WHERE TO PROSECUTE CYBERCRIMES

JACOB TAKA WALL[†]

ABSTRACT

Selecting the appropriate venue for a criminal trial has been a matter of constitutional concern since the founding of the country. The issue is thought to be essential to the fair administration of justice and thus public confidence in the criminal justice system. Constitutionally, crimes must be prosecuted in the states and districts in which they were committed. However, the rise of cybercrime has complicated the venue inquiry: cyberspace, the domain of cybercrime, and physical space have become increasingly decoupled. Consequently, under America's primary but dated cybercrime law, the ideal location for a trial may not be a constitutionally proper venue. This Note explores several possible approaches to permitting cybercrime trials to take place in the locations where they belong, including through an old but recently revisited judicially-created test for venue and through possible legislative reform.

[†] Duke University School of Law, J.D. expected, May 2020; The Evergreen State College, B.S., June 2017.

INTRODUCTION

Andrew Auernheimer is a hacker and self-proclaimed Internet "troll,"[1] as well as a notorious "neo-Nazi white supremacist."[2] Over the years, Auernheimer has claimed a lengthy list of cyber-exploits.[3] In one of his most infamous, he and a co-conspirator discovered a vulnerability in AT&T's customer login system,[4] which they programmatically exploited to harvest the email addresses of 114,000 AT&T customers.[5] Consequently, on March 18, 2013,[6] he was convicted of violating the Computer Fraud and Abuse Act[7]—the primary federal statute used to prosecute computer hacking[8]—and sentenced to 41 months in prison.[9] Following his release from prison, Auernheimer publicly declared

---

[1] *See* Tom McCarthy, *Andrew Auernheimer's Conviction over Computer Fraud Thrown Out*, GUARDIAN (Apr. 11, 2014, 1:18 PM), https://www.theguardian.com/technology/2014/apr/11/andrew-auernheimers-weev-conviction-vacated-hacking ("Auernheimer, a self-described internet troll and hacker, was found guilty in November 2012 conspiracy to gain unauthorised access to AT&T public servers, after he obtained thousands of email addresses of iPad owners.").

[2] *Andrew "Weev" Auernheimer*, S. POVERTY L. CTR., https://www.splcenter.org/fighting-hate/extremist-files/individual/andrew-%E2%80%9Cweev%E2%80%9D-auernheimer.

[3] *See* Adrian Chen, *The Internet's Best Terrible Person Goes to Jail: Can a Reviled Master Troll Become a Geek Hero?*, GAWKER (Nov. 27, 2012, 10:05 AM), http://gawker.com/5962159/the-internets-best-terrible-person-goes-to-jail-can-a-reviled-master-troll-become-a-geek-hero ("He was the star of a blockbuster 2008 *New York Times* magazine profile about internet trolling, the art of provoking online for provocation's sake. 'I hack, I ruin lives, I make piles of money,' he boasted in the *Times*. He's also taken credit for attacks on Livejournal and Amazon, shocked audiences on live Australian television, and served as the president of an internet trolling organization whose very name the government prosecutor in charge of his case would not pronounce.").

[4] United States v. Auernheimer, 748 F.3d 525, 530 (3d Cir. 2014).

[5] *Id.* at 531.

[6] Kim Zetter, *AT&T Hacker 'Weev' Sentenced to 3.5 Years in Prison*, WIRED (Mar. 18, 2013, 11:57 AM), https://www.wired.com/2013/03/att-hacker-gets-3-years/.

[7] 18 U.S.C. § 1030 (2012).

[8] *See* Elkin Girgenti, *Computer Crimes*, 55 AM. CRIM. L. REV. 911, 921 (2018) ("The Computer Fraud and Abuse Act ('CFAA') is the primary federal statute used to prosecute the unauthorized access and use of computers and computer networks.").

