The evidence at trial permitted a reasonable jury to find that the e-mail/ICC-ID pairings were neither unprotected, nor open to the public.

There was no search on Google, Bing, or any other search engine that a person could enter that would return the e-mail/ICC-ID pairings. Likewise, there was no link on any AT&T webpage that could be clicked on to return this information. No one could have stumbled upon this information inadvertently. Members of the general public who lacked expertise in reading and manipulating computer code could not have gained access to this information. Indeed, it was not easy for Spitler, an experienced computer hacker, to obtain this information from AT&T's servers.

The complicated steps that Spitler had to take to access the e-mail/ICC-ID pairings on the AT&T server support the jury's factual conclusion that Spitler's use of the server was unauthorized. When Spitler purchased a replacement SIM card for an iPad and put it in his modem, it did not work. A251-52. Because he

did not own an iPad, Spitler could not find any direct or easy way to register his SIM card online, so he tried downloading the entire iPad IOS operating system onto his computer. A253. After downloading the operating system, Spitler discovered that it was encrypted, and he had to find the encryption key and decrypt the firmware image before he could continue. A253. After that, Spitler had to scour the operating system to find a way to access the registration page. A254. Spitler eventually was able to find a URL for registering his SIM card. A254-55. But when Spitler entered his ICC-ID into the URL, it still did not work. A255. Spitler next tried using an iPad simulator, including the software development key, to try to get the modem to work with his SIM card. A255. Through this process, Spitler learned that an iPad could access the AT&T server's registration website, but a different type of computer could not. A256. So Spitler changed the user agent on his system to pretend he was using an iPad. A256-57. After spoofing the user agent, Spitler was then able to access AT&T's server by typing the following obscure line into the URL, substituting his ICC-ID number for the Xs below:

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

A254-55; A727. That was the complicated process that Spitler had to follow in order to access AT&T's server and begin his brute force attack, which retrieved

additional e-mail/ICC-ID pairings. What Spitler did, in common parlance, was "hack" into AT&T's servers.[7] And even after the successful initial hack, Spitler needed help from Auernheimer and others at Goatse security to retrieve the full 114,000 e-mail/ICC-ID pairings. A266-70, A283; SA148-50.

Obtaining the ICC-ID/email combinations required purposeful action by a determined individual with computer expertise. This information was not made available by AT&T to the general public. The jury was entitled to conclude, as Spitler himself concluded, *see* A264, A318, that AT&T had not made this information publicly available, and the conspirators' access of this information was unauthorized.

Contrary to Auernheimer's contention, this case is nothing like *Pulte Homes, Inc. v. Laborers' Intern. Union*, 648 F.3d 295 (6th Cir. 2011). That case, which arose from an employment dispute between a home builder and a labor union, stands for the unremarkable proposition that a union's campaign to make telephone calls and send e-mails to a company's business executives does not constitute accessing the company's computers "without authorization" in violation of the CFAA, even if the volume of calls and e-mails was purposefully designed to

[7] "In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network." *See* http://en.wikipedia.org/wiki/Hacker_(computer_security).

overwhelm the company's computer system.[8] The facts in *Pulte Homes* are nothing like the facts in this case. The campaign against Pulte Homes involved the union's use of publicly available telephone numbers and e-mail addresses to contact business executives at the company. No one in the union needed any expertise, like Spitler and Auerheimer had, to carry out the computer "attack" against Pulte Homes, which was based simply on the volume of calls and e-mails sent. The actions taken by Spitler and Auernheimer, in contrast, required computer expertise to impersonate authorized users by exploiting flaws in the access controls to AT&T's servers. The two cases have nothing in common.

Auernheimer also relies on *EF Cultural Travel BV v. Zefer Corporation*, 318 F.3d 58 (1st Cir. 2003), but that case does not support his legal contentions either. EF Cultural Travel BV ("EF") and Explorica, Inc. were two competitors in the student travel business. *Id.* at 60. Explorica hired a computer company, Zefer Corporation, to build a scraper to collect two years of pricing data from EF's website, intending to use the data to try to undercut EF's prices and thereby gain customers. *Id.* "A scraper, also called a 'robot' or 'bot,' is nothing more than a

[8] *Pulte Homes* did not decide whether such a scheme could constitute "exceeding authorization" in violation of the CFAA because, as the Court pointedly noted, the complaint did not contain that allegation.

computer program that access information contained in a succession of webpages stored on the accessed computer." 318 F.3d at 60.

EF sued Explorica and Zefer, alleging, among other things, a violation of the CFAA. The District Court granted EF a preliminary injunction, finding that Zefer's use of the scraper exceeded its authorized access because it went beyond EF's "reasonable expectations" of the use of its website. *Id.* at 62. The First Circuit disagreed and criticized the "reasonable expectations" standard. The First Circuit held that, if EF did not want others to use scrapers, it simply should have said so on its website. *Id.* at 63. The Court noted that although EF no doubt disliked the use of the scraper, it likewise would have disliked the compilation of the information manually. *Id.* at 63. "EF did not purport to exclude competitors from looking at its website and any such limitation would raise serious public policy concerns." *Id.* at 63. Businesses in competition with each other certainly are permitted to compare prices advertised to the public.

EF's website, of course, was freely open to the public, who used it to find prices and book travel. To access the website, Zefer's program presumably did not have to pretend to be anyone else. Zefer was not trying to obtain information linked to any individual user; rather, it wanted the freely available pricing information that anyone could have obtained. The First Circuit held,

unsurprisingly, that writing a "bot" or program to obtain publicly available information more efficiently was not a crime under the CFAA.

The scraper program that Spitler wrote was very different from the one written by Zefer for Explorica. Each web page accessed by Zefer's program reflected the publicly-available price of a different publicly-available tour. AT&T, in contrast, designed its login page, which propagated an e-mail address, to be readily accessible only to a single individual, *i.e.*, the individual whose unique ICC-ID was automatically recognized by the server. A410, A470-71, A473. While Zefer's program simply automated a process that could have been done by any member of the public with the time and patience to ask repeatedly for the publicly-available information, Spitler's scraper program, in contrast, successfully gained non-public information by sequentially *impersonating* unique users who had pre-registered with AT&T, and gaining information that *the users* had provided to AT&T.

The record is abundantly clear that the e-mail/ICC-ID pairings obtained by the conspirators could not have been obtained by anyone other than a skilled and determined computer hacker. If an ordinary, but reasonably sophisticated computer user, like a typical judicial law clerk, had been assigned the task of compiling a list of e-mail addresses of iPad users available on AT&T's servers, he

almost certainly would not have been able to duplicate what Spitler did. The law clerk would likely go to AT&T's website and search in vain for any links or other means to access this information. No hyperlinks or search engine requests would have produced the desired results. Indeed, the only reason that Spitler discovered the way to access this information was because he was trying to do something else improper, *i.e.*, to gain access to AT&T's $30 per month unlimited data plan for a device that was not eligible for that service. Only in the course of doing that unrelated hack, did Spitler discover the flaw in AT&T's security system that would reveal the e-mail addresses of authorized iPad users. So even discovering the security flaw, not to mention exploiting it, required a level of sophistication unavailable to the vast majority of internet users. The jury was entitled to find that this information was not publicly available.

C. It Is Not A Bar To Prosecution Under The CFAA That The Victim Employed Bad Security.

Auernheimer states that "[i]t would be different if AT&T had protected its data with a password." DB22. Actually, what Auernheimer is attempting to do here is not provide an example, but instead to prescribe the particular security measures that AT&T and others must take before criminal liability can be imposed for unauthorized access into their computer systems. But that is not the way that

criminal law generally works, and there is no reason for this Court to impose the particular security requirements suggested by Auernheimer or the *amici* as prerequisites to liability under the CFAA.

When a teenager brings his bicycle to school and leaves it unlocked in front of the school, an individual who takes the bicycle clearly has committed theft, even though the bicycle was left unsecured. Similarly, a trespass occurs when an unauthorized person enters someone else's residence, even when the front door is left open or unlocked. The absence of adequate security is not a defense to a crime, although it may affect the degree of the crime or the severity of the sentence imposed.

Likewise, in using computers, people commit security lapses all the time. If a government employee, after properly signing in to her account, leaves her workstation unattended without logging out, that does not authorize the office's cleaning person to access her computer and start entering search requests for classified government information or even search requests for the government employee's personal e-mails. The government employee almost certainly failed to comply with proper security procedures by leaving her computer unattended, but the knowing and purposeful exploitation of that security breach by the cleaning

person could be prosecuted as a violation of the CFAA because the access was unauthorized and any reasonable person would know that.[9]

As the above example demonstrates, a person can improperly access a computer without violating a code-based restriction or without using someone else's password. There are norms of behavior that are generally recognized by society, and violating those norms of behavior – by taking unattended property or accessing a computer without authorization – can constitute a crime. *See U.S. v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (authorization is "typically analyzed on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user"); *U.S. v. Morris,* 928 F.2d 504, 510 (2d Cir. 1991) (defendant committed unauthorized access where he "did not use [certain computer] features in any way related to their intended function"). The jury here was required to determine whether a "reasonable person" would have known that the conspirators' accessing AT&T's computer server here was

[9] The same would be true for an unsophisticated computer user who connects to the internet without using a firewall or establishes a wireless network at home, but does not secure that network. In either instance, wrongdoers easily could access information on the user's computer, but only Auernheimer would argue that this access was therefore "authorized" and not a violation of the CFAA.

unauthorized. The Government was required to prove this beyond a reasonable doubt. That was not a difficult or close question here.

Auernheimer cites *Snow v. DirecTV, Inc*., 450 F.3d 1314 (11th Cir. 2006), which interprets an analogous unauthorized access statute, the Stored Communications Act ("SCA"), codified at 18 U.S.C. § 2701 *et seq*., for the proposition that protection should not be afforded to systems that are not adequately protected. DB27. But *Snow* is easily distinguishable from this case, and its reasoning undermines, rather than advances, Auernheimer's arguments.

The SCA was part of the Electronic Communications Privacy Act of 1986 ("ECPA"), which was enacted "to update the then existing federal wiretapping law to protect the privacy of the growing number of electronic communications." 450 F.3d at 1320. Snow brought an action under the SCA against DirecTV, alleging that DirecTV's employees accessed his website's electronic bulletin board without authorization. The District Court dismissed the action for failure to state a claim, and the Eleventh Circuit affirmed that dismissal.

Under the ECPA's express statutory provisions, it is not unlawful to intercept or access an electronic communication that is "readily accessible to the general public." 450 F.3d at 1320 (*quoting* 18 U.S.C. § 2511(2)(g)). Members of the public could access Snow's electronic bulletin board by simply going to his

website, registering, creating a password, and agreeing to the terms of use. 450 F.3d at 1321. Therefore, the Eleventh Circuit had no difficulty concluding that the bulletin board was open to the general public, and Snow had not stated a claim under the SCA.

In reaching this conclusion, however, the Eleventh Circuit noted that its reasoning was fully compatible with *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), a case with facts more directly analogous to what occurred here. As *Snow* explained:

> In *Konop*, plaintiff Konop created a list of Hawaiian Airlines employees who were eligible to access the website. *Id.* at 872. To gain access, one had to enter an eligible employee's name, create a password, and click "SUBMIT" indicating acceptance of the terms and conditions, which prohibited users from disclosing the website's contents and prohibited viewing by Hawaiian Airlines management. *Id.* at 872-73. In contrast, Snow alleged that registrants needed only to create a password and acknowledge that they were not associated with DirecTV or another prohibited entity. *Konop's website, unlike Snow's, required users wishing to view the electronic Bulletin board's contents to have knowledge (an eligible employee's name) that was not publicly available.* Snow had no such limitation. In order to be protected by the SCA, an Internet website must be configured in some way so as to limit ready access by the general public.

450 F.3d at 1322 (emphasis added). Here, in direct analogy to *Konop*, the conspirators had to have knowledge that was not publicly available to access AT&T's servers, *i.e.*, an individual authorized user's ICC-ID. While employee

names or ICC-IDs could be researched or guessed by those trying to hack into the respective systems, they nevertheless were limits imposed by the website designers to restrict the general public's access to the information available there. That the restrictions were circumvented did not mean that the information was "publicly available."

Finally, the express language of the ECPA, which specifies that it is not unlawful to intercept or access an electronic communication that is "readily accessible to the general public," 18 U.S.C. § 2511(2)(g), demonstrates that Congress knows how to write such a limitation if that is what it intends. It is noteworthy that, for the CFAA, Congress chose to rely on lack of authorization rather than lack of accessibility, as a basis for liability.

D. Spitler's Use Of Individual User's ICC-IDs Is Not Fundamentally Different From Using Another Person's Password.

Auernheimer and the *amici* agree that accessing a computer by using someone else's password constitutes unauthorized access under the CFAA (unless the person who controlled access to the computer authorized that particular use). Auernheimer argues that "[b]y choosing not to protect the e-mail addresses with a password, AT&T authorized the public to view them." DB25. Likewise, MF argues that "[t]he ICC-ID is not a Password." MF Br.10. These two arguments are

mistaken. Here, Spitler's use of ICC-IDs was not fundamentally or functionally different from the misuse of other people's passwords.

The argument that the ICC-ID "is not a password," begs the question of what counts as a "password." Wikipedia defines a "password" as "a secret word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access." *See* http://en.wikipedia.org/wiki/Password. MK makes the facile argument that an ICC-ID is not a password because it is frequently printed on the outside of phone packaging, and thus is not secret. But that cannot be correct. Combinations to locks are often printed on the packaging, but the combination nevertheless is the secret "password" that opens the lock. Openness to the public prior to purchase is irrelevant, because after purchase the combination becomes the owner's secret. So too with an ICC-ID. Once a phone or other device using an ICC-ID is purchased, no one can easily learn the ICC-ID unless he or she actually possesses it.

