PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 13-1816

UNITED STATES OF AMERICA
v.

ANDREW AUERNHEIMER,
a/k/a Weev
a/k/a Weelos
a/k/a Escher

ANDREW AUERNHEIMER,
Appellant

On Appeal from the United States District Court
for the District of New Jersey
(No. 2:11-cr-00470-001)
District Judge: Hon. Susan D. Wigenton

Argued: March 19, 2014

Before: CHAGARES, GREENAWAY, JR., and
VANASKIE, Circuit Judges.

(Filed: April 11, 2014)

OPINION

Tor B. Ekeland, Esq.
Mark H. Jaffe, Esq.
Tor Ekeland, P.C.
155 Water Street.
Sixth Floor, Suite Two
Brooklyn, NY 11201

Orin S. Kerr, Esq. [ARGUED]
George Washington University
2000 H Street, N.W.
Washington, DC 20052

Marcia C. Hofmann, Esq.
25 Taylor Street
San Francisco, CA 94102

Hanni M. Fakhoury, Esq.
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Attorneys for Appellant

Paul J. Fishman, Esq.
Glenn J. Moramarco, Esq. [ARGUED]
Office of United States Attorney
Camden Federal Building & Courthouse
401 Market Street
Camden, NJ 08101

Mark E. Coyne, Esq.
Office of United States Attorney
970 Broad Street
Newark, NJ 07102
Attorneys for Appellee

Christopher C. Walsh, Esq.
Harvard Law School
Cyberlaw Clinic
23 Everett Street
Second Floor
Cambridge, MA 02138

Alexander C. Muentz, Esq.
Temple University
Department of Criminal Justice
1115 Pollett Walk
Philadelphia, PA 19122

Jennifer S. Granick, Esq.
Stanford Law School
Center for Internet & Society
559 Nathan Abbott Way
Stanford, CA 94305

Steven P. Ragland, Esq.
Keker & Van Nest
633 Battery Street
San Francisco, CA 94111
Attorneys for Amicus Appellants

CHAGARES, Circuit Judge.

This case calls upon us to determine whether venue for Andrew Auernheimer's prosecution for conspiracy to violate the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and identity fraud under 18 U.S.C. § 1028(a)(7) was proper in the District of New Jersey. Venue in criminal cases is more than a technicality; it involves "matters that touch closely the fair administration of criminal justice and public confidence in it." United States v. Johnson, 323 U.S. 273, 276 (1944). This is especially true of computer crimes in the era of mass interconnectivity. Because we conclude that venue did not lie in New Jersey, we will reverse the District Court's venue determination and vacate Auernheimer's conviction.

I.

A.

The relevant facts are fairly simple and not in dispute. Apple, Inc. introduced the first iPad, a tablet computer, in 2010. Customers who purchased the version that had the capability to send and receive data over cellular networks (commonly referred to as "3G") had to purchase a data contract from AT&T, Inc. ("AT&T"), which at the time was the exclusive provider of data services for this version of the iPad. Customers registered their accounts with AT&T over the Internet on a website that AT&T controlled. In the registration process, customers were assigned a user identifier

("user ID") and created a password — login credentials that they would need in order to access their accounts through AT&T's website in the future. The user ID assigned to each customer was that customer's email address.

AT&T decided to make it easier for customers to log into their accounts by prepopulating the user ID field on the login screen with their email addresses. To do this, AT&T programmed its servers to search for an iPad user's Integrated Circuit Card Identifier ("ICC-ID") when a user directed her browser to AT&T's general login webpage (AT&T's "URL"[1]). An ICC-ID is the unique nineteen- or twenty-digit number that identifies an iPad's Subscriber Identity Module, commonly known as a SIM Card. The SIM Card is the computer chip that allows iPads to connect to cellular data networks.

If AT&T's servers recognized the ICC-ID as associated with a customer who had registered her account with AT&T, then AT&T's servers would automatically redirect the customer's browser away from the general login URL to a different, specific URL. That new specific URL was unique for every customer and contained the customer's ICC-ID in the URL itself. Redirecting the customer's browser to the new specific URL told AT&T's servers which email address to populate in the user ID field on the login page. This shortcut reduced the amount of time it took a customer to log into her account because, with her user ID already populated, she had to enter only her password.[2]

---

[1] URL is shorthand for uniform resource locator, which is defined as "a specific address . . . used by a browser in locating the relevant document [on the Internet]." URL, Oxford Eng. Dictionary, http://www.oed.com/view/Entry/258858?redirectedFrom=URL#eid (last visited Mar. 27, 2014). It is more commonly known as a "web address." Appendix ("App.") 255.