[9] *Auernheimer*, 748 F.3d at 532.

himself a neo-Nazi, although he conceded that he had long been a "critic of Judaism."[10] He is also Jewish.[11]

On April 11, 2014, approximately 13 months into his sentence, the Third Circuit vacated Auernheimer's conviction.[12] The court determined "that venue did not lie in New Jersey," where he was tried and convicted.[13] Although Auernheimer obtained and disclosed the email addresses of thousands of New Jersey residents, "neither he nor [his co-conspirator] was ever in New Jersey while allegedly committing the crime," and "the servers accessed were not in New Jersey."[14]

I. VENUE GENERALLY

The Auernheimer case exemplifies a recurring issue in cybercrime prosecutions.[15] Venue is the place where a defendant may stand trial, and it properly lies where the crime was committed.[16] "But, in today's wired world of telecommunication and technology, it is often difficult to determine exactly where a crime was committed, since different elements may be widely scattered in both time and space, and those elements may not coincide with the accused's actual presence."[17] In the age of the Internet, a cybercriminal, his target computer, and his actual, human victims—those who genuinely experience the harm of his actions—are often located in different, distant states, thus obscuring the location where the crime was committed and complicating the venue inquiry. This Note examines the approaches that federal courts have taken to resolve this issue, including the prevailing approach of, in effect,

---

[10] Andrew Auernheimer, *What I Learned from My Time in Prison*, DAILY STORMER (Oct. 1, 2014), https://dailystormer.name/what-i-learned-from-my-time-in-prison/.

[11] Michael Edison Hayden, *Neo-Nazi Who Calls for 'Slaughter' of Jewish Children Is of Jewish Descent, His Mom Says*, NEWSWEEK (Jan. 3, 2018, 6:25 AM), https://www.newsweek.com/neo-nazi-andrew-weev-auernheimer-daily-stormer-jewish-descent-768805.

[12] *Auernheimer*, 748 F.3d at 529.

[13] *Id.*

[14] *Id.* at 531.

[15] *See generally* OFFICE OF LEGAL EDUC., U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 116–20 (2d ed. 2015) [hereinafter PROSECUTING COMPUTER CRIMES], *available at* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (describing the issues and ambiguities of venue in cybercrime prosecutions).

[16] *See* U.S. CONST. art. III, § 2, cl. 3 ("The Trial of all Crimes, except in Cases of Impeachment, shall be by Jury; and such Trial shall be held in the State where the said Crimes shall have been committed . . . .").

[17] United States v. Saavedra, 223 F.3d 85, 86 (2d Cir. 2000).

not resolving it at all. Until cybercrime venue is more properly specified, either by the courts or by statute, it will remain a source of ambiguity in the prosecution of cybercrimes and a convenient option for defendants to challenge the charges against them without addressing the merits of their cases and conduct.

A. Constitutional Basis

In criminal proceedings, a defendant's venue right arises from two clauses of the Constitution.[18] First, the Constitution specifies that "The Trial of all Crimes . . . shall be held in the State where the said Crimes shall have been committed . . . ."[19] Second, the Vicinage Clause guarantees the accused in all criminal prosecutions the right to trial "by an impartial jury of the State and district wherein the crime shall have been committed."[20] The Federal Rules of Criminal Procedure echo the constitutional commands, requiring prosecution "in a district where the offense was committed."[21] Notably, however, "when [the offense is] not committed within any State, the Trial shall be at such Place or Places as the Congress may by Law have directed."[22]

The Constitution's venue provisions were introduced as a reaction to Great Britain's efforts to transport colonists "beyond Seas to be tried."[23] The earliest concerns emerged in 1769, after the House of Commons recommended trial in England for treason in the Massachusetts Bay colony.[24] The issue reemerged in 1772 after Parliament enacted a statute allowing for trial of certain offenses in England.[25] Although these fears were never truly realized, they prompted the creation of both clauses.[26]

---

[18] *See, e.g.*, United States v. Cabrales, 524 U.S. 1, 6 (1998) ("The Constitution twice safeguards the defendant's venue right . . . .").
[19] U.S. CONST. art. III, § 2, cl. 3.
[20] U.S. CONST. amend. VI.
[21] FED. R. CRIM. P. 18; *see also Cabrales*, 524 U.S. at 6 (quoting FED. R. CRIM. P. 18) ("Rule 18 of the Federal Rules of Criminal Procedure, providing that 'prosecution shall be had in a district in which the offense was committed,' echoes the constitutional commands.").
[22] U.S. CONST. art. III, § 2, cl. 3.
[23] *See* THE DECLARATION OF INDEPENDENCE para. 21 (U.S. 1776).
[24] Paul Mogin, "*Fundamental Since Our Country's Founding": United States v. Auernheimer and the Sixth Amendment Right to Be Tried in the District in Which the Alleged Crime Was Committed*, 6 U. DENV. CRIM. L. REV. 37, 40–41 (2016).
[25] *Id.*
[26] *Id.* at 42.