An ICC-ID, unlike a password, is a unique identifier. In that regard, when it is used to gain access to a server, it can be even more secure than a password

chosen by a user, which frequently can be guessed.[10] Certainly a 19 or 20 digit ICC-ID is harder to guess using brute force than a typical four-digit ATM access code, misuse of which would certainly constitute a CFAA violation. In this case, the AT&T server automatically read the unique ICC-ID of the presumed iPad device accessing its website before providing the paired e-mail address information to the user. When Spitler pretended to be using an iPad and then manually entered another person's ICC-ID and other information into the URL, that allowed him to retrieve the other person's e-mail address. The ICC-ID was a "shared secret" between the user and the server, A327, which was part of the way that AT&T attempted to control access to its server.[11]

MF also notes that full access to an individual user's 3G network account required a traditional password, which the user had registered with AT&T. MF

---

[10] *See* The 25 Most Popular Passwords of 2012, *available at* http://gizmodo.com/5954372/the-25-most-popular-passwords-of-2012.

[11] MF also asserts that ICC-IDs are not secret because ICC-ID numbers on iPads are assigned sequentially and so "if you know any iPad number, you know every iPad number." MF Br.11. That argument is fallacious. What is secret is the identity of the particular device associated with a unique ICC-ID, not the range of available ICC-IDs. Social security numbers or bank account numbers can be assigned sequentially and still be secret. It is the use that is made of these identifying numbers, regardless of how they are assigned, that is relevant. Here, Spitler used the ICC-IDs to impersonate users on AT&T's servers and thereby gain access to each user's e-mail address. He did it sequentially, but each time he did it he was obtaining unauthorized information.

Br.10. That is true. But that does not negate the fact that the ICC-ID was a step in the process that AT&T utilized to verify the identity of individuals to whom it was providing server access, and that Spitler and Auernheimer misused that unique identifier in order to gain access. To simply assert that an ICC-ID is not a "password," or that the webpage was not "password protected" does not negate that using someone else's ICC-ID to gain access can make that entrance unauthorized. Certainly a jury was entitled to so find.

E. It Does Not Matter That The AT&T Server Responded As It Was Programmed To Do.

Auernheimer argues that "AT&T programmed its computer to respond to *anyone* who visited the correct address; it did exactly as it was programmed to do. Visiting a website does not carry an implicit promise that the visitor is someone the website owner would like them to be." DB29. But that cannot be the test. The issue is not whether an attacker violates an implicit promise, the issue is whether the victim network was accessed without authorization. When Jack goes to a computer and enters Jane's password, the computer responds exactly as it was programmed to do. It gives Jack access to Jane's information, but that is still unauthorized access. Here, Spitler wrote code that allowed him, through the use of carefully designed URLs, to "spoof" the iPads of actual iPad owners, such that

AT&T's servers were fooled into treating Spitler's accesses as though they were accesses by the true owners of the spoofed iPads. In other words, AT&T's servers were tricked into returning information that its system was designed to return only to the actual iPad owners, and only when they were accessing AT&T's servers through their iPads. Auernheimer's suggestion that this access was legal since AT&T's system was in fact responding to the URLs as it was designed to do, is as absurd as arguing that picking a lock to commit trespass is legal simply because the lock responded to a configuration of lock picks in the exact way that it was mechanically designed to respond.

More importantly, the suggestion by some of the *amici* that entering information in a URL cannot, by definition, constitute computer hacking would de-criminalize some of the worst computer hacking exploits ever prosecuted in this country. For example, Albert Gonzalez was the mastermind of a credit card theft ring responsible for reselling more than 170 million credit card and ATM numbers from 2005 through 2007, the largest such fraud in history. *See* http://en.wikipedia.org/wiki/Albert_Gonzalez. Gonzalez's ring used what is known as an SQL injection attack, which can be performed by entering an "address" in a URL or entering data in publicly facing web forms.[12] In many

[12] "SQL" stands for "structured language query."

common SQL injection attacks, the challenge for the hackers is to determine the correct characters to send to the network's database storing the data the attacker intends to exfiltrate. However, once the vulnerability is determined and the appropriate combination of characters is discovered, many SQL injection attacks can be reduced to a URL because malicious code entered into a form field in a website is often delivered to the victim's network from the attacker's computer in the form of a URL that includes within it the malicious string.

Spitler similarly modeled AT&T's system for authenticating users, then reduced the attack he found to be effective into a URL, which allowed him to write code or a script which sent more than 100,000 iterated versions of the URL to AT&T's servers in order to return information intended only for legitimate iPad owners accessing the server through their iPads. And the result of these attacks, like the result in SQL injections, is that the browser returns unauthorized data from a database. An SQL injection attack is among the most dangerous and notorious hacks used today, and any argument that suggests that entering information into a URL cannot be a computer hack would provide a safe haven for some behavior that Congress doubtless intended to criminalize. *See, generally,* OWASP Top 10 - 2013, "The Ten Most Critical Web Application Security Risks"

(listing injection attacks as the number one security risk in 2013), *available at* http://owasptop10.googlecode.com/files/OWASP Top 10 - 2013.pdf.

F. Neither This Prosecution, Nor the Government's Interpretation Of The CFAA, Threatens To Criminalize Innocent Web Surfing By Ordinary Internet Users.

Auernheimer asserts that, under the Government's theory, people who are merely surfing the web and visit a webpage might land in jail. DB27. Hardly. Under section 1030(a)(2)'s express language, no liability will be imposed for "access[ing] a computer without authorization or exceed[ing] authorized access" unless it was done "intentionally." 18 U.S.C. § 1030(a)(2). Indeed, Congress specifically amended § 1030(a)(2) in 1986 to change the scienter requirement from "knowingly" to "intentionally" because, in part, "intentional acts of unauthorized access – rather than mistaken, inadvertent, or careless ones – [we]re precisely what the Committee intend[ed] to proscribe." S. Rep. No. 99-432, at 3-4 (1986), available at 1986 WL 31918, at *3-*4. Congress expressly substituted the "intentional" standard "to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." *Id.* at *6. The statute is not a trap for the unwary, and the facts of this case certainly do not raise that problem. *See U.S. v. Moyer*, 674 F.3d 192, 211-12 (3d Cir. 2012) ("Scienter requirements in criminal statutes

alleviate vagueness concerns because a *mens rea* element makes it less likely that a defendant will be convicted for an action committed by mistake.") (internal quotes omitted).

G. The Rule Of Lenity Has No Application Here.

Auernheimer argues that if "authorization" is ambiguous, the rule of lenity requires that it be narrowly construed. DB31. But it is not clear what narrower interpretation Auernheimer claims the District Court should have adopted here. As already noted, the Court instructed the jury that, because the charges incorporated a violation of the New Jersey statute, they had to find "access without password-based permission or code-based permission, or in violation of a code-based restriction by impersonating an authorized user." A706. Auernheimer did not request any narrower jury instruction.

More importantly, as a matter of law, the term "authorization" is not ambiguous, and the rule of lenity therefore does not apply. While before the District Court, Auernheimer raised a vagueness claim in his motion to dismiss the indictment, and the Court properly rejected that claim, finding that the terms of the statute, especially as applied to the conduct alleged here, were not ambiguous. A21-23.

> The rule [of lenity] is not properly invoked simply because a statute requires consideration and interpretation to confirm its meaning. It applies only if there is such grievous ambiguity or uncertainty in a statute that, after seizing everything from which aid can be derived, the Court can make no more than a guess as to what Congress intended.

U.S. v. Kouevi, 698 F.3d 126, 138 (3d Cir. 2012); *see also Dean v. U.S.*, 556 U.S. 568, 577 (2009) ("The simple existence of some statutory ambiguity, however, is not sufficient to warrant application of the rule of lenity, for most statutes are ambiguous to some degree").

"A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning." *Perrin v. U.S.*, 444 U.S. 37, 42 (1979). As the District Court noted, the phrase "without authorization" in the CFAA has been construed by several courts "based on its ordinary, dictionary definition." A21 (citing cases). The phrase "without authorization" means "without permission" or "without approval." *See, e.g., WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204, 206 (4th Cir. 2012); *Pulte Homes*, 648 F.3d at 303-04; *LVRC Holdings LLC,* 581 F.3d at 1133. There is no doubt, grave or otherwise, that Congress intended the terms in the CFAA to be interpreted in this common sense, everyday manner. *See* S. Rep. No. 99-432, at 13 (1986), available at 1986 WL 31918, at *7 (commenting that the

term "exceeds authorized access," the definition of which includes "access[ing] a computer with authorization," is "self-explanatory").[13]

H. The "White Hat" Computer Hacking Community Has Nothing To Fear From This Prosecution.

The term "hacker" is "commonly used to refer to someone who can gain unauthorized access to other computers. A hacker can 'hack' his or her way through the security levels of a computer system of network."[14] Hacking need not be criminal. People who operate within the computer security community commonly distinguish between the "good guys," who are known as "white hats,"

---

[13] In his rule of lenity argument, Auernheimer cites *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*). There, the Ninth Circuit held that the phrase "exceeds authorized access" in the CFAA is limited to access restrictions, and does not cover a violation of private computer use policies, such as those adopted by employers for their employees' use of work computers for nonbusiness purposes. *But see U.S. v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (former SSA employee exceeded authorized access to database in violation of policy permitting access for official business reasons only); *U.S. v. John*, 597 F.3d 263, 272 (5th Cir. 2010) (violation of company's computer policy could constitute "exceeding authorized access"); *EF Cultural Travel BV*, 318 F.3d at 62, 64 ("lack of authorization could be established by an explicit statement on the website restricting access" or a violation of an employee confidentiality agreement). Putting aside whether *Nosal* is correct on this score, there is no allegation here that the conspirators' access to AT&T's servers was unauthorized because it was in violation of a contractual arrangement. Thus, there is no reason for this Court to address the split in the Circuits that *Nosal* creates in defining "exceeds authorized access."

[14] *See* http://www.techterms.com/definition/hacker.

and the "bad guys," who are known as "black hats." In general, "white hats" identify weaknesses in computer systems so they can be fixed, while "black hats" "violate computer security for personal gain (such as stealing credit card numbers or harvesting personal data for sale to identity thieves) or for pure maliciousness." "Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats," *available at* http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/. There is also an in-between group, of "gray hats."

> A black hat hacker would compromise a computer system without permission, stealing the data inside for their own personal gain or vandalizing the system. A white-hat hacker would ask permission before testing the system's security and alert the organization after compromising it. A gray-hat hacker might attempt to compromise a computer system without permission, informing the organization after the fact and allowing them to fix the problem. While the gray-hat hacker didn't use their access for bad purposes, they compromised a security system without permission, which is illegal.

Id.

MF argues that "researchers commonly use techniques *technologically* indistinguishable from Auernheimer's conduct in this case." MF Br.11 (emphasis added). That limitation is crucial. Voluntary firefighters commonly use techniques that are *physically* indistinguishable from those breaking and entering into your home. Intent, of course, often distinguishes what is criminal from what is legal. For example, state of mind is crucial in distinguishing assault from self

defense. Similarly, consent or authorization is crucial in distinguishing trespass from legally permissible entry. Here, Spitler and Auernheimer were prosecuted not simply for the technological steps they took, but also for taking those actions with full knowledge that their accessing of the AT&T computer servers was not authorized by the owner of the servers.

Indeed, the examples MF describes in arguing that this prosecution will chill legitimate security research fail to prove its case. MF cites, for example, research to fight malicious software on Android smartphones. MF Br.12-13. But the example, as described by MF, involved the downloading of free software applications from Google's Play store. *Id.* at 12. Nothing in this prosecution would remotely suggest that a researcher would need to fear prosecution under the CFAA as a result of downloading freely available software from an online store. AT&T was not operating a store that was designed to sell or give away e-mail information to the public. MF next cites the Wall Street Journal's investigation of online price discrimination. *Id.* at 13-14. But the investigation conducted there, as described by MF, again involved researchers investigating prices on a publicly

available website of a national chain store designed to sell its goods to the general public. Again, that is not remotely like this case.[15]

Although Auernheimer tried to present an image of himself to the jury as a "white hat" hacker who was motivated primarily by a desire to inform the public of AT&T's security breach, rather than by a desire for personal gain, the guilty verdict demonstrates that the jury rejected these claims, and it is not difficult to see why. All of Auernheimer's statements at the time of the crime refuted his self-serving trial testimony. For example, Auernheimer did not follow the "white hat" rule, or even the "gray hat" rule, of disclosing the security violation to the affected company. SA164. Indeed, he was "laughing out loud" about his transgressions in the Goatse Security chat room:

> lolllllll white hats are angry cause i violated their precious disclosure rules by going to a dotcom gossip rag

SA165. The chats clearly demonstrate that, rather than concern about the privacy of others, Auernheimer was motivated by a desire for personal gain. *See* A318-19, A390; SA166.

---

[15] MF also argues that reporters covering data privacy at Scripps News were threatened with a civil suit for purported violations of the CFAA by a private company that the reporters had investigated. MF Br.17. The Government is hardly responsible for every allegation made by a civil attorney seeking to intimidate a news organization. MF notes that the threat was disregarded by the reporters, and MF has not reported that any criminal or civil lawsuit was filed.