[2] To make this more concrete, when an iPad user wanted to log into her account, she would direct her browser to "https://dcp2.att.com/OEPNDClient/". If AT&T's server recognized the ICC-ID of the iPad that made the request as an iPad that was already registered with AT&T, its servers would automatically redirect the user to

Daniel Spitler, Auernheimer's co-conspirator, discovered this feature of AT&T's login process. Although he did not own an iPad, he purchased an iPad SIM Card, hoping to install it on another computing device and then take advantage of the unlimited cellular data plan that AT&T offered for $30 per month. At first, he did not know how to register his SIM Card, so he downloaded the iPad operating system onto his computer, decrypted it, and browsed through the operating system's code to try to find a way to register it. In the course of doing so, he came across AT&T's registration URL. He noticed that one of the variables in the registration URL was a field requiring an ICC-ID.

Spitler then directed his computer's web browser to the registration URL and inserted his iPad's ICC-ID in the requisite place. AT&T's servers were programmed only to permit browsers that self-identified as iPad browsers to access the registration URL. This required him to change his browser's user agent. A user agent tells a website what kind of browser and operating system a user is running, so servers that someone is attempting to access can format their responses appropriately. App. 256.

After changing his browser's user agent to appear as an iPad, Spitler was able to access the AT&T login page. He noticed that his email address was already populated in the login field and surmised that AT&T's servers had tied his email address to his ICC-ID. He tested this theory by changing the ICC-ID in the URL by one digit and discovered that doing so returned a different email address. He changed the ICC-ID in the URL manually a few more times, and each time the server returned other email addresses in the login field.

Spitler concluded that this was potentially a noteworthy security flaw. He began to write a program that he called an "account slurper" that would automate this process. The account slurper would repeatedly access the

---

"https://dcp2.att.com/OEPNDClient/openPage?ICCID=XXXXXXXXXXXXXXXXXX&IMEI=0", where the string of "X"s is the nineteen- or twenty-digit ICC-ID.

AT&T website, each time changing the ICC-ID in the URL by one digit. If an email address appeared in the login box, the program would save that email address to a file under Spitler's control.

Spitler shared this discovery with Auernheimer, whom he knew through Internet-based chat rooms but had never met in person. Auernheimer helped him to refine his account slurper program, and the program ultimately collected 114,000 email addresses between June 5 and June 8, 2010. Its method — guessing at random — is called a "brute force" attack, a term of art in the computer industry referring to an inefficient method of simply checking all possible numbers.

While Spitler's program was still collecting email addresses, Auernheimer emailed various members of the media in order to publicize the pair's exploits. Some of those media members emailed AT&T, which immediately fixed the breach. One of the media members contacted by Auernheimer was Ryan Tate, a reporter at Gawker, a news website. Tate expressed interest in publishing Auernheimer's story. To lend credibility to it, Auernheimer shared the list of email addresses with him. Tate published a story on June 9, 2010 describing AT&T's security flaw, entitled "Apple's Worst Security Breach: 114,000 iPad Owners Exposed." The article mentioned some of the names of those whose email addresses were obtained, but published only redacted images of a few email addresses and ICC-IDs.

Evidence at trial showed that at all times relevant to this case, Spitler was in San Francisco, California and Auernheimer was in Fayetteville, Arkansas. The servers that they accessed were physically located in Dallas, Texas and Atlanta, Georgia. Although no evidence was presented regarding the location of the Gawker reporter, it is undisputed that he was not in New Jersey.

B.

Despite the absence of any apparent connection to New Jersey, a grand jury sitting in Newark returned a two-count superseding indictment charging Auernheimer with conspiracy to violate the CFAA, 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(ii), in violation of 18 U.S.C. § 371 (count one),

and fraud in connection with personal information in violation of 18 U.S.C. § 1028(a)(7) (count two, commonly referred to as "identity fraud"). To enhance the potential punishment from a misdemeanor to a felony, the Government alleged that Auernheimer's CFAA violation occurred in furtherance of a violation of New Jersey's computer crime statute, N.J. Stat. Ann. § 2C:20-31(a). See 18 U.S.C. § 1030(c)(2)(B)(ii).

Auernheimer moved to dismiss the superseding indictment shortly after it was returned by the grand jury. In addition to asserting several challenges concerning the CFAA violation, he argued that venue was not proper in the District of New Jersey. The District Court acknowledged that neither he nor Spitler was ever in New Jersey while allegedly committing the crime, and that the servers accessed were not in New Jersey, but denied his motion nonetheless. It held that venue was proper for the CFAA conspiracy charge because Auernheimer's disclosure of the email addresses of about 4,500 New Jersey residents affected them in New Jersey and violated New Jersey law. It further held that because venue was proper for the CFAA count, it was also proper for the identity fraud count because proving the CFAA violation was a necessary predicate to proving the identity fraud violation.