B. The Basic Venue Inquiry

To determine where venue is proper, courts look to the "locus delicti" of the offense—the place where the crime was committed.[27] When Congress has not indicated such a place in the statute, "the locus delicti must be determined from the nature of the crime alleged and the location of the act or acts constituting it."[28] This is a two-step inquiry. First, a court identifies "the conduct constituting the offense (the nature of the crime)" by identifying each "essential conduct element" of the offense.[29] Second, the court discerns "the location of the commission of the criminal acts."[30] Venue may lie wherever any essential conduct element was carried out.[31] Venue must be proper as to each count; the propriety of venue for one charge does not by itself confer proper venue upon the other charges.[32]

C. Venue in Auernheimer

The charges against Auernheimer were questionable in several respects.[33] As Auernheimer's lawyers argued, to obtain the email addresses, Auernheimer merely accessed an unprotected, public website.[34] His conduct, while perhaps undesirable, was not obviously

---

[27] *See* United States v. Anderson, 328 U.S. 699, 703 (1946) ("Since the statute does not indicate where Congress considered the place of committing the crime to be, the *locus delicti* must be determined from the nature of the crime alleged and the location of the act or acts constituting it." (citation omitted)); *see also Locus Delicti*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining "locus delicti" as the "place where an offense was committed").

[28] *Anderson*, 328 U.S. at 703 (citing United States v. Bowman, 260 U.S. 94, 97–98 (1922)).

[29] United States v. Rodriguez-Moreno, 526 U.S. 275, 279–80 (1999).

[30] *Id.* at 279.

[31] *See id.* at 281–82 ("[W]here a crime consists of distinct parts which have different localities the whole may be tried where any part can be proved to have been done." (quoting United States v. Lombardo, 241 U.S. 73, 77 (1916))).

[32] *See, e.g.*, United States v. Beech-Nut Nutrition Corp. 871 F.2d 1181, 1188 (2d Cir. 1989) (citing United States v. Bozza, 365 F.2d 206, 220–22 (2d Cir.1966) and United States v. Davis, 666 F.2d 195, 198 (5th Cir. Unit B 1982)) ("[W]hen a defendant is charged in more than one count, venue must be proper with respect to each count.").

[33] *See* United States v. Auernheimer, 748 F.3d 525, 532 (3d Cir. 2014) ("[T]his appeal raises a number of complex and novel issues that are of great public importance in our increasingly interconnected age.").

[34] *See* Appellant's Opening Brief at 18–32, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014) (No. 13-1816), 2013 WL 3380740 (making this argument).

unauthorized, as required by the Computer Fraud and Abuse Act.[35] Likewise, as a policy matter, one might question whether compiling a collection of email addresses—characteristically public-facing addresses used by people to communicate with one another—should be deservedly punished by a multiyear prison sentence.[36]

Regardless of one's general feelings toward Auernheimer and his case, cybercrime cases like his call into question the traditional constitutional inquiry and rationale for venue. As the Third Circuit has itself previously observed, "the [Supreme] Court has consistently viewed the venue provisions of the Constitution as important safeguards protecting an accused from unfairness and hardship in defending against prosecution by the federal government."[37]

The Internet is an inherently nationwide, indeed worldwide, technology and practically everyone knows it—certainly someone like Auernheimer with "thirteen years of experience in networking" ought to.[38] Consequently, when a criminal concocts a scheme that harms victims "throughout the country," the criminal "can hardly complain that their very *modus operandi* subject[s] them to prosecution in numerous districts."[39]

In light of this feature of the Internet, under the traditional inquiry, venue for cybercrime prosecutions may often be appropriate in seemingly arbitrary and unanticipated locations anyway, depending on the charges. The cybercriminal's target computer may be located in an

---

[35] *See* 18 U.S.C. § 1030 (2012) (requiring the defendant access a computer "without authorization" or in excess of "authorized access").

[36] There are certainly cases where one may be harmed by exposure on the membership, customer, or user list of a particular group. *See, e.g.*, Seattle Times Co. v. Rhinehart, 467 U.S. 20, 36–37 (1984) (preventing the Seattle Times from publishing a list of donors to a fringe religious group that was produced in pretrial discovery); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 466 (1958) (holding that freedom of association prevented Alabama from subpoenaing the NAACP's membership list); Tom Lamont, *Life After the Ashley Madison Affair*, GUARDIAN (Feb. 27, 2016, 7:05 PM), https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked (describing the aftermath of the leaking of an infidelity-promoting website's user list, including resignations, divorces, and suicides). As a practical matter, however, it is unlikely that such a harm could result from being exposed as an AT&T customer. It is also unclear whether, even in some of the more egregious cases, federal felony charges are just.