The groups of security researchers and computer professionals who have filed *amicus* briefs in this case need not be troubled by this prosecution of this black hat hacker. Major technology companies today – Microsoft, Google, Facebook, PayPal, and Mozilla, to name a few – all pay bounties to white hat hackers who find flaws in their systems and thereby help keep them secure.[16] The Government is not aware of any instance in which a security researcher who followed the rules of ethical hacking was prosecuted for violating the CFAA. Often, when a white hat hacker discovers and reports a security flaw, he is rewarded financially for his work by the company that he has hacked. But no one, not even a white hat hacker, gets to make his own rules.

[16] *See* The Washington Post, "Mark Zuckerberg's Facebook Page Was Hacked By An Unemployed Web Developer," August 19, 2013, *available at*: http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/19/mark-zuckerbergs-facebook-page-was-hacked-by-an-unemployed-web-developer/.

II. THE JURY PROPERLY CONVICTED AUERNHEIMER OF A FELONY VIOLATION OF THE CFAA.

Standard of Review: plenary review over challenges to the sufficiency of the evidence, *Taftsiou*, 144 F.3d at 290, and plain error review for arguments not raised below, *U.S. v. Olano*, 507 U.S. 725, 731 (1993).

Auernheimer advances several arguments that he contends require this Court to reduce his felony convictions to misdemeanors. First, he argues that the felony enhancement relied upon by the Government, *i.e.*, a violation of N.J.S.A. § 2C:20-31(a), was improper because it constituted impermissible "double-counting." Second, he argues that the Government did not bear its burden of proving a violation of the New Jersey statute. This latter argument has two parts. Auernheimer alleges that the Government failed to prove that the conspirators breached a "code-based" barrier when accessing AT&T's servers. He also argues that the conduct proven at trial occurred outside of the territorial reach of the New Jersey courts. None of these contentions has any merit.

A. The New Jersey Statute Is A Proper Felony Enhancer Because It Requires Proof Of An Additional Element – Distribution – That Is Not Required For A Misdemeanor Violation Of The CFAA.

A violation of 18 U.S.C. § 1030(a)(2) is ordinarily a misdemeanor, but it can be charged as a felony if the Government proves, as is relevant here, that "the offense was committed in furtherance of any criminal or tortious act in violation of

the . . . laws of . . . any State." 18 U.S.C. § 1030(c)(2)(B). The Government charged that Auernheimer's conspiracy involved a violation of the CFAA that was in furtherance of a violation of N.J.S.A. § 2C:20-31(a), which criminalizes the knowing or reckless disclosure of certain information obtained after improperly accessing a computer.[17] The District Court correctly found that this was a proper felony enhancer. A23-25.

The District Court noted that N.J.S.A. § 2C:20-31(a) has an additional required element that is not contained in 18 U.S.C. § 1030(a)(2), and that the Government was relying on factual allegations to prove the enhancement that were different from and in addition to the allegations necessary to prove the CFAA violation. A24-25. While both statutes require the Government to prove that the defendant obtained information after accessing a computer without authorization or in excess of authorization, the New Jersey statute requires, in addition, that the defendant disclosed or caused to be disclosed any data or personal identifying information so obtained. A24, A703-05.

---

[17] The statute 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, computers system and knowingly or recklessly discloses or causes to be disclosed any data, data base, computer software, computer programs or personal identifying information."

In short, to prove the CFAA *misdemeanor*, the Government was required to prove that the conspirators improperly accessed AT&T's computers and obtained data from it. To prove the CFAA *felony*, the Government was required to prove that the conspiracy was not only to obtain data from computers, but also to disclose improperly obtained personal data. To suggest, as Auernheimer does, that these are essentially the same crime, subjecting him to double punishment, simply ignores both the specific allegations and the facts proven at trial. If Auernheimer had not disclosed the personal identifying information of the victims, then the crime would have been only a misdemeanor. By taking that extra step, the crime was more significant, and it was properly elevated to felony status.

Auernheimer relies principally on *U.S. v. Cioni*, 649 F.3d 276 (4th Cir. 2011), but that case is inapposite. In *Cioni*, the Fourth Circuit held that the Government could not elevate a misdemeanor violation of 18 U.S.C. § 1030 into a felony by alleging that the CFAA offense was "in furtherance of" a violation of 18 U.S.C. § 2701 where the Government relied upon the very same conduct "to charge both the underlying violation of § 1030(a)(2)(C) as well as the elevating violation of § 2701," and the Government conceded that there was "no evidence that the defendant committed [the CFAA] offense 'in furtherance of any' separate

and distinct 'criminal or tortious act in violation of the Constitution or laws of the United States or of any State.'" *Id.* at 282. But the Court further noted that:

> If the government had proven that Cioni accessed Freeman's e-mail inbox and then used the information from that inbox to access another person's electronic communications, no merger problem would have arisen. But the government charged and attempted to prove two crimes using the same conduct of attempting, but failing, to access only Patricia Freeman's e-mail account. This creates a merger problem, implicating double jeopardy principles.

Id. at 283. Here, in contrast, the Government produced evidence of an additional step, disclosure of personal identifying information by Auernheimer, that eliminates any possible merger problem between the two offenses.

B. The Evidence, Taken In The Light Most Favorable To The Verdict, Supported A Finding That The Conspirators Violated The New Jersey Statute.

Auernheimer also argues that the evidence at trial did not support the jury's verdict that the conspirators violated the New Jersey statute. He is mistaken, as the evidence overwhelmingly supported the verdict.

1. The Government Proved That The Conspirators Violated The New Jersey Statute By Violating Code-Based Restrictions.

The evidence permitted the jury to find that the conspirators accessed AT&T's servers by violating code-based restrictions. First, Spitler changed the user agent string on his computer to that of an iPad, which was a change in code

that was *necessary* to allow him to access AT&T's server. A255-57, A474. Auernheimer asserts that "user agents do not regulate access. They are merely browser setting that allow users to optimize how a webpage looks for the user's own convenience." DB30. But that assertion is flatly contradicted by the record. The Government does not dispute that user agents, *generally speaking*, are intended to optimize how a webpage looks, and that sophisticated computer users are capable of changing their browser agents,[18] but *the record here* is undisputed that having the wrong user agent did not change how the AT&T webpage appeared, but instead denied access to the AT&T server entirely.[19] A255-57, A474. Because, in this case, the user agent string was a restriction put in place by the programers, based on computer code, that restricted access to the system, it was a "code-based restriction."

---

[18] The Government is skeptical about Auernheimer's claim that changing a user agent is "very common," but that is not an issue this Court needs to decide. The Government suspects that only a small percentage of internet users even know what a "user agent" is, or have ever purposefully changed a user agent. A defense witness, R. David Hulsey, testified that spoofing an iPad requires technical sophistication. A468-69. What is commonly done by computer professionals and hackers is not commonly done by internet users in general.

[19] *See also* http://en.wikipedia.org/wiki/User_agent ("The User-Agent string is one of the criteria by which Web crawlers may be *excluded from accessing* certain parts of a Web site . . . ." (emphasis added).

While he was spoofing an iPad, Spitler also impersonated authorized users by submitting their unique ICC-IDs to gain access to the AT&T server. One method of circumventing code-based restrictions is for the user to "engage in false identification and masquerade as another user." Orin Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes," 78 N.Y.U.L.R. 1596, 1644 (Nov. 2003), *see also id.* at 1664 (correctly guessing a password constitutes access "under false identification" and is a type of code-based unauthorized access). That is precisely what Spitler did here by using a brute force computer program to eventually discover 114,000 different ICC-IDs that corresponded with registered users.

Moreover, even if this Court were to conclude that impersonating an authorized user does not constitute a violation of a "code-based restriction," the New Jersey statute nevertheless was still violated. The instruction given by the Court, which permitted the jury to convict the defendant if there was a "violation of a code-based restriction by impersonating an authorized user," A706, was based on New Jersey case law which clearly holds that impersonating an authorized user constitutes "unauthorized access." *See State v. Riley*, 988 A.2d 1252, 1263 (N.J.Super.L. 2009) ("unauthorized access" occurred "where the defendant impersonated authorized users") (*citing State v. Gaikwad*, 793 A.2d 39, 44

(N.J.Super.A.D. 2002) (defendant convicted of illegally accessing a computer system had a consistent pattern of "impersonating the user")). So whether it is a violation of a code-based restriction is really beside the point. Regardless of how it is characterized, impersonating an authorized user to gain access to a computer is the prototypical case of unauthorized access.

The evidence that Spitler impersonated authorized users was overwhelming. By falsely telling the AT&T server that he was using an iPad, while supplying the unique ICC-ID of other people's iPads, Spitler was impersonating other authorized users when he accessed AT&T's server.

2. The Conduct Was Within The Territorial Reach Of New Jersey's Criminal Laws Because There Were Victims Who Were Harmed In New Jersey.

Auernheimer also argues that the conduct alleged and proven here was beyond the territorial reach of New Jersey's criminal laws. That claim, which was not raised before the District Court, is reviewed for plain error only.[20] Regardless

[20] To show plain error, "there must be (1) error, (2) that is plain, and (3) that affect[s] substantial rights." *U.S. v. Cotton*, 535 U.S. 625, 631 (2002) (citations and internal quotation marks omitted). An error is "plain" if it is "clear" or "obvious" under "current law." *Johnson v. U.S.*, 520 U.S. 461, 467 (1997). An error "affect[s] substantial rights" if it "affected the outcome of the district court proceedings." *Cotton*, 535 U.S. at 631 (citation omitted). "If all three conditions are met, an appellate court may then exercise its discretion to notice a forfeited error, but only if (4) the error seriously affect[s] the fairness, integrity, or public reputation of judicial proceedings." *Id.* (citation omitted). In the sufficiency

of the standard of review, the claim is without merit. New Jersey law certainly extends to the protection of victims of computer crimes located within the State's boundaries.

By New Jersey statute, "a person may be convicted under the law of this State of an offense committed by his own conduct or the conduct of another for which he is legally accountable if," among other things, "[e]ither the conduct which is an element of the offense *or the result* which is such an element occurs within this State." N.J.S.A. § 2C:1-3(a)(1) (emphasis added). Similarly, New Jersey's criminal laws extend their reach to "[w]hen the result which is an element of an offense consists of inflicting a harm upon a resident of this State . . . [and] the result occurs within this State, *even if the conduct occurs wholly outside this State*, and any property that was affected by the offense was located outside this State." N.J.S.A. § 2C:1-3(g) (emphasis added). Finally, New Jersey has extended the territorial reach of its courts for the prosecution of computer crimes to, among other places, "where the actual damage occurs." N.J.S.A. § 2C:20-34.

---

context, plain error requires a defendant to show "a fundamental miscarriage of justice," *U.S. v. Gordon*, 290 F.3d 539, 547 (3d Cir. 2002), which is a deficiency that is "so clear that'the trial judge and prosecutor were derelict in even permitting the jury to deliberate," *U.S. v. Wright-Barker*, 784 F.2d 161, 172 (3d Cir. 1986) (internal quotes omitted).

The "harm" here, which was an element of the offense, was the disclosure of personal identifying information of the New Jersey victims. Even assuming that the actionable conduct "occur[red] wholly outside this State," the crime was still within the territorial reach of New Jersey's courts because the result inflicted "a harm upon a resident of this State." Similarly, the "actual damage," that the statute was meant to prevent, *i.e.*, the dissemination of personal identifying information, occurred in New Jersey and elsewhere. *See* A148-50 (FBI agent in Newark reviewed Gawker article on internet). New Jersey is entitled to protect its residents from harm in this manner. *U.S. v. Roche*, 611 F.2d 1180, 1183 (6th Cir. 1980) ("acts done outside a jurisdiction, but intended to produce and producing detrimental effects within it, justify a State in punishing the cause of the harm as if [the perpetrator] had been present at the effect," *quoting Strassheim v. Daily*, 221 U.S. 280, 285 (1911) (Holmes, J.)).

Auernheimer also argues that the New Jersey statute violates the Dormant Commerce Clause. Not so. As the Supreme Court recently explained:

> Our dormant Commerce Clause jurisprudence significantly limits the ability of States and localities to regulate or otherwise burden the flow of interstate commerce. It is driven by a concern about *economic protectionism* – that is, regulatory measures designed to benefit in-state economic interests by burdening out-of-state competitors. . . . *The crucial inquiry . . . must be directed to determining whether the challenged statute is basically a protectionist measure* or whether it

> can fairly be viewed as a law directed to legitimate local concerns, with effects upon interstate commerce that are only incidental.

McBurney v. Young, 133 S.Ct. 1709, 1719-20 (2013) (emphasis added) (internal citations and quotation marks omitted). As Auernheimer notes elsewhere, every State provides protection to its citizens against unauthorized computer access. The challenged New Jersey statute is not a protectionist measure; rather it addresses a legitimate concern – computer security – and it provides protection for New Jersey victims that is comparable to the laws enacted by other States. Moreover, the law treats perpetrators who are New Jersey residents and perpetrators outside the State in precisely the same manner. Auernheimer has not attempted to show that it is more burdensome for him or others to comply with the New Jersey law than it is to comply with the comparable laws in the other 49 States, and he has not shown any particular burden on interstate commerce from the statute.

American Booksellers Foundation v. Dean, 342 F.3d 96 (2d Cir. 2003), which Auernheimer cites in support of his Dormant Commerce Clause claim, DB38, does not require this Court to hold otherwise. There, the Second Circuit held that a Vermont statute criminalizing the transfer of sexually explicit materials "harmful to minors" violated the First Amendment rights of operators of internet websites. *Id.* at 99-102. In *dicta*, the Court also found that the statute violated the

Dormant Commerce Clause. *Id.* at 102-04. The reasoning in that case does not apply to this very different statute, and it is not consistent with the Supreme Court's more recent pronouncements on the limited scope of Dormant Commerce Clause jurisprudence. *See, e.g., McBurney*, 133 S.Ct. at 1719-20, *Department of Revenue of Ky. v. Davis*, 553 U.S. 328, 337-39 (2008). Indeed, the Second Circuit has itself subsequently characterized the holding cited by Auernheimer as *dicta* and has emphasized the limited nature of that *dicta*. *See SPGGC, LLC v. Blumenthal*, 505 F.3d 183, 195 (2d Cir. 2007); *see also American Booksellers Foundation v. Strickland*, 601 F.3d 622, 628 (6th Cir. 2010) (Ohio statute criminalizing sending of harmful material to juveniles "does not affect out-of-state actors differently than in-state actors" and does not violate the Dormant Commerce Clause).