Auernheimer's trial lasted five days and resulted in a guilty verdict on both counts. Initially, both parties requested a jury instruction on venue. App. 575. Venue is a question for the jury and the court "must specifically instruct the jury on venue" if "(1) the defendant objects to venue prior to or at the close of the prosecution's case-in-chief, (2) there is a genuine issue of material fact with regard to proper venue, and (3) the defendant timely requests a jury instruction." United States v. Perez, 280 F.3d 318, 334 (3d Cir. 2002). Although Auernheimer objected to venue and requested an instruction, the District Court held that there was no genuine issue of material fact. It concluded that the Government had established that venue was proper in New Jersey as a matter of law and declined to instruct the jury on venue. App. 591.

After denying Auernheimer's post-trial motions, the District Court sentenced him to forty-one months of imprisonment. Auernheimer timely appealed.

II.

The District Court had jurisdiction pursuant to 18 U.S.C. § 3231. We have jurisdiction pursuant to 28 U.S.C. § 1291. Our review of the District Court's legal decision regarding venue is plenary. United States v. Pendleton, 658 F.3d 299, 302 (3d Cir. 2011).

III.

Although this appeal raises a number of complex and novel issues that are of great public importance in our increasingly interconnected age, we find it necessary to reach only one that has been fundamental since our country's founding: venue. The proper place of colonial trials was so important to the founding generation that it was listed as a grievance in the Declaration of Independence. See The Declaration of Independence para. 21 (U.S. 1776) (objecting to "transporting us beyond seas to be tried for pretended offences"). It was of such concern that the Constitution of the United States "twice safeguards the defendant's venue right." United States v. Cabrales, 524 U.S. 1, 6 (1998). Article III requires that "the Trial of all Crimes . . . shall be held in the State where the said Crimes shall have been committed." U.S. Const. art. III, § 2, cl. 3. The Sixth Amendment further provides that "[i]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed." Id. amend VI. This guarantee is codified in the Federal Rules of Criminal Procedure, which require that "the [G]overnment must prosecute an offense in a district where the offense was committed." Fed. R. Crim. P. 18.

Congress may prescribe specific venue requirements for particular crimes. Pendleton, 658 F.3d at 303. Where it has not, as is the case here, we must determine the crime's locus delicti. Id.; see also Black's Law Dictionary 1025 (9th ed. 2009) (defining locus delicti as the "place where an offense was committed"). "[T]he locus delicti must be determined from the nature of the crime alleged and the location of the act or acts constituting it." United States v. Anderson, 328 U.S. 699, 703 (1946); accord United States v.

Rodriguez-Moreno, 526 U.S. 275, 279 (1999); Cabrales, 524 U.S. at 6-7. To perform this inquiry, we "must [1] initially identify the conduct constituting the offense . . . and then [2] discern the location of the commission of the criminal acts." Rodriguez-Moreno, 526 U.S. at 279. Venue should be narrowly construed. Johnson, 323 U.S. at 276.

Continuing offenses, such as conspiracy, that are "begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a). In the context of a conspiracy charge, "venue can be established wherever a co-conspirator has committed an act in furtherance of the conspiracy." Perez, 280 F.3d at 329; accord Hyde v. United States, 225 U.S. 347, 356-67 (1912). The Government must prove venue by a preponderance of the evidence. United States v. Root, 585 F.3d 145, 155 (3d Cir. 2009).

In performing our venue inquiry, we must be careful to separate "essential conduct elements" from "circumstance element[s]." Rodriguez-Moreno, 526 U.S. at 280 & n.4. For example, in Cabrales the Supreme Court considered whether venue for money laundering activities was proper in Missouri. 524 U.S. at 4. The laundered proceeds were generated by illegal narcotics sales in Missouri, but all acts constituting the money laundering offense took place in Florida. Id. The Court held that venue was improper in Missouri. Id. at 10. The Supreme Court, later reflecting on Cabrales, observed that the "existence of criminally generated proceeds" was only a "circumstance element" of money laundering. Rodriguez-Moreno, 526 U.S. at 280 n.4. Although it was an element of the crime that the Government had to prove to the jury, it was a "circumstance element" because it was simply a fact that existed at the time that the defendant performed her laundering acts. Only "essential conduct elements" can provide the basis for venue; "circumstance elements" cannot. United States v. Bowens, 224 F.3d 302, 310 (4th Cir. 2000).

A.

Count one charged Auernheimer with conspiracy to violate CFAA § 1030(a)(2)(C) and (c)(2)(B)(ii). In the

indictment and at trial, the Government identified the nature of the conduct constituting the offense as the agreement to commit a violation of the CFAA in furtherance of a violation of New Jersey's computer crime statute, N.J. Stat. Ann. § 2C:20-31(a). Venue would be proper in any district where the CFAA violation occurred, or wherever any of the acts in furtherance of the conspiracy took place. See Perez, 280 F.3d at 329; see also Rodriguez-Moreno, 526 U.S. at 281-82 (citing Hyde, 225 U.S. at 356-67).