[37] United States v. Passodelis, 615 F.2d 975, 977 (3d Cir. 1980).

[38] Auernheimer, *supra* note 10.

[39] *See* United States v. Royer, 549 F.3d 886, 895 (2d Cir. 2008).

unknown, distant, and ultimately surprising location,[40] yet venue may very well be appropriate there.[41] And it seems unlikely that a cybercriminal would carefully investigate the geographic location of that computer to determine whether it would be a suitable venue for his eventual prosecution.[42] It seems even more unlikely that a cybercriminal would consider the suitability of each district through which his digital signals may pass on their way to his target computer—even though he could conceivably be prosecuted for, for example, wire fraud in each district.[43] In the age of cloud computing, the physical location of software and websites is frequently mutable and diffuse.[44] It is unclear how selecting these locations as constitutionally proper venues is fairer for or imposes less hardship on defendants—nevertheless, they are so selected anyway.

In Auernheimer's case, the government sensibly tried to establish venue based on the location of his victims.[45] A cybercrime defendant may actually be more familiar with the location of his victims

---

[40] Ingrid Burrington, *Why Amazon's Data Centers Are Hidden in Spy Country*, ATLANTIC (Jan. 8, 2016), https://www.theatlantic.com/technology/archive/2016/01/amazon-web-services-data-center/423147/ (describing the difficulties of locating Amazon's cloud computing data centers).

[41] *See* United States v. Auernheimer, 748 F.3d 525, 531 (3d Cir. 2014) (suggesting that venue was not appropriate because "the servers accessed were not in" the district).

[42] The foreseeability of "some form of legal proceedings" in the venue is an aspect of whether venue is constitutionally fair. *See* United States v. Miller, 808 F.3d 607, 622 (2d Cir. 2015) ("These observations also suggest that the strong interest in the dispute maintained by [the venue], as the home of [the victim] and the courts vested with relevant authority, and the possibility of some form of legal proceedings there, were foreseeable to [the defendant].").

[43] *See, e.g.*, United States v. Pace, 314 F.3d 344, 349–50 (9th Cir. 2002) ("Therefore, venue is established in those locations where the wire transmission at issue originated, passed through, or was received, or from which it was 'orchestrated.'").

[44] *See Where Your Data is Located*, MICROSOFT: TRUST CTR., https://www.microsoft.com/en-us/trustcenter/privacy/data-management/data-location (then click on the drop-down bar entitled "Data storage and transfers") ("Customer data may be replicated within a selected geographic area for enhanced data durability in case of a major datacenter disaster, and in some cases, will not be replicated outside it.") (last visited Oct. 21, 2018); *Amazon EC2*, AMAZON WEB SERVS., https://aws.amazon.com/ec2/ (last visited Oct. 21, 2018); *see also supra* note 40 and accompanying text.

[45] *See Auernheimer*, 748 F.3d at 536.

than the location of the computers that happen to be running the software through which he victimizes them.[46]

Moreover, with the development of modern transportation and communication technologies, in cases where much of the evidence will be digital and thus readily available anywhere in the world,[47] the hardship imposed on cybercrime defendants has only further shrunk. And, naturally, the venue where the victims are located will have a significant interest in addressing the crime.

II. VENUE BASED ON EFFECTS

In the Auernheimer case, the government argued that venue ought to be proper where the effects of a crime are felt.[48] If venue could so lie, then venue would have been proper in New Jersey, where Auernheimer was tried—thousands of those whose information he exposed were located there.[49] The Third Circuit declined to follow this approach,[50] but the government's efforts were not meritless. The Second Circuit long ago developed a substantial contacts test for determining the permissibility of venue, of which the location of the effects of the crime is one of four factors.[51] The test has had arguably greater influence in the

---

[46] Although not so in *Auernheimer*, the victims of cybercrimes are frequently major corporations. Many, especially in the technology industry, are aware that, for example, Microsoft is located in Redmond, Washington. *See* CITY OF REDMOND, REDMOND TRAVEL DIARY SURVEY (2010), *available at* https://www.redmond.gov/common/pages/UserFile.aspx?fileId=70609 ("Redmond is best known as the home of Microsoft (for which Redmond has become a metonym) . . . .") (last visited Oct. 22, 2018).