In sum, there is no colorable Dormant Commerce Clause claim here, and certainly Auernheimer has not established "plain error."

III. THE DISTRICT COURT DID NOT PLAINLY ERR BY NOT, *SUA SPONTE*, OVERTURNING THE IDENTITY FRAUD CONVICTION BECAUSE AUERNHEIMER ALLEGEDLY DID NOT POSSESS OR TRANSFER THE E-MAIL ADDRESSES 'IN CONNECTION WITH" UNLAWFUL ACTIVITY.

Standard of Review: plain error for issues not raised below. *Olano*, 507 U.S. at 731.

Auernheimer argues, for the first time on appeal, that his conviction for identity fraud (Count Two) "must be overturned" because, he claims, he "did not possess or transfer the e-mail addresses 'in connection with' unlawful activity." DB38.[21] This argument presents a straw man. The guilty verdict on Count Two was proper because a rational jury could have found that Auernheimer used the ICC-IDs with the intent to commit the crime of unauthorized access of a computer. That is all the statute requires.

Auernheimer relatedly argues, again for the first time on appeal, that the Government was required to prove two separate unlawful acts to uphold a conviction under § 1028(a)(7). Auernheimer has cited no case law that so holds, and the plain language of the statute does not support his legal contention. Thus,

---

[21] While before the District Court, Auernheimer argued that Count Two should be dismissed for three different reasons: (1) the alleged authorized access was over before the conduct underlying Count Two began, (2) the "in connection with" language refers to present or future criminal conduct, and not past criminal conduct, and (3) his conduct was protected by the First Amendment. A78-80. The Court addressed those issues in a written opinion. A27-29.

there was no plain error.[22] More importantly, the evidence presented to the jury supports a finding that Auernheimer did indeed commit two entirely separate unlawful acts – unlawful access of a computer using other people's means of identification, and unlawful transfer of personal identifying information.[23]

A. Auernheimer Used The ICC-IDs, Which Were A Means Of Identification, With The Intent To Access AT&T's Server Unlawfully.

The federal identity fraud statute punishes, among other things, an individual 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) (emphasis added). Auernheimer mistakenly focuses on his "*transfer*" of the *e-mail addresses*. But the correct focus should be on his "*use*" of

---

[22] *See U.S. v. Harris*, 471 F.3d 507, 512 (3d Cir. 2006) (no plain error exists where Supreme Court has not ruled and Third Circuit has not issued a precedential opinion); *U.S. v. Clark*, 237 F.3d 293, 298-99 (3d Cir. 2001) (no plain error where defendant fails to cite any controlling authority for his position).

[23] Auernheimer also argues that his conviction on Count Two must be overturned because he did not violate § 1030(a)(2)(C), which is the charged predicate violation of Federal law. DB39. For the reasons already presented by the Government in support of the conviction on Count One, that portion of Auernheimer's claim is without merit.

the *ICC-IDs*. Auernheimer used the ICC-IDs, which qualified as a means of identification, "with the intent to commit" the federal crime of unauthorized computer access.

While before the District Court, Auernheimer did not dispute that the ICC-IDs constituted a "means of identification," nor could he have done so. A "means of identification" is "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any . . . unique electronic identification number, address, or routing code . . . or telecommunication identifying information or access device[.]" 18 U.S.C. § 1028(d)(7)(D). While the e-mail addresses likewise constitute a "means of identification," they were not the means of identification that Spitler and Auernheimer *used* to commit the crime. Rather, the e-mail addresses were the fruits of the crime, while the unique ICC-IDs were the means used to access the computers improperly.

Viewed in this way, the violation of the federal identity fraud statute is straight-forward and clear. If you obtain or use someone else's social security number in order to get access to his or her social security or medical records, it is identity fraud. If you obtain or use someone else' taxpayer identification number in order to get access to his or her tax returns, it is identity fraud. If you obtain or

use someone else's password or ICC-ID in order to get access to his or her computer or server, it is identity fraud. There is nothing controversial here.

Auernheimer suggests that the Government's reading of the statute is too broad because it necessarily conflates a violation of the computer access statute with a violation of the identity fraud statute. But that is not the case. There are numerous way to commit unauthorized access to a computer – some of them involve using passwords and other unique identifiers, while others involve more complex computer hacking. When an individual improperly accesses a computer using a password or other unique personal identifier, it can be charged as identity fraud. *Cf. U.S. v. Barrington*, 648 F.3d 1178, 1192-93 (11th Cir. 2011) (defendant who used others' computer passwords properly convicted of aggravated identity theft).

B. Even If, As Auernheimer Alleges Without Case Law Support, The Government Is Required To Prove Two Different Underlying Unlawful Acts, The Proofs Did So.

Auernheimer also argues that the Government was required to prove, but did not prove, two different underlying unlawful acts, one involving the unlawful acquisition of means of identification, and a wholly separate crime involving "unlawful activity other than the wrongful act of obtaining the means of identity." DB39. This argument likewise was not raised before the District Court, and thus is

reviewed for plain error only. Regardless of the standard of review, the contention is without merit.

Applying the statute's clear and unambiguous terms, a violation of § 1028(a)(7) is established by proving that Auernheimer knowingly transferred, without lawful authority, means of identification of other persons in connection with his unlawful accessing of AT&T's servers, which constituted a violation of Federal law. *See Hanif v. Attorney General*, 694 F.3d 479, 484 (3d Cir. 2012) ("courts must presume that a legislature says in a statute what it means and means in a statute what it says") .

Contrary to Auernheimer's suggestion, the criminal activity here did not constitute simply a single crime involving the unlawful obtaining or possession of other people's means of identification. There were, quite plainly, two separate unlawful acts. First, there was the CFAA violation that involved the unlawful acquisition of individuals' means of identification (their e-mails and ICC-IDs) through the hacking of the AT&T computer, and then there was the unlawful transfer of that information to Gawker, in violation of New Jersey law. Therefore, even if Auernheimer is correct that "the statutory text . . . requir[es] the government to prove two different kinds of unlawfulness," DB40, the Government

proved two different kinds of unlawfulness here – acquisition in violation of Federal law and transfer in violation of State law.

There can be little doubt that these two unlawful activities, the acquisition of the information, and the subsequent transfer of the information, were "in connection with" each other. Auernheimer claims that the phrase "in connection with" is "notoriously vague." Br.42. The phrase is broad, but it is not vague. *See, e.g.*, *U.S. v. Loney*, 219 F.3d 281, 284 (3d Cir. 2000) (undefined terms in the guidelines and statutes should be interpreted using their ordinary meaning, and "the phrase 'in connection with' should be interpreted broadly").

As originally enacted, subsection (a)(7) referred only to acting "with the intent to commit, or to aid or abet," another to commit a crime. *See* Pub. L. No. 105-318, § 3(a)(4), 114 Stat. 3076 (1998). In 2004, subsection (a)(7) was expanded to include acting "in connection with" unlawful activity. *See* Pub. L. No. 108-275, § 3, 118 Stat. 832 (2004). That specific language was added with the express purpose of broadening the reach of section 1028(a)(7) and expanding criminal liability. *See* H.R. Rep. No. 528, 108th Cong., 1st Sess. (2004).[24]

---

[24] "The addition of the words 'in connection with' would broaden the reach of section 1028(a)(7) in two important ways. First, it will make possible the prosecution of persons who knowingly facilitate the operations of an identity-theft ring by stealing, hacking, or otherwise gathering in an unauthorized way other people's means of identification, but who may deny that they had the specific

Auernheimer's vagueness allegations are based on hypotheticals that are far removed from the instant case. DB42. As previously noted, outside the First Amendment context, vagueness challenges to a criminal statute are judged on the basis of the facts of the given case, not on the basis of hypothetical other prosecutions. *Moyer*, 674 F.3d at 211. Here, the identity theft involved the violation of two different statutes, one federal and one state. Therefore, even assuming Auernheimer is correct that a successful prosecution under § 1028(a)(7) requires proof of two unlawful acts, that legal requirement clearly was satisfied in this case.

The District Court did not err, much less plainly err, in not dismissing Count Two of the Indictment for the reasons alleged.

---

intent to engage in a particular fraud scheme. Second, it will provide greater flexibility for the prosecution of section 1028(a)(7) offenses. With this proposed change, prosecutors would have the option of proving that the defendants either had the requisite specific intent to commit a particular unlawful activity or engaged in the prohibited use, transfer, or possession of others' means of identification in connection with that unlawful activity." H.R. Rep. No. 528, 108th Cong., 1st Sess. (2004).

IV. VENUE WAS PROPER IN THE DISTRICT OF NEW JERSEY FOR BOTH COUNTS OF THE INDICTMENT.

Standard of Review: plenary. *U.S. v. Pendleton*, 658 F.3d 299, 302 (3d Cir. 2011).

Auernheimer (supported by NACDL), argues that the District of New Jersey lacked venue for the two charges in the indictment. The argument is mistaken for several reasons. First, Auernheimer's analysis relies upon a flawed legal premise. Auernheimer appears to assume that the only proper test for determining venue in a criminal case is a "crucial elements" test. Neither the Supreme Court, nor this Court, has ever so held. There is also a broader test – the "substantial contacts" test – which this Court has endorsed. Regardless of whether the narrower "crucial elements" test or the broader "substantial conducts" is applied, venue was proper for both counts of conviction in the District of New Jersey.

A. This Court Has Endorsed A "Substantial Contacts" Test For Venue In Criminal Cases, And That Precedent Has Never Been Overturned By The Supreme Court Or This Court.

A criminal defendant has a constitutional and statutory right to be tried in the district in which the crime was committed. *U.S. v. Rodriguez-Moreno*, 526 U.S. 275, 278 (1999). "When the crimes consists of distinct acts occurring in different places, venue is proper where any part of the crime occurs." *Pendleton*, 658 F.3d at 303; *see* 18 U.S.C. § 3237 (crime that is "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"). Additionally, in a conspiracy, venue is proper "wherever a co-conspirator has committed an act in furtherance of the conspiracy." *U.S. v. Perez*, 280 F.3d 318, 329 (3d Cir. 2002).

Auernheimer and NACDL argue that the proper test for determining venue here is a "crucial elements" test. DB45-46; NACDL Br.22-23. While satisfying the crucial elements test in a judicial district is sufficient to establish venue, *see Perez*, 280 F.3d at 328-29, that does not imply that the "crucial elements" test is the exclusive means for establishing venue. In *U.S. v. Goldberg*, this Court adopted the "substantial contacts" test for venue:

> A review of the relevant authorities demonstrates that there is no single defined policy or mechanical test to determine constitutional venue. Rather, the test is best described as a *substantial contacts* rule that takes into account a number of factors–the site of the defendant's acts, the elements and nature of the crime, the *locus of the effect of the criminal conduct*, and the suitability of each district for accurate fact finding.

830 F.2d 459, 266 (3d Cir. 1987) (emphasis added) (venue proper in E.D.Pa. for counts charging wire fraud and interstate transportation of fraudulently obtained money, even though the charged transmissions and transportation did not begin or end or even pass through that district) (*quoting U.S. v. Reed*, 773 F.2d 477, 480 (2d

Cir. 1985)).[25] This court's precedential decision in *Goldberg* has not been overturned by any subsequent decision of the Supreme Court or this Court.

Auernheimer and NACDL may have concluded that *Goldberg* is no longer good law in light of *Rodriguez-Moreno*, which they cite as controlling authority for the crucial elements test. But if that is their belief, they are mistaken. In *Rodriguez-Moreno*, the Court specifically left open the question, argued by the Government there, that "venue may permissibly be based upon the effects of a defendant's conduct in a district other than the one in which the defendant performs the acts constituting the offense." 526 U.S. at 279 n.2. Thus, *Rodriguez-Moreno* does not undermine the continuing validity of cases such as *Goldberg*, which permit consideration for venue purposes of "the locus of the effect of the criminal conduct."

Two of the leading federal criminal law treatises agree that the "substantial contacts" test for venue, adopted by this Court in *Goldberg*, remains good law today. *See* Daniel Coquilette, *et al.*, 25 Moore's Federal Practice, § 618.05[3][a] at 10-11 (March 2013) (when a crime involves more than one judicial district, there

---

[25] *See also U.S. v. Davis*, 689 F.3d 179, 186 (2d Cir. 2012); *U.S. v. Muhammad*, 502 F.3d 646, 652 (7th Cir. 2007); *U.S. v. Zidell*, 323 F.3d 412, 423 (6th Cir. 2003); *but see U.S. v. Jefferson*, 674 F.3d 332, 369 n.48 (4th Cir. 2012) (declining to adopt a "substantial contacts" test for venue).

are different potential methods for determining venue – one focuses "on the verbs, key terms, and policies underlying the statute defining the crime," and another, the "substantial contacts" test, which "takes into account a number of factors including the site of the defendant's acts and effect of the criminal conduct."); Wright & Henning, Federal Practice and Procedure, Criminal 4th, § 302 (2013) ("Courts apply the substantial contacts test to determine whether venue is proper under the particular facts of the case, especially in cases in which the defendant's own acts did not take place in the district."). As the Seventh Circuit has noted, the Supreme Court's discussion of "the nature of the crime alleged and the location of the act or acts constituting it," is simply the starting point for considering venue:

> [W]e shall not forget that the Supreme Court has referred to these two factors simply as a guide, not a rigid test. Nor shall we forget the admonition of our sister circuits that "there is no single defined policy or mechanical test to determine constitutional venue. Rather the test is best described as a substantial contacts rule . . . ."