The charged portion of the CFAA provides that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section." 18 U.S.C. § 1030(a)(2)(C). To be found guilty, the Government must prove that the defendant (1) intentionally (2) accessed without authorization (or exceeded authorized access to) a (3) protected computer and (4) thereby obtained information. See United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007) (delineating the elements in a similar manner). The statute's plain language reveals two essential conduct elements: accessing without authorization and obtaining information.[3]

New Jersey was not the site of either essential conduct element. The evidence at trial demonstrated that the accessed AT&T servers were located in Dallas, Texas, and Atlanta, Georgia. App. 443-44. In addition, during the time that the conspiracy began, continued, and ended, Spitler was obtaining information in San Francisco, California (App. 233), and Auernheimer was assisting him from Fayetteville, Arkansas (App. 366). No protected computer was accessed and no data was obtained in New Jersey.

[3] The Department of Justice's own manual on prosecuting computer crimes provides in its section devoted to venue that "it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access and where the information is obtained." Computer Crime & Intellectual Prop. Section, Dep't of Justice, Prosecuting Computer Crimes 118, available at http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (last visited Mar. 26, 2014) ("DOJ Manual").

This is not the end of our analysis, however, because the Government did not just charge Auernheimer with conspiracy to commit an ordinary violation of the CFAA, but also with conspiring to violate the CFAA in furtherance of a state crime. The Government can increase the statutory maximum punishment for a subsection (a)(2) violation from one year to five years if it proves one of the enhancements contained in § 1030(c)(2)(B). The enhancement relevant here provides for such increased punishment if "the offense was committed in furtherance of any criminal or tortious act in violation of the . . . laws of . . . any State." Id. § 1030(c)(2)(B)(ii). "[A]ny 'facts that increase the prescribed range of penalties to which the criminal defendant is exposed' are elements of the crime" that must be proven to the jury beyond a reasonable doubt.[4] Alleyne v. United States, 133 S. Ct. 2151, 2160 (2013) (quoting Apprendi v. New Jersey, 530 U.S. 466, 490 (2000)). This is true even if they are explicitly termed "sentence enhancement[s]" in the statute. Apprendi, 530 U.S. at 494 n.19 (quotation marks omitted).

The New Jersey statute allows for criminal liability "if the person purposely or knowingly and without authorization, or in excess of authorization, accesses any . . . computer [or] computer system and knowingly or recklessly discloses, or causes to be disclosed any data . . . or personal identifying information." N.J. Stat. Ann. § 2C:20-31(a). Its essential conduct elements are accessing without authorization (or in excess of authorization) and disclosing data or personal identifying information.

Here, none of the essential conduct elements of a violation of the New Jersey statute occurred in New Jersey. As discussed, neither Auernheimer nor Spitler accessed a

[4] Just because the enhancement is an "element" that the Government needed to prove beyond a reasonable doubt does not mean that it was an "essential conduct element" of a § 1030(a)(2)(C) violation within the meaning of Rodriguez-Moreno that could establish venue. For the purposes of this opinion, however, we will assume (without deciding) that the enhancement could contain "essential conduct elements."

computer in New Jersey.[5] The disclosure did not occur there either. The sole disclosure of the data obtained was to the Gawker reporter. There was no allegation or evidence that the Gawker reporter was in New Jersey. Further, there was no evidence that any email addresses of any New Jersey residents were ever disclosed publicly in the Gawker article. The alleged violation of the New Jersey statute thus cannot confer venue for count one.

Just as none of the conduct constituting the CFAA violation or its enhancement occurred in New Jersey, none of the overt acts that the Government alleged in the superseding indictment occurred in New Jersey either. The indictment listed four overt acts: writing the account slurper program, deploying the account slurper program against AT&T's servers, emailing victims to inform them of the breach, and disclosing the emails addresses obtained to Gawker. The co-conspirators collaborated on the account slurper program from California and Arkansas and deployed it against servers located in Texas and Georgia. The Government offered no evidence whatsoever that any of the victims that Auernheimer emailed were located in New Jersey, or that the Gawker reporter to whom the list of email addresses was disclosed was in the Garden State.

Because neither Auernheimer nor his co-conspirator Spitler performed any "essential conduct element" of the underlying CFAA violation or any overt act in furtherance of the conspiracy in New Jersey, venue was improper on count one.