[47] The Court has noted that the "hardship of defending prosecutions in places remote from home" arises at least in part from the "accused's difficulties, financial and otherwise, of marshalling his witnesses." United States v. Johnson, 323 U.S. 273, 278 (1944) (citation omitted).

[48] *See Auernheimer*, 748 F.3d at 536.

[49] *See supra* notes 13 and 14 and accompanying text.

[50] *See Auernheimer*, 748 F.3d at 536 ("It is far from clear that this Court has ever 'adopted' this test. We have mentioned it only once. . . . No panel of this Court has ever cited . . . this test since—either before, or especially after, the Supreme Court clarified the venue inquiry in *Cabrales* and *Rodriguez–Moreno*.").

[51] *See* United States v. Reed, 773 F.2d 477, 482 (2d Cir. 1985) ("Third, places that suffer the effects of a crime are entitled to consideration for venue purposes. Such districts have an obvious contact with the litigation in their interest in preventing such effects from occurring.").

Sixth Circuit.[52] And the Department of Justice cautiously suggests this as a potential option for federal prosecutors.[53]

A. The Second Circuit's Substantial Contacts Test

The first case to suggest that effects-based venue may be permissible was *United States v. Reed*.[54] In *Reed*, the Second Circuit determined that the test for venue "is best described as a substantial contacts rule that takes into account a number of factors."[55] The court identified four factors in particular: "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."[56] The court first noted that "[v]irtually all the caselaw" supports venue based on the first factor—the site of the defendant's acts.[57] But the court described the remaining factors as "also important," because they "often give sites other than where the acts occurred equal standing so far as venue is concerned."[58]

According to *Reed*'s substantial contacts test, "places that suffer the effects of a crime are entitled to consideration for venue purposes" because they "have an obvious contact with the litigation in their interest in preventing such effects from occurring."[59] This language appears to suggest that merely causing an effect in a district may be sufficient to support venue there.

The *Reed* court provided two examples of this effects-based approach to setting venue: "Hobbs Act and Taft-Hartley criminal prosecutions may be brought in districts where interstate commerce is affected as well as where the acts took place."[60] The Hobbs Act,

---

[52] *See infra* notes 69–71 and accompanying text (describing the Sixth Circuit's approach that generally favors extending venue where there are substantial contacts).

[53] *See* PROSECUTING COMPUTER CRIMES, *supra* note 15, at 120 ("In some cases, venue might also lie in the district where the effects of the crime are felt. . . . Prosecutors seeking to establish venue by this method are encouraged to contact CCIPS at (202) 514-1026.").

[54] *Reed*, 773 F.2d 477; *see also* Mogin, *supra* note 24, at 47 ("In *United States v. Reed*, the Second Circuit embraced a novel approach to determining where venue is proper under the Constitution.").

[55] *Reed*, 773 F.2d at 481.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.* at 482.

[60] *Id.* (citing United States v. Craig, 573 F.2d 513, 517 (7th Cir. 1978) and United States v. Billups, 692 F.2d 320, 331–33 (4th Cir. 1982)).

however, defines its offense in terms of causing an effect.[61] The Taft-Hartley Act is less clearly defined in such terms.[62] In the relevant case on the Taft-Hartley Act cited by the *Reed* court, the Fourth Circuit found venue proper in the Eastern District of Virginia after an illicit transaction in New York "affected" an area within the district.[63] However, the Fourth Circuit also determined "that one element of a section 186(b) Taft-Hartley offense is that the 'giving' must be proved to be to a representative of an employee of an industry *affecting commerce*"—effectively reading an effects-based element into the statute.[64] Thus, the "same venue rationale"—that where an element is defined in terms of affecting commerce, venue will lie wherever commerce is affected—applied to the Tart-Hartley Act as to the Hobbs Act.[65]

The Second Circuit has "alternately applied and ignored the substantial contacts test" since deciding *Reed*.[66] Moreover, even when applying *Reed*, the Second Circuit has frequently noted that *Reed* "does not represent a formal constitutional test" and is merely "helpful in determining whether a chosen venue is unfair or prejudicial to a defendant."[67] For example, when "all of the substantial contacts appear

---

[61] *See* 18 U.S.C. § 1951 (2012) (punishing, in relevant part, one who "affects commerce . . . by robbery or extortion").