502 F.3d at 652 (*quoting Reed*, 773 F.3d at 481, and citing cases).

B. Under the "Crucial Elements" Analysis, Properly Applied, Venue Is Proper In New Jersey For Count One.

Even assuming that the narrower "crucial elements" analysis is the proper test for venue in this case, Auernheimer misapplies that analysis, and therefore comes to the wrong conclusion about venue. Determining where a crime was

committed is a two-step process that requires a court to look both at "the nature of the crime alleged" and "the location of the act or acts constituting it." *Rodriguez-Moreno*, 526 U.S. at 279; *accord Pendleton*, 658 F.3d at 303 (describing the "two-pronged approach").

Auernheimer makes two mistakes in applying the crucial elements standard. First, and foremost, he misidentifies the nature of the crime charged in Count One of the indictment, which leads him to ignore the "crucial element" of proving that the conspiratorial scheme involved a violation of the New Jersey law protecting the disclosure of personal identifying information. Second, his analysis fails to recognize that the failure of the conspirators to obtain authorization from the more than 4,500 victims located in New Jersey before using their ICC-IDs to access the AT&T servers, likewise was a "crucial element" of Count One. Either of these mistakes, taken alone, demonstrates that venue was, contrary to his contention, proper in New Jersey for the Count One conspiracy charge.

1. Venue Was Proper In New Jersey Because Proving That The Scheme Involved A Violation Of New Jersey's Disclosure Statute Was An "Essential Element" Of The Charged Conspiracy.

Auernheimer and the NACDL misidentify, at step one of the process, the nature of the crime charged. *See Rodriguez-Moreno*, 526 U.S. at 279 ("a court must initially identify the conduct constituting the offense (the nature of the crime)"). Auernheimer and the NACDL analyze the venue issue in Count One as if the question presented is where, in general, it is proper to prosecute any violation (including misdemeanor violations) of the CFAA. But the Government did not charge some sort of generic computer frauds crime; rather, it charged (via the conspiracy statute) a particular felony violation of the CFAA, *i.e.*, one that was based on an underlying violation of New Jersey state law involving New Jersey victims. The CFAA crime charge in Count One was tied to the violation of New Jersey's privacy statute, and because of that, venue was proper in New Jersey.

Count One charged Auernheimer with violating 18 U.S.C. § 371 by conspiring with Spitler and others to access AT&T's servers without authorization *in violation of New Jersey law* (namely N.J.S.A. 2C:20-31(a)), contrary to 18 U.S.C. § 1030(a)(2)(C) and 1030(c)(2)(B)(ii). A6 at ¶5, A15 at ¶ 27. The object of the conspiracy was "to steal and disclose the personal identifying information of

thousands of individuals, to cause monetary and reputational damage to AT&T and to create monetary and reputational benefits for" the conspirators. A6 at ¶ 6. In order for the jury to return a guilty verdict on that charge, the Government had to prove beyond a reasonable doubt that Auernheimer knowingly joined the conspiracy and intended to access a computer improperly in order to violate the New Jersey law protecting the disclosure of personal identifying information of its residents. A697, A704-05.

Thus, the "nature of the crime" charged in Count One involved not only accessing a computer, but also disclosing the personal identifying information of New Jersey residents. The disclosure of personal identifying information of New Jersey residents, in violation of New Jersey law, is what made the charged crime a felony. To ignore that additional aspect of the crime, as Auernheimer does, misrepresents the nature of the crime charged.

Auernheimer makes the same mistake, in essence, that the defendant made in challenging venue in *U.S. v. Rodriguez-Moreno*, 526 U.S. 275 (1999). That case arose from a theft of 30 kilograms of cocaine from a Texas drug dealer. Rodriguez-Moreno and others kidnaped Ephrain Avendano, the middleman in the deal, and they drove him from Texas to New Jersey. The conspirators used an apartment in New Jersey as a base of their operation for a few days while they

searched for the thief. Not finding the thief, the kidnapers moved to New York and then Connecticut, again bringing Avendano with them. In Connecticut, the kidnapers obtained a .357 magnum revolver and threatened to use it to kill Avendano.

Rodriguez-Moreno and his codefendants were tried in the District of New Jersey for, among other things, using or carrying a firearm during and relation to the kidnaping, in violation of 18 U.S.C. § 924(c)(1). This Court held, in a 2-to-1 opinion with Judge Alito dissenting, that although there was venue in New Jersey for the kidnaping charges, New Jersey lacked venue for the 924(c)(1) charge because no firearm was "used" or "carried" in New Jersey. *U.S. v. Palma-Ruedas*, 121 F.3d 841, 847-51 (3d Cir. 1997).

Justice Scalia agreed with this Court, noting "[t]he short of the matter is that this defendant, who has a constitutional right to be tried in the State and district where his alleged crime was "committed," has been prosecuted for using a gun during a kidnaping in a State and district *where all agree he did not use a gun during a kidnaping*." 526 U.S. at 285 (emphasis added). Justice Scalia suggested that simply stating the case should be enough to decide it. *Id.* But Justice Scalia's reasoning, which closely follows Auernheimer's reasoning, was rejected by the Supreme Court majority.

The Supreme Court found that venue was proper in New Jersey for the firearms offense. The Court declined to focus on just the formal elements of a stand-alone firearms offense, *i.e.*, where the "using" or "carrying" of the gun occurred, but instead the Court focused on the nature of the overall offense. The firearms offense was linked to the predicate kidnaping offense, and the use of the firearm did not have to occur in New Jersey in order for New Jersey to have venue over the firearms offense.

The § 924(c)(1) provision analyzed in *Rodriguez-Moreno* is an enhanced penalty provision, just like the violation of § 1030(c)(2)(B)(ii) charged against Auernheimer (via the conspiracy statute) is an enhanced penalty provision. Just as it did not matter in *Rodriguez-Moreno* that the defendant did not "use" or "carry" the firearm in New Jersey, it does not matter here that the defendant did not "access" the computer in New Jersey. The verbs in the statute are not the sole determinant of the "nature of the crime." *See Rodriguez-Moreno*, 526 U.S. at 280 (declining to endorse the "verb test" for venue). The crime charged here is conspiracy to unlawfully access a computer in order to violate New Jersey's privacy statute. This is, in essence, using a computer "during and in relation to" a violation of New Jersey's privacy law.

Venue necessarily lies in New Jersey to enforce the protection of New Jersey's privacy laws for New Jersey residents. "Acts done outside a jurisdiction, but intended to produce and producing detrimental effects within it, justify a state in punishing a cause of harm as if he had been present at the effect." *Goldberg*, 830 F.2d at 463 (*quoting Strassheim*, 221 U.S. at 285); *accord Roche*, 611 F.2d at 1183; *see also U.S. v. Root*, 585 F.3d 145, 156 (3d Cir. 2009) ("[t]he locality of a crime for the purpose of venue extends 'over the whole area through which force propelled by an offender operates.'") (*quoting U.S. v. Johnson*, 323 U.S. 273, 275 (1944)).

In sum, an "essential element" of Count One, which the Government was required to prove beyond a reasonable doubt, was that Auernheimer knowingly joined the conspiracy, the aim of which was to access a computer improperly in violation of the New Jersey law protecting the disclosure of personal identifying information of its residents. A697, A704-05. Thus, under the "critical elements" test, venue was proper in New Jersey because the object of the conspiracy was the unauthorized disclosure of personal identifying information of New Jersey residents in violation of New Jersey law.

2. Venue Was Proper In New Jersey Because Proving That The Conspirators Failed To Obtain Authorization From The New Jersey Victims Before Using Their ICC-IDs Was An "Essential Element" Of The Charged Conspiracy.

There is a second problem with Auernheimer's venue analysis under the "crucial elements" test. One of the elements of the crime, which the Government had to prove beyond a reasonable doubt, was that the conspirators accessed AT&T's computers "without authorization." A703-04. For the more than 4,500 victims located in New Jersey, as for all the victims, the conspirators failed to obtain their authorization before using their ICC-ID numbers to access the AT&T servers. A264-65. "If the statute makes it a crime to fail to do some act required by law, the failure takes place in, and the proper venue is, the district in which the act should have been done." Wright & Henning, Federal Practice and Procedure, Criminal 4th, §302 (April 2013); *citing Johnston v. U.S.*, 351 US. 215, 219-20 (1956); *U.S. v. Lombardo*, 241 U.S. 73 (1916); *accord U.S. v. Johnston*, 227 F.2d 745, 747-49 (3d Cir. 1956); *U.S. v. Muench*, 153 F.3d 1298, 1300-04 (11th Cir. 1998); *U.S. v. Murphy*, 117 F.3d 137, 139-41 (4th Cir. 1997).

NACDL argues that the failure to obtain authorization is a circumstance, and not an action. NACDL Br.27. This is the type of syntactical argument that Judge Alito rejected in his dissenting opinion in *Palma-Ruedas*, *see* 121 F.3d at 860, and

his reasoning was vindicated by the Supreme Court in *Rodriguez-Moreno*, *see* 526 U.S. at 278. A statute written syntactically to criminalize the unauthorized *accessing* of a computer, is the same as a statute written syntactically to criminalize *failing* to obtain authorization to access the computer. *See* 121 F.3d at 860 (Alito, J., dissenting) (rewriting the syntax of a § 924 violation). Failing to obtain authorization from the victims is an action or omission *taken by the defendant himself* while committing the crime, and thus is not a mere "circumstance" of the crime. *See U.S. v. Bowens*, 224 F.3d 302, 310 (4th Cir. 2000) (distinguishing a "circumstance element" from an "essential conduct element"). The Government proved that the defendants failed to obtain authorization from any of the New Jersey based victims of the offense, A264-65, and that failure to obtain authorization before accessing their accounts was an element of the offense, which satisfies the venue requirement in New Jersey.

The NACDL places heavy reliance on *Bowens*, but the reasoning there helps the Government, not the Defendant. Although *Bowens* looked to conduct constituting the "essential conduct elements" of a crime when determining the "nature of the offense," 224 F.3d at 312, the Court nevertheless noted that where "the essential conduct elements [are] defined not just in terms of the forbidden act, *i.e.*, "assault" or "retaliate," but rather in terms of their effects (intimidation of a

witness or obstruction of the administration of justice), *venue [is] proper in the district where those prescribed effects would be felt*," 224 F.3d at 313 (emphasis added). Here, again, the particular felony charged in the indictment is accessing a computer for the purpose of disclosing personal information in violation of the New Jersey privacy statute, and the "essential conduct element," therefore, is defined not just in terms of the forbidden act of access, but also by the effects of that access, *i.e.*, the disclosure.[26] Thus, "venue [is] proper where those prescribed effects would be felt," 224 F.3d at 313, which here, for the more than 4,500 New Jersey victims, is in New Jersey. Venue lies in New Jersey because the

[26] Auernheimer relies on *U.S. v. Cabrales*, 524 U.S. 1 (1998), where the issue presented was whether venue was proper in Missouri for money laundering offenses, where the Government conceded that Cabrales engaged in no money laundering in Missouri, and her bank deposits and withdrawals all occurred in Florida. The Government relied upon the fact that the proceeds used by Cabrales were generated from drug trafficking activity of others in Missouri. But the Court held that was not enough, noting that Cabrales was not charged with either conspiracy or with aiding and abetting the Missouri drug trafficking. *Id.* at 7. The Court emphasized that Cabrales was prosecuted "for transactions which began, continued, and were completed only in Florida." *Id.* at 8. The Court held that, on those facts, Cabrales' money laundering took place wholly within Florida, and venue was improper in Missouri. *Id.* at 7-10. *Cabrales* does not apply here not only because it interprets a wholly different statute, but also because Auernheimer was charged with acting purposefully in furtherance of the violation of the New Jersey privacy statute, while Cabrales was merely acting "'after the fact' of an offense begun and completed by others." *Id.* at 7.

conspirators failed to obtain authorization from the 4,500 New Jersey victims of the offense.

C. Under the "Substantial Contacts" Standard, Venue Is Proper In New Jersey For Count One.

Since venue is proper in New Jersey under the "crucial elements" standard, properly applied, it doubtless is proper in New Jersey under the broader "substantial contacts" standard. Under the substantial contacts standard, the Court is expressly permitted to consider not only the elements and nature of the crime, but also "the locus of the effect of the criminal conduct." *Goldberg*, 830 F.2d at 466. Thus, the Court properly may base venue by taking into account the location of the victims of the offense. Since the conspiracy charged in Count One was a scheme involving the distributing of information in violation of New Jersey disclosure laws, the 4,500 victims located in New Jersey were more than sufficient to establish venue there. *See Goldberg*, 830 F.2d at 463 (acts producing detrimental effects within a State by outsiders can be punished in the State where the effects are felt).

D. Venue Was Proper In New Jersey Pursuant to 18 U.S.C. § 3237 Because The Offense Continued In New Jersey, Where The Gawker Article Was Accessible And Was Indeed Accessed.

Venue was proper in New Jersey for Count One for another independent reason. Pursuant to 18 U.S.C. § 3237, a crime "commenced 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." Here, the crime commenced in Arizona, where Spitler was located, and it continued in many other districts, including New Jersey, where the Gawker article was published and accessed.