---

[5] We also note that in order to be guilty of accessing "without authorization, or in excess of authorization" under New Jersey law, the Government needed to prove that Auernheimer or Spitler circumvented a code- or password-based barrier to access. See State v. Riley, 988 A.2d 1252, 1267 (N.J. Super. Ct. Law Div. 2009). Although we need not resolve whether Auernheimer's conduct involved such a breach, no evidence was advanced at trial that the account slurper ever breached any password gate or other code-based barrier. The account slurper simply accessed the publicly facing portion of the login screen and scraped information that AT&T unintentionally published.

B.

We now turn to count two of the indictment because venue must be analyzed independently for each count. See Root, 585 F.3d at 155. Count two charged Auernheimer with violating 18 U.S.C. § 1028(a)(7), which punishes anyone 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 [federal crime, or state or local felony]." The statute's plain language indicates that the statute punishes someone who (1) knowingly (2) transfers, possesses, or uses without lawful authority (3) a means of identification of another person (4) with the intent to commit, or in connection with, any violation of federal law or any state felony. See United States v. Abdelshafi, 592 F.3d 602, 607 (4th Cir. 2010) (delineating the elements of a violation of aggravated identity fraud in 18 U.S.C. § 1028A(a)(1), which are virtually identical, in a similar fashion); United States v. Stephens, 571 F.3d 401, 404-05 (5th Cir. 2009) (same).

The two essential conduct elements under § 1028(a)(7) are transfer, possession, or use, and doing so in connection with a federal crime or state felony. Cf. Rodriguez-Moreno, 526 U.S. at 280 (noting that "during and in relation to any crime of violence" was an essential conduct element of a firearms statute). Starting with the latter essential conduct element, the Government charged Auernheimer with committing identity fraud "in connection with" the ordinary violation of CFAA § 1030(a)(2)(C). As should be clear by now, no conduct related to the ordinary CFAA violation occurred in New Jersey.

There was also no evidence that Auernheimer's transfer, possession, or use occurred in New Jersey. The Government advances two theories of how he could have satisfied this essential conduct element. First, it contends that he violated § 1028(a)(7) by knowingly using the ICC-IDs of other people's iPads to access AT&T's servers. See Gov't Br. 64-66. Venue fails under this theory because there was no allegation or evidence that he used the ICC-IDs in New Jersey. The alleged conspirators used the ICC-IDs in their

account slurper program, which was programmed from California and Arkansas, and did not access any computer or obtain any information in New Jersey.

The Government also argues that Auernheimer violated the statute by transferring the list of email addresses that he obtained to Gawker with the intent to violate the New Jersey computer crime statute. See Gov't Br. 67-69. But there was no allegation in the indictment or evidence at trial that the Gawker reporter to whom he transferred the email addresses was in New Jersey — and no essential conduct element of the alleged violation of New Jersey law occurred in New Jersey either.[6]

Because Auernheimer did not commit any essential conduct of the identity fraud charge in New Jersey, venue was also improper on count two.

IV.

The Government does not dispute the locations of Auernheimer, Spitler, and AT&T's servers during the period of time that Auernheimer was committing the alleged crimes. Instead, it advances a series of other reasons why there was no defect in venue that warrants vacating his conviction. None of them are availing.

A.

The Government argues that we need not rely on the essential conduct elements test mandated by Cabrales and Rodriguez-Moreno because we have "adopted," Gov't Br. 71,

[6] Further, count two of the indictment charged Auernheimer with transferring, possessing, and using the means of identification of others in connection with only an ordinary violation of CFAA § 1030(a)(2)(C). It did not mention the violation of New Jersey law or the § 1030(c)(2)(B)(ii) enhancement at all. This second theory thus "broaden[s] the possible bases for conviction from that which appeared in the indictment." United States v. McKee, 506 F.3d 225, 229 (3d Cir. 2007) (quotation marks omitted). It cannot be a permissible basis upon which to find venue for count two.

a "substantial contacts test." Under this approach, frequently employed by the Court of Appeals for the Second Circuit, a number of factors help to determine whether venue was proper, including "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 factfinding." United States v. Reed, 773 F.2d 477, 481 (2d Cir. 1985). The Government contends that venue is proper in New Jersey because about four percent (approximately 4,500 of 114,000) of the email addresses obtained from AT&T's website belonged to New Jersey residents, thereby satisfying the "locus of the effect[s]" consideration. See id.

It is far from clear that this Court has ever "adopted" this test. We have mentioned it only once. See United States v. Goldberg, 830 F.2d 459, 466 (3d Cir. 1987). The test was cited in a long block quote to Reed, and then analyzed in a single sentence. Id. The Goldberg panel did not need to rely on the locus of the effects of the defendant's conduct in that case because all of his acts took place in the district in which he was tried. Id. No panel of this Court has ever cited Goldberg, or any other case, for this test since — either before, or especially after, the Supreme Court clarified the venue inquiry in Cabrales and Rodriguez-Moreno.