[62] Nowhere in the definition of the relevant criminal offense do the words "affects" or "effects" or any variants thereof appear. *See* 29 U.S.C. § 186(b)(1) (2012) ("It shall be unlawful for any person to request, demand, receive, or accept, or agree to receive or accept, any payment, loan, or delivery of any money or other thing of value prohibited by subsection (a)."). Rather, when read in conjunction with § 186(a), the "any person" of § 186(b)(1) becomes a person "affecting commerce." *See* 29 U.S.C. § 186(a)(1)–(4) (2012) (listing classes of prohibited recipients, all of whom must be "affecting commerce").

[63] *See Billups*, 692 F.2d at 331–32.

[64] *See id.* at 333 ("Although worded differently, a *sine qua non* of a section 186(b) violation is that the forbidden act affect commerce.").

[65] *Id.*

[66] United States v. Coplan, 703 F.3d 46, 80 (2d Cir. 2012) (comparing United States v. Royer, 549 F.3d 886, 893 (2d Cir. 2008) and United States v. Saavedra, 223 F.3d 85, 92–93 (2d Cir. 2000), both approvingly citing *Reed*, with United States v. Tzolov, 642 F.3d 314, 321 (2d Cir. 2011), which questioned the latter three factors of the substantial contacts test).

[67] *Saavedra*, 223 F.3d at 93; *see also* United States v. Kirk Tang Yuk, 885 F.3d 57, 70 (2d Cir. 2018) ("We have acknowledged that this is not a 'formal constitutional test,' but have nevertheless found it to be a valuable safeguard for a defendant whose contacts with the district of prosecution are minimal." (citation omitted)); United States v. Rutigliano, 790 F.3d 389, 399 (2d Cir. 2015) ("[The substantial contacts] inquiry is made only if 'the defendant argues that his prosecution in the contested district will result in a hardship to him,

to be in Illinois," a court may have "serious doubts that venue lies in the Southern District of New York."[68] Thus, the substantial contacts test may function more as a potential limit on venue, rather than an option for extending venue to other districts.

B. Substantial Contacts in Other Circuits

The Sixth Circuit adopted the substantial contacts test in 1986, less than a year after *United States v. Reed* was decided.[69] Where "[o]ther circuits have used the substantial contacts test to ensure that venue is constitutionally adequate," the Sixth Circuit has "applied the substantial contacts test to determine which districts qualify as venues."[70] The Sixth Circuit has found, for example, that "two factors—the elements of the crime and the locus of its effects—can outweigh the location of Defendant's acts and satisfy the substantial contacts test."[71] The Sixth Circuit has also stated that venue is proper when only the locus-of-effects and the most-suitable-for-fact-finding factors are satisfied.[72]

The Fourth Circuit once cited the substantial contacts test with approval,[73] and indeed the Second Circuit relied on a Fourth Circuit opinion in crafting the locus-of-effects factor of the *Reed* test.[74] The Fourth Circuit later backed away from this approach, however, claiming that the reasoning for the approach was irreconcilable with later Supreme Court precedent.[75] Interestingly, in the most recent Supreme Court case

---

prejudice him, or undermine the fairness of his trial.'" (quoting *Coplan*, 703 F.3d at 80)); United States v. Abdallah, 528 F. App'x 79, 83 (2d Cir. 2013) (describing the substantial contacts factors as "useful guideposts," but "not mandatory . . . for a valid venue").

[68] United States v. Alvarez, No. S3 11 CR 169(VB), 2012 WL 4794442, at *3 (S.D.N.Y. Oct. 9, 2012). The defendant in the cited case was ultimately convicted. *See* United States v. Alvarez, 601 F. App'x 16, 18 (2d Cir. 2015), *cert. denied*, 135 S. Ct. 2337 (2015) (affirming Alvarez's convictions).

[69] *See* United States v. Williams, 788 F.2d 1213, 1215 (6th Cir. 1986) ("We now adopt the substantial contacts test as well as the rationale and framework of analysis articulated by the *Reed* court.").

[70] United States v. Castaneda, 315 F. App'x 564, 569 (6th Cir. 2009).

[71] *Id.*

[72] *See* United States v. Brika, 416 F.3d 514, 528 (6th Cir. 2005) ("Venue was proper in the Southern District of Ohio under both 18 U.S.C. § 3237(a) and the substantial contacts test.").

[73] *See* United States v. Cofield, 11 F.3d 413, 417 (4th Cir. 1993).

[74] *See supra* note 60 and accompanying text.