U.S. v. Rowe, 414 F.3d 271 (2d Cir. 2005), is instructive on determining venue for internet crimes. Larry Rowe, a Kentucky resident, while working on his home computer, posted an advertisement for child pornography on an internet chat room. A detective working in New York saw the posting, and Rowe was charged in the Southern District of New York with advertising to receive, exchange or distribute child pornography in violation of 18 U.S.C. § 2251(c). Rowe filed a motion for transfer of venue to Kentucky, which was denied, and after conviction, he challenged venue on appeal.

The Second Circuit found venue was proper in New York, even though Rowe did his advertising for child pornography from Kentucky and did not direct it

to New York or indeed anywhere in particular. The Second Circuit hinged its analysis on § 3237, which, for offenses involving multiple districts, permits venue in any district where the offense was "begun, continued, or completed." The Second Circuit adopted the reasoning of the district court, which stated:

> [Rowe] must have known or contemplated that the advertisement would be transmitted by computer to anyone the whole world over who logged onto the site and entered the chat room . . . . It is clear that the chat room could be entered in this district and in fact was entered in this district . . . . It is clear that both the statutes and the case law and the Constitution permit crimes of this sort to be prosecuted in any jurisdiction where any part of the crime occurred.

414 F.3d at 279; *see also U.S. v. Sutton*, 13 F.3d 595, 598-99 (2d Cir. 1994) (*per curiam*) (venue of prosecution for mailing fake driver's licenses was proper in district to which licenses were sent, even though defendant mailed licenses from outside that district).

Here, the crime indisputably was "committed in more than one district." 18 U.S.C. § 3237. Spitler began the crime in California, A233; Auernheimer assisted him in Arkansas, A185; Spitler transferred the list of e-mail/ICC-ID pairings from California to Arkansas, A285; and Auernheimer transferred the list from Arkansas to a reporter at Gawker, A348-49, SA159, with the intention that the list be available nationwide, SA160. The article that Gawker published was publicly available on its website, and it contained personal identifying information for some

prominent individuals, which information had been obtained by the conspirators and transferred to Gawker. SA131-34. Among the people who accessed the article was Philip Frigm, an FBI special agent working on the case in Newark, New Jersey. A148-50.

Under well-settled principles of conspiracy law, Auernheimer is personally responsible for Gawker's publication of personal identifying information in New Jersey and elsewhere. *See, e.g.*, *U.S. v. Bradley*, 644 F.3d 1213, 1255 n.87 (11th Cir. 2011) ("To satisfy the venue requirement, an overt act may be committed by any conspirator, anyone who aids or abets a conspirator, or anyone a conspirator causes to act"); *U.S. v. Royer*, 549 F.3d 886, 896 (2d Cir. 2008) (conspirators are responsible for "acts that the conspirators caused others to take that materially furthered the ends of the conspiracy"); *cf. U.S. v. McCoy*, 678 F.Supp.2d 1336, 1343-45 (M.D. Ga. 2009) (defendant, who sent links to obscene websites, aided and abetted computer server in its interstate transportation of obscene material); *see also Whitfield v. U.S.*, 543 U.S. 209, 218 (2005) ("this Court has long held that venue is proper in any district in which any overt act in furtherance of the conspiracy was committed, even where an overt act is not a required element of the conspiracy offense").

Just as Rowe must have known that his advertisement would be available anywhere once it was posted on the internet, so too Auernheimer knew that the information he provided to Gawker for publication would be available anywhere once it was published. Rowe was properly subjected to prosecution in New York when a law enforcement officer in New York accessed the information he made publicly available there. So too, Auernheimer is properly subjected to prosecution in New Jersey, where a law enforcement officer accessed the information he provided to Gawker. *See also McCoy*, 678 F.Supp.2d at 1343-45 (venue was proper in Georgia to prosecute defendant for sending obscene material into Georgia; although defendant resided in Minnesota and operated his computer there, he sent links to obscene websites to a law enforcement officer in Georgia, who opened the links, thereby aiding and abetting the computer server's interstate transportation of obscene material).

U.S. v. Powers, 2010 WL 1418172 (D. Neb. March 4, 2010), is also persuasive on this point. Chad Powers, who lived in Arizona, gained access to the email account of a woman in Nebraska, and he emailed partially nude images of her to others. *Id.* at *1. Powers was charged with exceeding authorized access to the victim's computer in violation of 18 U.S.C. § 1030(a)(2)(C), in furtherance of a violation of Nebraska's statute governing invasion of privacy and intentional

infliction of emotional distress. *Id.* The pictures were stored on a server at AOL, where the victim maintained her email account, rather than on the victim's personal computer in Nebraska. *Id.* at *2. The case was indicted in Nebraska, and Powers filed a motion to dismiss for improper venue, arguing that he had never been physically present in Nebraska, and the computer he allegedly used to commit the crime was in Arizona. *Id.*

The court, citing 18 U.S.C. § 3237, held that venue nevertheless was proper in Nebraska because the crime, which allegedly began in Arizona, was completed in Nebraska. *Id.* at *2 ("Although Powers may not have been physically present in Nebraska, and the computer used to facilitate the violation was located in Arizona, venue would be proper in any district in which the offense began in one district, and was completed or committed in any other district."). The court relied upon the fact that the victim of the offense "resided in and was injured in Nebraska when Powers violated CFAA," and that "Powers committed the violation in furtherance of tortious acts, specifically violations of Nebraska law under invasion of privacy and intentional infliction of emotional distress." *Id.*[27]

[27] The court also noted that some of the emails Powers forwarded were sent to recipients in Nebraska. *Id*.

The same reasoning applies here. Although Auernheimer may not have been physically present in New Jersey, and the computer used to facilitate the violation was not located in New Jersey, the offense continued into New Jersey. The victims – in this case the thousands of New Jerseyans who had their confidential ICC-ID/e-mail pairings disclosed to Gawker – resided in New Jersey when Auernheimer violated the § 1030(a)(2)(C) offense in furtherance of the New Jersey criminal statute prohibiting the disclosure of personal identifying information obtained without authorization. As *Powers* concluded, the defendant "may be prosecuted in any district where such crime began, continued, or completed." *Id.* Accordingly, venue was proper in New Jersey.

E. Auernheimer's Proposed Venue Rule Is Impractical And Unworkable.

The rhetorical strength of Auernheimer's argument lies in his claim that, under the Government's view of venue, an aggressive federal prosecutor could forum shop and charge any computer crime in any jurisdiction throughout the country. DB45, DB49-50. That argument is a red herring. The only reason that Auernheimer could have been charged with different versions of a CFAA violation in many, if not all states, is because he had 114,000 victims of his offense. Had Auernheimer stolen and disclosed personal identifying information of one or only a

handful of individuals, he would not have been subjected to possible nationwide prosecution. The decision as to the number of victims was completely in the hands of Auernheimer and Spitler, not the Government.

This is important because, rather than be concerned with Auernheimer's threat of prosecutors running amok in search of a more adventageous venue, this Court must be concerned with the implications of the stunted venue rule that Auernheimer proposes for CFAA cases that involve far fewer victims. According to Auernheimer, venue for computer frauds crimes lies only in a district where either the perpetrator did his hacking, or where the computer server hacked into is located. DB46. That venue rule is impractical and unworkable.

Suppose an elderly widow living in New Jersey keeps her savings in an FDIC-insured national bank, and she checks her balances and does her bill-paying online. A computer hacker operating from a back room in Hong Kong appropriates her password, hacks into her account, and loots the account of her life's savings. Let's further assume that the bank has located its servers in Atlanta. Under Auernheimer's theory of venue, a charge under the Computer Crimes Fraud Act could not be prosecuted in the District of New Jersey, and must instead be prosecuted in Atlanta. But that makes no sense. The New Jersey-based victim is not going to call the police in Atlanta, and that jurisdiction may not be particularly

interested in investigating or prosecuting the crime. The harm that the statute was meant to prevent occurred in New Jersey, and that is where venue should lie.

To be sure, if the hacker illegally accessed without authorization the personal email accounts of 114,000 people located throughout the United States, then the Government would indeed have its choice of venue. But that would be because of the dispersed location of the large number of victims that the hacker selected, not because the venue rule proposed by the Government is over inclusive. Had the victims here been 114,000 mail fraud victims, venue likewise would be available throughout the country. *See U.S. v. Grenoble*, 413 F.3d 569, 574 n.1 (6th Cir. 2005) (venue in mail fraud is proper where the mail is deposited, received, or moves through). A workable venue rule must cover small scale, as well as large scale, computer crimes.

Auernheimer correctly notes that internet crimes are different from other crimes, DB49-50, but he draws the wrong conclusion from those differences. Given the amorphous nature of the internet and the rise of "cloud" computing, the physical location of a computer server is not, in the real world, a factor of major significance. In this case, the AT&T servers apparently were in Dallas and

Atlanta.[28] But they could have been physically located somewhere else, and the crime and its "essential nature" would have been unchanged. A small business owner whose website is hosted by, for example, monster.com, or an individual making internet purchases or doing online banking, almost certainly has no idea where the computer server he or she is using is located. While the presence of a server in a particular location is sufficient to permit venue there, the location of the server is not always dispositive, as Auernheimer supposes, in determining where a computer crime is committed.

When people and businesses in New Jersey are the victims of computer-related crimes, they call the local police department or the local office of the FBI, they don't call law enforcement officials in distant locales where the relevant computer servers are located. Crimes are prosecuted, for the most part, where they are investigated. It is unremarkable to note that "places that suffer the effects of a crime are entitled to consideration for venue purposes." *Muhammad*, 502 F.3d at 654; *Reed*, 773 F.3d at 482; *accord Goldberg*, 830 F.2d at 266 (venue considerations include "the locus of the effect of the criminal conduct"). The

[28] Defense witness Timothy Glantz testified that he did not know where AT&T's iPad servers were located, but he did not dispute that certain documents shown to him by Auernheimer's counsel suggested that the servers were in Dallas and/or Atlanta. A435.

location of victims matters, especially in computer crimes, where so much of the crime occurs in cyberspace or "the cloud."

Section 1030(a)(2) is not a statute designed to protect computers as *machinery*, rather it is designed to protect people and businesses who maintain *information* on the machines. *See* S. Rep. No. 99-432, at 6 (1986) ("The premise of [§ 1030(a)(2)] is privacy protection") (available at 1986 WL 31918, at *6). Auernheimer's crabbed venue argument completely disregards "the nature of the crime." By focusing on the location of servers, Auernheimer and the NACDL miss the forest for the trees. Because Auernheimer and Spitler committed a computer crime that had more than 4,500 victims in New Jersey, venue was proper in New Jersey.

F. Venue Was Proper In New Jersey On Count Two.

Venue was proper in New Jersey on the identity fraud charge in Count Two for two independent reasons. First, if this Court concludes, as it should, that venue was proper in New Jersey for Count One, then it must conclude that venue was proper for Count Two because Count Two is based on the predicate offense charged in Count One, and that connection alone is sufficient to establish venue. And if this Court were to conclude that venue was not proper in New Jersey for the charged CFAA offense, then this Court must separately analyze venue for Count

Two. In doing so, this Court should find that the Government sufficiently proved venue in New Jersey for the charged identity fraud offense.

1. Venue Was Proper In New Jersey On Count Two Because It Is Based On The Predicate Offense Charged In Count One, For Which Venue Was Proper.

Count Two charged Auernheimer with "knowingly transfer[ring], possess[ing], and us[ing], without lawful authority, means of identification of other persons, including means of identification of New Jersey residents, in connection with unlawful activity, specifically, the unlawful accessing of AT&T's servers," A16, contrary to 18 U.S.C. § 1030(a)(2)(C), in violation of 18 U.S.C. § 1028(a)(7). Assuming venue was proper in New Jersey for Count One, for any or all of the reasons argued above, then venue necessarily was proper as well for Count Two, which charged identity fraud "in connection with" the same underlying violation of the CFAA.

In *U.S. v. Magassouba*, 619 F.3d 202, 203 (2d Cir. 2010), the Second Circuit held, in an aggravated identify theft case, that venue was proper "in any district where the predicate felony offense was committed, even if the means of identification of another person was not transferred, possessed, or used in that district." As the Second Circuit noted, this is a straight-forward application of the reasoning in *Rodriguez-Moreno*, which interpreted similar statutory language and

held that venue in a prosecution for using or carrying a firearm *during and in relation to* a crime of violence is proper in any district where the crime of violence was committed, even if the firearm was used or carried only in a different district. *Id.* at 206. Here, as in both *Rodriguez-Moreno* and *Magassouba*, the predicate offense is a "critical part" of the other offense, and "prosecution is appropriate in any district in which venue is appropriate for the predicate." *Id*.

2. Even If Venue Was Improper In New Jersey For The CFAA Count, Venue Nevertheless Was Proper In New Jersey For The Identity Fraud Count.

If this Court were to conclude that venue was improper in New Jersey for Count One, then it should conduct a separate analysis concerning Count Two, which charged an identity fraud conspiracy. Even if the location of computer servers and hackers are crucial for determining venue in a CFAA violation, they are not the same factors that must be examined for a charge of identity fraud.

The "essential nature" of an identity fraud case is the improper adoption by a defendant of the identity of another person. Here, Spitler and Auernheimer improperly adopted the identity of more than 4,500 New Jersey residents when they committed this offense. Count Two specifically refers to Auernheimer's transfer, possession, and use of the "means of identification of New Jersey residents" when describing the offense. A16. While it is at least arguable that, for

the CFAA offense, AT&T was the primary victim and the New Jersey residents were only secondary victims, for the identity fraud count, it is beyond cavil that the victims are the individuals whose personal-identifying information was improperly obtained by the conspirators.