Even if it could be said that we perhaps tacitly endorsed this test once almost thirty years ago, the test operates to limit venue, not to expand it. Cases from the Court of Appeals for the Second Circuit make this clear. The test "does not represent a formal constitutional test," but rather is merely "helpful in determining whether a chosen venue is unfair or prejudicial to a defendant." United States v. Saavedra, 223 F.3d 85, 93 (2d Cir. 2000). To satisfy this test, there must be "more than 'some activity in the situs district'; instead, there must be 'substantial contacts.'" United States v. Davis, 689 F.3d 179, 186 (2d Cir. 2012) (quoting Reed, 773 F.2d at 481). There "must be some sense of venue having been freely chosen by the defendant." Id. (alteration and quotation marks omitted). If a defendant argues that the chosen venue is constitutionally infirm but that it did not result in any hardship to him, the court only determines the locus delicti and does not then analyze

whether there were "substantial contacts." See United States v. Magassouba, 619 F.3d 202, 205 n.2 (2d Cir. 2010). This test thus serves to limit venue in instances where the locus delicti constitutionally allows for a given venue, but trying the case there is somehow prejudicial or unfair to the defendant.

Even assuming that the substantial contacts test is viable within our Circuit, it cannot serve as a sufficient basis for conferring venue. The Government argues only that it has minimally satisfied one of the four prongs of the test — the "locus of the effect of the criminal conduct." There was no evidence at trial that Auernheimer's actions evinced any contact with New Jersey, much less contact that was "substantial." The Government has not cited, and we have not found, any case where the locus of the effects, standing by itself, was sufficient to confer constitutionally sound venue.

Undoubtedly there are some instances where the location in which a crime's effects are felt is relevant to determining whether venue is proper. See Rodriguez-Moreno, 526 U.S. at 279 n.2 (reserving the issue of whether venue may also be permissibly based on the location where a crime's effects are felt). But those cases are reserved for situations in which "an essential conduct element is itself defined in terms of its effects." Bowens, 224 F.3d at 311. For example, in a prosecution for Hobbs Act robbery, venue may be proper in any district where commerce is affected because the terms of the act themselves forbid affecting commerce. See 18 U.S.C. § 1951(a); accord United States v. Smith, 198 F.3d 377, 383 (2d Cir. 1999). This is consistent with Congress's prerogative to "provide that the locality of a crime shall extend over the whole area through which force propelled by an offender operates." Johnson, 323 U.S. at 275.

Sections of the CFAA other than § 1030(a)(2)(C) do speak in terms of their effects. For example, § 1030(a)(5)(B) criminalizes intentionally accessing a computer without authorization and recklessly causing damage. Because that

crime is defined in terms of its effects — the damage caused — venue could be proper wherever that occurred.[7]

Congress, however, did not define a violation of § 1030(a)(2)(C) in terms of its effects. The statute simply criminalizes accessing a computer without authorization and obtaining information. It punishes only the actions that the defendant takes to access and obtain. It does not speak in terms of the effects on those whose information is obtained. The crime is complete even if the offender never looks at the information and immediately destroys it, or the victim has no idea that information was ever taken.

B.

The Government also argues that venue was proper in New Jersey because Auernheimer failed to obtain authorization from approximately 4,500 New Jersey residents to "use[] their ICC-ID numbers to access the AT&T servers." Gov't Br. 80. The Government argues that when a statute makes it a crime to fail to do some required act, venue can lie in the district in which the act should have been done. The Government concludes that venue is proper because Auernheimer and Spitler failed to obtain authorization from about 4,500 people in New Jersey prior to accessing AT&T's servers.

This rule only applies, however, when a preexisting legal duty requires the act that the defendant failed to do. See 1 Wayne R. LaFave, Substantive Criminal Law § 6.2(a) (2d ed. 2003) (noting that crimes of omission are generally limited by specific duties such as relationship, statute, contract, assumption of care, creation of peril, controlling the conduct of others, and landowner); accord United States v. Sabhnani, 599 F.3d 215, 237 (2d Cir. 2010). Failure to

[7] The Department of Justice manual again tailors its guidance to this assessment, noting that a prosecution under § 1030(a)(5) "may be brought where the effects are felt because those charges are defined in terms of 'loss,' even if the bulk of network crimes may not be prosecuted in a district simply because the effects of the crime are felt there." DOJ Manual at 120.

perform a required act could confer venue where a defendant should have performed that act when a statute penalizes inaction, such as failure to report to a military draft board (see, e.g., Johnston v. United States, 351 U.S. 215, 219-20 (1956)), failure to report to prison after being sentenced (see, e.g., United States v. Overaker, 766 F.2d 1326, 1327 (9th Cir. 1985)), or failure to file income tax returns (see, e.g., United States v. Garman, 748 F.2d 218, 219 (4th Cir. 1984)). Here, Auernheimer was under no such preexisting duty — legal or otherwise. Like most statutes, the charged portion of the CFAA punishes affirmative acts, not inaction. His failure to obtain authorization cannot confer venue in every district in which a potential victim lived.