[75] *See* United States v. Bowens, 224 F.3d 302, 312 (4th Cir. 2000) ("Our reasoning in *Cofield*, however, cannot be reconciled with the Supreme Court's later decisions in *Cabrales* and *Rodriguez–Moreno*.").

that the Fourth Circuit cited as irreconcilable, the Court explicitly left open the possibility of an effects-based approach to setting venue.[76]

The Tenth Circuit has explicitly rejected the substantial contacts test.[77] The Seventh and Eleventh Circuits have indicated some approval for the test.[78] The remaining circuits have yet to seriously consider the issue.

C. Auernheimer under the Substantial Contacts Test

In the Auernheimer case, the government argued that the Third Circuit had adopted the substantial contacts test in a previous case.[79] The Third Circuit sharply criticized this claim, but eventually admitted that the court had "perhaps tacitly endorsed [the substantial contacts] test once almost thirty years ago."[80] The court determined, however, that even under the substantial contacts test, venue would have been inappropriate in New Jersey because "the test operates to limit venue, not to expand it."[81] Moreover, the government had only "minimally satisfied one of the four prongs of the test," and the "locus of effects, standing by itself," is not sufficient to confer venue.[82] The Third Circuit further suggested that the possibility left open by the Supreme Court as to effects-based venue[83] referred only to statutes where "an essential conduct element is defined in terms of its effect."[84]

---

[76] *See* United States v. Rodriguez-Moreno, 526 U.S. 275, 279 n.2 (1999) ("The Government argues that venue also 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. Because this case only concerns the *locus delicti*, we express no opinion as to whether the Government's assertion is correct." (citation omitted)).

[77] *See* United States v. Smith, 641 F.3d 1200, 1208 (10th Cir. 2011) ("We decline to adopt this 'substantial contacts' test.").

[78] *See* United States v. Muhammad, 502 F.3d 646, 652 (7th Cir. 2007) (relying on the "admonition" of the substantial contacts test); United States v. Muench, 153 F.3d 1298, 1301 (11th Cir. 1998) ("The place that suffers the effects of a crime deserves consideration for venue purposes.").

[79] *See* United States v. Auernheimer, 748 F.3d 525, 536 (3d Cir. 2014) ("The Government argues that . . . we have 'adopted' a 'substantial contacts test.'" (citation omitted)).

[80] *Id.*

[81] *Id.*

[82] *Id.* at 537.

[83] *See supra* note 76 and accompanying text.

[84] *Auernheimer*, 748 F.3d at 537 (quoting United States v. Bowens, 224 F.3d 302, 311 (3d Cir. 2000)).

The Third Circuit's conclusion about the application of the substantial contacts test is likely correct under Second Circuit precedent. Despite the Second Circuit's initial articulation of the test, the Second Circuit has primarily used it as an additional constraint to ensure the fairness of venue.[85] However, under the Sixth Circuit approach to the substantial contacts test—where fewer factors[86] must be satisfied and the substantial contacts test is used more readily as a means of extending the reach of venue[87]—this conclusion may be incorrect.

III. LEGISLATIVE SOLUTIONS

Several circuits have held that effects-based venue is unconstitutional, outside of a few circumstances directed by statute.[88] Nevertheless, as there are legitimate policy reasons to provide for effects-based venue in cybercrime cases, existing cybercrime statutes should be modified accordingly.

A. Redefining the Offense

When causing an effect is an essential conduct element of a crime, the crime may be prosecuted wherever the effect was caused.[89] Thus, by defining the cybercrimes in terms of the effects they cause on victims, venue would be appropriate in the location or locations of those victims.

Portions of the Computer Fraud and Abuse Act are already defined in terms of effects, but these provisions have unfortunate drawbacks compared to those that are not already defined in such terms.

---

[85] *See supra* note 67 and accompanying text (describing how the Second Circuit has come to apply the substantial contacts test primarily as a limit on venue, rather than a tool for expanding its reach).

[86] Notably, the Sixth Circuit has suggested that only the latter two elements may be necessary. *See supra* note 72 and accompanying text. The third element, the locus of effects, was clearly satisfied, with thousands of victims in New Jersey. The fourth element, the availability of evidence, may also have been arguably satisfied, to the extent that the evidence was electronic. *See supra* Part I.B.

[87] *See supra* notes 70 and 72 and accompanying text (arguing that the Sixth Circuit may use the substantial contacts test to extend venue to districts where other circuits would not).

[88] *See supra* note 84 and accompanying text.