All of the arguments made in the prior sections of this brief concerning the overt acts that the conspirators performed in New Jersey, the continuing nature of the offense with its consequences in New Jersey, the failure to obtain authorization from New Jersey residents, the overt acts that the conspirators performed in New Jersey, including the publication in New Jersey and accessing in New Jersey of personal identifying information, continue to apply to Count Two. But venue in New Jersey is even clearer here than in Count One because identity fraud is a more personal victim-based harm than computer fraud, and the residence of the victims matters far more here than the location of the computer servers.

G. There Is No Evidence Of Forum Shopping, Or Any Other Concerns About Improper Venue, In This Case.

Although Auernheimer and the NACDL raise the specter of governmental overreach in their arguments concerning venue, there is no evidence of any such overreach in this case. In fact, the record suggests that Auernheimer was probably advantaged, rather than disadvantaged, by the Government's choice of forum.

Auernheimer was vigorously represented on a *pro bono* basis by high quality legal counsel who were based in Brooklyn, New York, which is a relatively easy commute to Newark, New Jersey, where Auernheimer was prosecuted. The record suggests that it would have been a burden for Auernheimer's *pro bono* counsel to have borne the expenses associated with trial in a distant location, such as Arkansas, California, Georgia, or Texas, where they contend that Auernheimer instead should have been prosecuted. See SA32.

If, as Auernheimer suggests, the Government in a future case might prosecute a defendant in a particular venue to gain an unfair tactical advantage, or in a venue that otherwise creates a hardship for a defendant, then he or she can file a motion for change of venue, which is subject to the District Court's sound discretion. No motion for change of venue was filed in this case. While there is no doubt Auernheimer wanted the charges here dismissed, there is no reason on this record to believe that he had a desire to actually be tried in a different judicial district.

H. If There Was Error Here, The Error Was Harmless.

Rule 52(a) of the Federal Rules of Criminal Procedure provides that "[a]ny error . . . that does not affect substantial rights must be disregarded." If Auernheimer was tried in the wrong venue, it did not affect his substantial rights.

Importantly, Auernheimer never filed a motion for change of venue or argued that the District of New Jersey was an unfavorable forum. Auernheimer wanted the indictment dismissed on venue grounds, but there is no indication that he actually wanted to be tried in a different forum. Instead, as noted above, the forum chosen by the Government benefitted Auernheimer by enhancing his ability to attract and retain experienced and capable counsel on a *pro bono* basis. Indeed, it likely would have been a hardship on the defense team if the case had been moved to the jurisdictions in which Auernheimer suggests venue is proper. Under these facts, Auernheimer was not harmed, even if venue was improper in New Jersey. *See, e.g., U.S. v. Hart-Williams*, 967 F.Supp. 73, 78-81 (E.D.N.Y. 1997) (concluding that improper venue in New York City has harmless error); *see also U.S. v. Brennan*, 183 F.3d 139, 149 (2d Cir. 1999) (concluding venue error not harmless, but noting that "we do not suggest that venue error can never be harmless").

V. THE DISTRICT COURT PROPERLY CALCULATED THE LOSS AMOUNT.

Standard of Review: plenary review over the District Court's interpretation of the Guidelines, and clear error review over factual findings; arguments not raised below reviewed for plain error. *U.S. v. Fumo*, 655 F.3d 288, 308-09 (3d Cir. 2012).

Auernheimer argues that the District Court erred in awarding him an eight-level sentencing enhancement, pursuant to U.S.S.G. § 2B1.1, for a loss amount of $73,167. His argument has three components. First, he argues that money spent by a company notifying its victims of a security breach should not count as loss. That legal contention is subject to plenary review. Second, he argues that if money spent notifying victims can count as loss, the expenditure here by AT&T was not "reasonable," and thus should not have counted as loss. The Court here found that the notification expenses were reasonable, and that factual determination is reviewed for clear error. Finally, Auernheimer argues that the Government failed to present sufficient proof of the loss amount. That contention, which was not raised below, is reviewed for plain error only.

A. The Cost Of Notifying Customers Of A Security Breach Constitutes "Loss" Under U.S.S.G. § 2B1.1.

As a general rules, loss under § 2B1.1, is the greater of actual loss or intended loss. U.S.S.G. § 2B1.1, Note 3(A). "Actual loss" means "the reasonably

foreseeable pecuniary harm that resulted from the offense." *Id.*, at Note 3(A)(i). "Reasonably foreseeable pecuniary harm" includes "pecuniary harm that the defendant knew or, under the circumstances, reasonably should have known was a potential result of the offense." *Id.*, at Note 3(A)(iv).

Most, if not all, States require a company that has suffered a computer security breach to notify its customers of the breach. Therefore, it is reasonably foreseeable that, when a hacker causes a security breach, the company whose computers were hacked into will notify its customers of the breach. Counting notification costs as "loss" is a straight-forward application of the general principles for calculating loss in any Guidelines case.

That is true not only under the rules for calculating Guidelines loss generally, but also under a more specific rule that *expands* the concept of loss for computer crimes. Note 3(A)(v)(III) provides:

> 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, Note 3(A)(v)(III) (emphasis added). Here, providing notification to the victims of the security breach was a cost to AT&T of responding

to the hacking offense. Under the plain language of the Guidelines, the reasonable cost of notifying customers of the breach was a proper part of the calculation of loss for a CFAA violation.

Moreover, Auernheimer's sentencing arguments assume that the only offense of conviction is the CFAA count. But Auernheimer was also convicted of identity fraud under 18 U.S.C. § 1028. None of the CFAA cases that Auernheimer cites in his brief address the calculation of "loss" for the offense of identity fraud. Therefore, even if Auernheimer could show, which he has not, that costs of notification are not properly part of "loss" for a CFAA offense, he has not shown that those costs do not constitute "loss" for his identity fraud offense. Once, again, because the law of virtually every state required AT&T to notify its affected customers, the costs that AT&T incurred in so doing were reasonably foreseeable to Auernheimer.

B. The District Court Was Not Clearly Erroneous In Finding That AT&T's Decision To Notify Its Customers By Mail Was Reasonable.

While before the District Court, Auernheimer asserted that AT&T's expenditure of $73,167 to mail notification of the breach to each of the 114,000 victims should not count as loss because the expenditure was unreasonable. Auernheimer asserted that AT&T's attempt to notify its affected customers by e-

mail was 98% successful. He contended that individual mailing was redundant, unnecessary, and unreasonable.

The reasonableness of AT&T's business judgment in deciding to send individual notification by mail to each of the victims is a factual question subject to clear error review. The District Court rejected Auernheimer's contention that the mail notification was "unnecessary or redundant," instead finding that it was "appropriate." A771. The Court also found that AT&T's decision to notify its customers by mail was "reasonably foreseeable." A771. These common-sense factual conclusions are supported in the record and not clearly erroneous.

The record shows that AT&T considered this a "very, very important" breach of privacy incident, which received an extremely high level of attention at the company. A214. AT&T received numerous complaints about the security breach, both via e-mail and the telephone. A221. Sherry Ramsey, an assistant vice-president at AT&T who focused on privacy issues, testified:

> We received a lot of complaints both e-mail and then also over the phone. . . . Our customers were frustrated. They were scared. They were angry. They felt like something personal to them had been taken away . . . .

A221. The company opted to send a letter to every customer whose e-mail had been breached and published. A221. In doing so, the company followed its

regular policy, any time there is a security breach, of evaluating the breach and notifying its customers. A214.

There is, of course, no reason to believe that AT&T took steps that were greater than necessary simply to increase Auernheimer's Sentencing Guidelines range. AT&T exercised its normal business judgment when it concluded that mailing individual notice to each of its customers was appropriate notification for this security breach. Auernheimer, who did as much as he could to try to hype the seriousness of the breach, is hardly in a sympathetic position to complain that AT&T over-reacted to his crime. The District Court's factual conclusion that AT&T's decision was appropriate is not clearly erroneous.

C. The District Court Did Not Plainly Err In Accepting The Government's Representation That AT&T Spent $73,671 To Notify Its Customers By Mail Of The Security Breach.

Auernheimer argues on appeal that the Government failed to bear its burden of proving the $73,671 loss amount. That contention should be reviewed for plain error only. The presentence report contained the Government's representation that "AT&T's notification of the security breach caused AT&T to incur losses of $73,167." PSR ¶ 52. In his written objections to the presentence report, Auernheimer made it clear that he was challenging the loss calculation as a matter of law, and he was challenging the reasonableness of AT&T's decision to spend

funds to provide individual mail notification to the victims of the offense. A748-50; *see also* PSR at page 43 (objection #1 by the defendant). Neither the Government, nor the Court, was put on notice by Auernheimer that he intended to challenge the veracity of the claim that AT&T spent $73,167 to notify by mail the 114,000 victims of the offense. Rather, Auernheimer appeared to accept that as a fact. *See, e.g.*, A750 (Auernheimer states that "all of the $73,167 'loss' was attributable to AT&T's direct mailing to customers even after it successfully notified its customers by e-mail").

Auernheimer's failure to attack the PSR's representation that $73,167 was spent to mail notice to the victims of the offense dooms Auernheimer's claim:

> A conclusion in the presentence investigation report which goes unchallenged by the defendant is, of course, a proper basis for sentence determination. In this respect, the report serves as a *prima facie* and sufficient showing of fact. The party challenging the report then has the burden of production, under Rule 32(c), to come forward with evidence that tends to indicate that the report is incorrect or incomplete.

U.S. v. McDowell, 888 F.2d 285, 291 n.1 (3d Cir. 1989).

Moreover, despite the absence of a challenge, the record supports the loss amount. FBI Special Agent Christine Schorle, in a sworn affidavit accompanying the criminal complaint, stated that "[t]o date, AT&T has spent approximately $73,000 in remedying the data breach. Those costs include, among other things,

the cost of contacting all iPad 3G customers to inform them of the breach and AT&T's response to it." A58. The District Court did not plainly err in finding that AT&T spent $73,167 notifying the victims of the security breach.

VI. THIS COURT SHOULD DECLINE TO CONSIDER ADDITIONAL ARGUMENTS RAISED ONLY IN THE *AMICUS* BRIEFS.

Amici have filed four brief in support of Auernheimer. Some of the briefs provide further information and argument in support of legal positions that Auernheimer has taken on appeal. But some of the *amici's* raise arguments that Auernheimer has not raised. This Court should decline to address issues that Auernheimer has not raised on appeal.

> [A]n *amicus* may not frame the issues for appeal. Absent the existence of "substantial public interests" calling us to depart from the general rule, we consider only issues argued in the briefs filed by the parties and not those argued in the briefs filed by interested nonparties.

DiBiase v. SmithKline Beacham Corp., 48 F.3d 719, 731 (3d Cir. 1995) (citations and quotation marks omitted). *Accord General Engineering Corp. v. V.I. Water & Power Authority,* 805 F.2d 88, 92 n.5 (3d Cir. 1986) ("Since [*amici's*] arguments present no jurisdictional issues or any extraordinary considerations, we decline to address the new issues raised in its brief."); *Knetsch v. U.S.*, 364 U.S. 361, 370 (1960) (Court had "no reason to pass upon" a "point made in an *amicus curie* brief" that "has never been advanced by the petitioners in this case").

This principle applies not only to entirely new issues, but also to issues raised and decided below that the appellant has chosen not to raise in its opening

appellate brief. *See N.J. Retail Merchants Ass'n v. Sidamon-Eristoff*, 669 F.3d 374 383 n.2 (3d Cir. 2012). Given the highly competent counsel that Auernheimer has here, and the significant issues he has raised, this Court should not address additional issues raised only in the *amicus* briefs. The Government will, however, address some of them briefly.[29]

A. This Court Should Not Consider The First Amendment Argument Raised By DMLP, And It Is Without Merit.

While before the District Court, Auernheimer argued that the charge contained in Count Two of the indictment violates the First Amendment because it attempts to criminalize his transmission to the press of publicly available information on a matter of important public concerns. A80. The Government responded that Count Two does not violate the First Amendment, A128-29, and the District Court agreed, A29. Auernheimer has not raised a First Amendment claim on appeal, and this Court should not address the issue.

In any event, the First Amendment claim raised by DMLP is without merit. DMLP argues that "under the First Amendment, disclosure of information of public importance cannot subject the defendant to additional punishment absent a state interest of the highest order." DMLP Br.6. That may well be the case, but

[29] The Government would be happy to provide supplemental briefing, if requested by the Court, on any of the issues raised by the *amici*.

that statement does not, in fact, describe what occurred here.

Auernheimer could have gone to a reporter and described in detail the security flaws in AT&T's server and the exact procedures he and Spitler took to breach AT&T's security. What he could not do, and what is not subject to First Amendment protection, is disclose the personal identifying information that he and Spitler obtained as a result of their breach of AT&T's security. The public interest was in relating the existence and nature of the problem, not in relating the personal identifying information of individual iPad users. It was Auernheimer's disclosure of personal identifying information that subjected him to additional punishment under the New Jersey statute. He was not subjected to additional punishment for merely informing the public of the existence of security lapses at AT&T.[30] As a result, he has no First Amendment claim.[31]

---

[30] DMLP suggests that the reporter at Gawker needed the personal identifying information to substantiate Auernheimer's claims. DMLP Br.10. The mere fact that a reporter requests a certain type of verification does not confer a license to do so. Certainly the reporter had other ways to verify Auernheimer's story. He could have gone to a computer expert to examine Spitler's slurper program and determine whether it would have worked. He could have contacted some of the victims to whom Auernheimer had sent e-mails and verified whether their security had been breached. While disclosing the personal identifying information of individuals was no doubt easy for Auernheimer and the reporter, it was not required for this story to become public.