C.

Finally, the Government argues that even if venue were improper, we should apply harmless error analysis and disregard the error because it did "not affect substantial rights." Fed. R. Crim. P. 52(a). Although the Government makes this argument only in passing — it occupies less than one page of its 118-page brief — we feel obliged to address it. The Government contends that its choice of forum actually benefitted Auernheimer, because locating his trial in Newark, New Jersey "enhance[d] his ability to attract and retain experienced and capable counsel on a pro bono basis." Gov't Br. 98; see also id. at 97 (noting that Newark was a "relatively easy commute" for Auernheimer's attorney from his office in Brooklyn, New York).

At the outset, we are skeptical that venue errors are susceptible to harmless error analysis. The Supreme Court has divided constitutional errors into two classes: "trial" and "structural." Arizona v. Fulminante, 499 U.S. 279, 307-10 (1991). Trial errors occur "during the presentation of the case to the jury" and can be "quantitatively assessed in the context of other evidence presented" in order to determine whether they are "harmless beyond a reasonable doubt." Id. at 307-08. These include "most constitutional errors." Id. at 306. Structural errors "defy" harmless error analysis because they "affect[] the framework within which the trial proceeds," id. at 309-10, "or indeed [] whether it proceeds at all," United States v. Gonzalez-Lopez, 548 U.S. 140, 150 (2006). These

include a "limited class of fundamental constitutional errors," Neder v. United States, 527 U.S. 1, 7 (1999), such as the denial of the rights to counsel, self-representation, or a public trial. See Gonzales-Lopez, 548 U.S. at 149 (listing examples and authority).

An error regarding venue exhibits many of the characteristics of structural error. If the District Court had found venue lacking upon Auernheimer's motion to dismiss, there would have been no trial in New Jersey at all. Even if venue had been raised only at trial, "if venue is improper no constitutionally valid verdict could be reached regardless of the [potentially] overwhelming evidence against the defendant." United States v. Miller, 111 F.3d 747, 757 (10th Cir. 1997) (Barrett, J., dissenting). The error thus "def[ies] analysis by harmless-error standards by affecting the entire adjudicatory framework." Puckett v. United States, 556 U.S. 129, 141 (2009) (quotation marks omitted). Holding that defective venue could ever be harmless would arguably reduce this constitutional protection to a nullity because, under the Government's formulation, the error would be harmless as long as the evidence against the accused of the substantive crime was overwhelming. It is doubtful that this is the way the venue protections in the Constitution were meant to operate. See also 4 Wayne R. LaFave et al., Criminal Procedure § 16.1(g) (4th ed. 2007) ("Failure of venue will not be treated as harmless error.").

The Supreme Court has never held that improper venue is subject to harmless error review. The Government has pointed to only one case where a court subjected defective venue to harmless error review. See United States v. Hart-Williams, 967 F. Supp. 73, 78-81 (E.D.N.Y. 1997). In Hart-Williams, the district court found the venue error harmless after the defendant was convicted at a courthouse in Brooklyn, New York, that was less than a mile from the courthouse where venue would have been proper in Manhattan, New York. See id. at 80. No court has cited Hart-Williams for this proposition, and the Court of Appeals for the Second Circuit has cast doubt on whether the district court's application of harmless error review remains good law. See United States v. Brennan, 183 F.3d 139, 149 (2d Cir. 1999) (holding that trial in Brooklyn, New York, where

venue was improper, was not harmless when the defendant timely objected to venue, even though venue would have been proper in Manhattan, New York); see also Saavedra, 223 F.3d at 100 n.5 (Cabranes, J., dissenting) (explicitly noting that Brennan forecloses applying harmless error analysis to defective venue).

Nonetheless, even assuming that defective venue could be amenable to harmless error review, the venue error here clearly affected Auernheimer's substantial rights. In order for an error to be harmless, "the Government must 'prove beyond a reasonable doubt that the error complained of did not contribute to the verdict obtained.'" Gov't of V.I. v. Davis, 561 F.3d 159, 165 (3d Cir. 2009) (quoting Chapman v. California, 386 U.S. 18, 24 (1967)). The question "is not whether, in a trial that occurred without the error, a guilty verdict would surely have been rendered, but whether the guilty verdict actually rendered in this trial was surely unattributable to the error." Sullivan v. Louisiana, 508 U.S. 275, 279 (1993). The venue error in this case is not harmless because there was no evidence that any of the essential conduct elements occurred in New Jersey. If Auernheimer's jury had been properly instructed on venue, it could not have returned a guilty verdict; the verdict rendered in this trial would have been different. See United States v. Durades, 607 F.2d 818, 820 (9th Cir. 1979) (failing to try defendant in district where crime was allegedly committed infringed the defendant's substantial rights); see also United States v. Glenn, 828 F.2d 855, 860 (1st Cir. 1987) (same); United States v. Stratton, 649 F.2d 1066, 1076 n.15 (5th Cir. 1981) ("A defendant's interest in being tried only in a district where venue properly lay clearly constitutes a substantial right." (quotation marks omitted)).

The Supreme Court has repeatedly made clear that the constitutional limitations on venue are extraordinarily important. "[Q]uestions of venue are more than matters of mere procedure. They raise deep issues of public policy in the light of which legislation must be construed." Travis v. United States, 364 U.S. 631, 634 (1961) (quotation marks omitted). "The provision for trial in the vicinity of the crime is a safeguard against the unfairness and hardship involved when an accused is prosecuted in a remote place." United

States v. Cores, 356 U.S. 405, 407 (1958); accord United States v. Passodelis, 615 F.2d 975, 977 (3d Cir. 1980). The founders were so concerned with the location of a criminal trial that they placed the venue requirement, which is "principally a protection for the defendant," Cabrales, 524 U.S. at 9, in the Constitution in two places. See U.S. Const. art. III, § 2, cl. 3 and amend. VI.

They did so for good reason. A defendant who has been convicted "in a distant, remote, or unfriendly forum solely at the prosecutor's whim," United States v. Salinas, 373 F.3d 161, 164 (1st Cir. 2004), has had his substantial rights compromised. Auernheimer was hauled over a thousand miles from Fayetteville, Arkansas to New Jersey. Certainly if he had directed his criminal activity toward New Jersey to the extent that either he or his co-conspirator committed an act in furtherance of their conspiracy there, or performed one of the essential conduct elements of the charged offenses there, he would have no grounds to complain about his uprooting. But that was not what was alleged or what happened. While we are not prepared today to hold that an error of venue never could be harmless,[8] we do not need to because the improper venue here — far from where he performed any of his allegedly criminal acts —

[8] We note that we are not dealing with a situation where the error complained of is that the trial judge failed to instruct the jury on venue. That claim may be reviewed for harmless error. See United States v. Casch, 448 F.3d 1115, 1117-18 (9th Cir. 2006) (noting that when proof of venue is clear, failure to instruct the jury can be considered harmless error); United States v. Martinez, 901 F.2d 374, 377 (4th Cir. 1990) (same); United States v. Moeckly, 769 F.2d 453, 461 (8th Cir. 1985) (same). In that situation, the failure to instruct would be harmless if the Government demonstrates under the Chapman standard that sufficient evidence of venue existed such that the jury would have come to that conclusion too. Cf. Neder, 527 U.S. at 7-11 (holding that an erroneous jury instruction that omitted an element of the offense is subject to harmless error analysis). The question that we address today is whether a venue defect could be harmless when there is no possibility that the jury could have found venue proper.

denied Auernheimer's substantial right to be tried in the place where his alleged crime was committed.[9]

V.

Venue issues are animated in part by the "danger of allowing the [G]overnment to choose its forum free from any external constraints." Salinas, 373 F.3d at 169-70 (citing Travis, 364 U.S. at 634). The ever-increasing ubiquity of the Internet only amplifies this concern. As we progress technologically, we must remain mindful that cybercrimes do not happen in some metaphysical location that justifies disregarding constitutional limits on venue. People and computers still exist in identifiable places in the physical world. When people commit crimes, we have the ability and obligation to ensure that they do not stand to account for those crimes in forums in which they performed no "essential conduct element" of the crimes charged. Rodriguez-Moreno, 526 U.S. at 280.

"Though our nation has changed in ways which it is difficult to imagine that the Framers of the Constitution could have foreseen, the rights of criminal defendants which they sought to protect in the venue provisions of the Constitution are neither outdated nor outmoded." Passodelis, 615 F.2d at 977. Just as this was true when we decided Passodelis in 1980 — after the advent of railroad, express mail, the telegraph, the telephone, the automobile, air travel, and satellite communications — it remains true in today's Internet age. For the forgoing reasons, we will reverse the District Court's venue determination and vacate Auernheimer's conviction.

[9] We in no way imply that venue cannot be waived by the defendant by failing to object to it in a timely fashion. See Perez, 280 F.3d at 328. Because Auernheimer explicitly moved to dismiss the indictment for lack of venue, there is no contention that he waived his venue right here.