[31] The principal case upon which DMLP relies in pressing its contention that New Jersey's statute should be subjected to First Amendment scrutiny is *Bartnicki*

B. This Court Should Not Consider The Ex Post Facto And Related Arguments Raised By A Group Of Security Researchers, And They Are Without Merit.

A group of security researchers ("SR") have filed an *amicus* briefing raising two arguments. First, SR argues that Auernheimer was improperly convicted because AT&T made a secret determination, after the fact, that Auernheimer's access of its servers was unauthorized. SR claims that this amounts to a "private criminal law," that cannot result in criminal liability, and may violate the Ex Post Facto Clause of the United States Constitution. These issues were not raised before the District Court and should not addressed for the first time on appeal. In any event, they are without merit.

There is no need for this Court to examine the contours of the Ex Post Facto Clause or the case law, if any, surrounding "private criminal laws." That is because the factual predicates for SR's legal arguments are flatly contradicted by

---

v. Vopper, 532 U.S. 514 (2001). But that case involved a civil claim against news organizations and an individual who had disclosed the contents of an illegally intercepted conversation on a matter of public importance, where none of the individuals sued had participated in the illegal interception. *Id.* at 525. Nothing in *Bartnicki* remotely suggests that the wrong-doer who had illegally intercepted the communications would receive First Amendment protection. *Id.* at 528. DMLP's reliance on *Ostergren v. Cuccinelli*, 615 F.3d 263 (4th Cir. 2010), is similarly misplaced because Ostergren did not improperly obtain the private information that she disclosed, but instead simply republished documents that the State had already disclosed publicly.

the record. SR argues that "[t]he data Mr. Auernheimer helped to access was intentionally made available by AT&T to the entire Internet, and access occurred through standard protocols that are used by every Web user." SR Br.3. The record does not support those assertions. As demonstrated in Point I(A), *supra*, AT&T did not design its system to make e-mail addresses available to the general public; rather, the system was designed to make individual e-mail addresses available to only the particular user who had provided that information to AT&T. And the steps Spitler took, with Auernheimer's assistance, were steps that only a sophisticated hacker could duplicate, and not steps taken by casual Web users. SR also argues that "no reasonable Internet user could have notice," SR Br.3, that the information was nonpublic. But, of course, Spitler himself knew that his access was unauthorized. A264, A318. Indeed, anyone would have known.[32]

Leaving aside the question of whether the Ex Post Facto Clause is implicated in a case involving actions by a private company, the Government agrees with

---

[32] In explaining what occurred here, SR uses the analogy of a librarian, and asserts that the information was publicly available because the librarian here (AT&T's server) gave Spitler permission to access the information he requested. SR Br.4-11. Actually, the librarian here initially denied Spitler access to the requested information, A255, and only after Spitler falsely identified himself to the librarian (using someone else's ICC-ID) and falsely told the librarian that he was using an iPad (by changing the user agent string), did the librarian agree to give him the requested information. This seems little different from taking out a library book using someone else's library card.

SR's contention that, if the information on AT&T's servers was intended to be open and available to the general public when Auernheimer and Spitler accessed it, and it became nonpublic only after the fact, then the conspirators did not violate the CFAA. Although AT&T certainly fixed the security flaw that Spitler exploited to gain access to the server, the relevant question put to the jury was whether Spitler's access to the server was unauthorized when he did it. The record supports that jury finding. If the record did not, then Auernheimer does not need the Ex Post Facto Clause to overturn the guilty verdicts.[33]

Finally, in making its public policy argument, SR asserts that what Auernheimer did was the same as what Consumers Union does when it tests for product safety. SR Br.18. Not really. Consumers Union purchases products in the open commercial market, thereby acquiring legal ownership, before it tests them. In that way, Consumers Union is like AT&T here, the legal owner of the property at issue, and not like Auernheimer and Spitler. Contrary to SR's contention, if Ralph Nader or Consumers Union wants to buy a car, analyze its computer systems, and report on what they find, that would not be a crime under any

[33] SR also invites this Court to adopt its characterization of the Ninth Circuit's holding in *Nosal* concerning liability under the CFAA for a violation of a company's written terms of computer usage policy. SR Br.13. But, as Auernheimer himself recognizes, DB24 & n.12, there is no terms of use agreement that the Government alleges was violated here.

interpretation of the CFAA put forward by the Government.

C. This Court Should Not Address the Vagueness And Jury Instruction Challenges Raised By NACDL, And They Are Without Merit.

While before the District Court, Auernheimer raised a vagueness challenge to the CFAA and sought dismissal of the indictment. A66-70. The Government opposed the motion, A90-105, and the District Court agreed with the Government, A21-23. NACDL argues that the District Court misinstructed the jury when it defined access without authorization as "access [to] a computer without approval or permission." NACDL Br.1. NACDL argues that, in order to avoid vagueness problems, the Court should have instructed the jury that access without authorization is limited to "computer hacking or, more precisely, circumventing a code-based barrier." NACDL Br.2. Auernheimer has opted not to raise a vagueness challenge to the CFAA in its opening brief on appeal, and it likewise has not challenged the jury instructions. Therefore, this Court should decline to reach the issues raised by NACDL. In any event, its claims are without merit.

Vagueness challenges that do not present First Amendment concerns must be judged on the facts of the case at hand, and not on the basis of hypotheticals. *Moyer*, 674 F.3d at 211. The question of unauthorized *access* under the CFAA does not raise any First Amendment issues. Importantly, Spitler admitted that he

knew his access here was unauthorized. Thus, this case simply is not a proper vehicle to raise a challenge to the vagueness of the statute.

NACDL asks in several hypotheticals, how a casual surfer of the internet would know when access is authorized by a website owner. But the CFAA criminalizes only access that is intentionally unauthorized or in excess of what is authorized. If the user does not in fact know, *as Spitler admittedly did here*, that his access was unauthorized, then he is not guilty of the crime. The Government is required to prove intentional misconduct beyond a reasonable doubt. Indeed, Congress amended the CFAA to limit its reach to intentional misconduct for this very reason. This is not a trap for the unwary.[34]

On the merits, this Court has noted, "[a] statute is unconstitutionally vague only if it fails provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits or authorizes arbitrary and discriminatory enforcement." *Moyer*, 674 F.3d at 211 (internal quotation marks omitted). Vagueness challenges in criminal cases "may be overcome in any specific case

---

[34] NACDL suggests that the Government's view here would criminalize internet searches that the NSA conducts and that the Government therefore has implicitly endorsed as legal. NACDL Br.4-5. It is well beyond the scope of the record in this case to discuss intelligently searches conducted by the NSA. Importantly, Congress specifically exempted "lawfully authorized investigative, protective, or intelligence activity" of entities like the NSA from the scope of the CFAA. *See* 18 U.S.C. § 1030(f).

where reasonable persons would know their conduct puts [them] at risk of punishment under the statute." *Id.* Here, a reasonable person would know that exploiting a vulnerability in AT&T computer servers by posing as actual, registered AT&T customers, and then harvesting the personal identifiers of more than 100,000 AT&T customers without their authorization or AT&T's, could lead to punishment under the statute. Certainly, Auernheimer knew that, when he described his actions as "theft" and tried to destroy the computer evidence of his misdeeds.[35]

[35] NACDL briefly discusses two highly-publicized CFAA cases – *U.S. v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), and the federal prosecution of Aaron Swartz. This is not a case like *Drew*, which involved a violation of *terms of use* on a website that otherwise was certainly *publicly available.* And without delving too deeply into the merits of the Swartz prosecution, the indictment alleged that Swartz utilized MIT's computers to carry out his scheme after circumventing repeated attempts by MIT to bar him from accessing their computer network. *See* http://www.documentcloud.org/documents/217117-united-states-of-america-v-aaron-swartz. That would, on its face, appear to be a textbook case of "unauthorized use" of a computer. *See* Orin Kerr, The Criminal Charges Against Aaron Swartz (Part 1: The Law) ("I think it's pretty clear that Swartz exceeded his authorized access here"), *available at* http://www.volokh.com/2013/01/14/aaron-swartz-charges/. It is hardly an example, as NACDL suggests, of the Government's use of a "patently defective" standard.

D. Auernheimer Has Not Argued, And This Court Should Not Decide, Whether Violation Of A "Code-Based Restriction" Is Required For Liability Under The CFAA.

Several of the *amici* argue that violations of the CFAA should be limited to code-based restrictions. This Court should decline the invitation of the *amici* to reach an issue that Auernheimer has not himself raised in his brief on appeal, and which is not presented on the facts of this case. This case is not an appropriate vehicle for addressing whether a violation of code-based restrictions is *required* in order to find a violation of the CFAA.

First, the jury instructions given by the District Court here render irrelevant to the outcome of this case the question of whether a violation of code-based restrictions is necessary in order to find a violation of the CFAA. The Court instructed the jury here that the object of the conspiracy, a violation of N.J.S.A. § 2C:20-31, required them to find that the access was "without password-based permission or code-based permission, or in violation of a code-based restriction by impersonating an authorized user," A705-06. As the Government conceded during the charge conference, if the jury did not find a violation of a code-based restriction, then there would and should be an acquittal on both counts. A568. The issue of whether a violation of the CFAA necessarily requires a finding of a violation of a code-based restriction simply is not presented in this case, and the

amici are asking for an advisory opinion.

Additionally, this case is not an appropriate vehicle for deciding the legal issue *amici* present because, contrary to their factual contention, the conspirators here did violate code-based restrictions when they hacked into AT&T's server. *See* Point II(B)(1), *supra*. Moreover, adopting a test for liability based on "code-based restrictions," is not the pancea that *amici* suggest. What constitutes a "code-based restriction" is subject to sharp disagreement that fails to solve the vagueness problems that allegedly infect the debate about authorized versus unauthorized access. *See* Kerr, "Cybercrime's Scope," 78 N.Y.U.L.R. at 1646 ("the distinction between regulation by code and regulation by contract is less an on-off switch than a continuum with two extremes. Examples exist that blend the two concepts."). This is not a suitable case to explore such intricacies.

E. The *Amici* Should Look To Congress, And Not The Courts, For The Particular Remedies They Seek.

Several of the *amici* trumpet the valuable contributions that they believe they have made and continue to make to the security of the internet. *Amici's* assertions about the value of their work, how it serves to improve the internet, and how they need unimpeded access to scrutinize the security of the data maintained on other people's computer networks, are all policy arguments that should be made to

Congress, not the Courts.

In adopting the CFAA, Congress established a law that criminalized the *intentional* and *unauthorized* access into someone else's computer. The Legislature is the proper body to decide if there security researchers need to have unimpeded access to private computer networks. Congress knows how to write whistle-blower protection or safe harbor provisions when it wants to, and only Congress can properly weigh the pros and cons of the policy-based arguments presented by *amici*.

This Court should interpret the CFAA as it is written, and not as *amici* would like it to have been written. Certainly there are legislative proposals for rewriting the CFAA that will do what *amici* seek. *See, e.g.*, Orin Kerr, "Aaron's Law, Drafting the Best Limits of the CFAA, And A Reader Poll on A Few Examples" (Jan. 27, 2013), *available at* http://www.volokh.com/2013/01/27/aarons-law-drafting-the-best-limits-of-the-cfaa-and-a-reader-poll-on-a-few-examples-part-i/. This case, however, is not a proper vehicle for rewriting the CFAA. *See, generally, NCAA v. Governor of New Jersey*, __ F.3d __, No. 13-1713, (3d Cir. Sept. 17, 2013) ("It is not our place to usurp Congress' role simply because PASPA may have become an unpopular law.").

CONCLUSION

For all these reasons, this Court should affirm the judgment of the District Court.

Respectfully submitted,
PAUL J. FISHMAN
United States Attorney

By: /s/ *Glenn J. Moramarco*
GLENN J. MORAMARCO
Assistant U.S. Attorney
401 Market St., 4th Floor
Camden, NJ 08101
(856) 968-4863

Date: September 20, 2013

CERTIFICATE OF COMPLIANCE

I hereby certify as an Assistant United States Attorney for the District of New Jersey that:

(1) this Brief for Appellee (the "Brief") does **not** comply with the length limitations of Fed. R. App. P. 32(a)(7) because it contains 26,495 words, which exceeds the normal 14,000-word limit. On August 5, 2013, the Government filed a motion requesting that it be permitted to file a brief not exceeding 26,500 words, which motion is still outstanding;

(2) the Brief complies with the typeface requirements of Fed. R. App. 32(a)(5) and the type style requirements of Fed. R. App. 32(a)(6) by using a Word Perfect X5 word-processing system and a proportionally-spaced typeface, namely Times New Roman, that is at least 14 points;

(3) the text of the PDF copy of the Brief is identical to the text of the paper copies of the Brief; and

(4) the PDF copy of the Brief was prepared on a computer that is automatically protected by a virus detection program, namely a continuously-updated version of Trend Micro OfficeScan, and no virus was detected.

/s/ *Glenn J. Moramarco*
GLENN J. MORAMARCO

Dated: September 20, 2013

CERTIFICATION OF FILING AND SERVICE

I hereby certify that on **September 20, 2013**, I caused the Brief for Appellee and the Supplemental Appendix for Appellee to be filed with the Clerk of the United States Court of Appeals for the Third Circuit via the Court's electronic filing system. I will deposit an original and nine paper copies of the brief and four copies of the Supplemental Appendix with the United States Postal Service as postage-prepaid first-class mail. Opposing counsel and *amici* will receive service via the Court's electronic filing system.

/s/ *Glenn J. Moramarco*
GLENN J. MORAMARCO

Dated: September 20, 2013