[89] *See Auernheimer*, 748 F.3d at 537 ("Undoubtedly there are some instances where the location in which a crime's effects are felt is relevant to determining whether venue is proper. But those cases are reserved for situations in which 'an essential conduct element is itself defined in terms of its effects.'" (citation omitted) (quoting *Bowens*, 224 F.3d at 311)); *see also* United States v. Davis, 689 F.3d 179, 187 (2d Cir. 2012) (quoting *Bowens* for the same proposition).

For example, as the Third Circuit observed in the Auernheimer case, "[18 U.S.C.] § 1030(a)(5)(B) criminalizes intentionally accessing a computer without authorization and recklessly causing damage."[90] But in addition to being more generally complicated than, for example, the offense Auernheimer was charged with,[91] this provision is much narrower than its plain text might suggest. "Damage" is limited to "impairment to the integrity or availability of data, a program, a system, or information."[92] Moreover, because damage does not include a more generalized sort of harm to human victims, but rather is limited to damage to information systems, the venue inquiry would likely center on the location of the computer, not its owner or those who are actually harmed by the cybercrime.

Despite the limitations of § 1030(a)(5)(B) discussed above, its basic form may be instructive. Computers are unfeeling inanimate objects, despite occasional appearances to the contrary. The victims of cybercrimes are the people who are harmed by them, both those who own the computers and those who own the stolen information residing on the computers. It would be a simple revision to extend "causing damage" to include "causing harm to people."

Nevertheless, because even those offenses that appear to be defined in terms of effects may need to be reevaluated, this approach to law reform may be inefficient and increase the burden of proof for the government. Revising every relevant offense may be needlessly time-consuming. More critically, the government may be forced to prove specific intent to injure people, rather than mere intent to access the computer system.

B. Specific Venue Provisions

Another, perhaps more convenient, option would be to add a statutory provision that specifies the proper location of venue.[93] This would effectively remove all doubt as to "where Congress considered the place of committing the crime to be."[94] For example, one of the main federal obstruction of justice statutes, which proscribes obstructing official proceedings, allows prosecution to "be brought in the district in

---

[90] *Auernheimer*, 748 F.3d at 537; 18 U.S.C. § 1030(a)(5)(B) (2012).
[91] Which only involves unauthorizedly obtaining information from a computer. *See* 18 U.S.C. § 1030(a)(2)(C) (2012).
[92] *Id.* § 1030(e)(8).
[93] *See* CHARLES DOYLE, CONG. RESEARCH SERV., RS22361, VENUE: A BRIEF LOOK AT FEDERAL LAW GOVERNING WHERE A FEDERAL CRIME MAY BE TRIED 3 (2018) (listing crimes with individual venue provisions).
[94] United States v. Anderson, 328 U.S. 699, 703 (1946).

which the official proceeding . . . was intended to be affected," as well as "in the district in which the conduct constituting the alleged offense occurred."[95] An analogous cybercrime venue provision might specify that prosecutions under the Computer Fraud and Abuse Act may be brought in the district in which at least some of the victims of the offense were located.

Specific venue provisions must fall within constitutional limits.[96] Fortunately, there is little doubt that a specific venue provision here would. In the obstruction of justice venue provision, the official proceeding need not be "pending" or even "about to be instituted."[97] To be prosecuted for obstructing an official proceeding, the defendant need not even have knowledge about the potential official proceeding.[98] Thus the mere fact that the particular real, human victims of one's cybercrime may be unknown to the defendant should not pose an obstacle.

CONCLUSION

When a crime is committed in cyberspace, identifying the physical place where it was committed is often challenging, even nonsensical. With traditional crimes, the criminal, the victim, and the scene of the crime are not strewn across the world—not so with cybercrimes. The traditional criminal venue inquiry, centering on the geographic scene of the crime, is thus ill-suited to cybercrimes. The

---

[95] 18 U.S.C. § 1512(i) (2012).

[96] *See* United States v. Salinas, 373 F.3d 161, 164 (1st Cir. 2004) (citing Travis v. United States, 364 U.S. 631, 635 (1961) and Armour Packing Co. v. United States, 209 U.S. 56, 73–75 (1908)) ("If the statute under which the defendant is charged contains a specific venue provision, that provision must be honored (assuming, of course, that it satisfies the constitutional minima)."). However, these constitutional limits on congressional definition of offenses are unclear. *See* United States v. Saavedra, 223 F.3d 85, 92 (2d Cir. 2000) ("The outer limits on how broadly Congress may define a continuing offense and thereby create multiple venues is unclear.").

[97] 18 U.S.C. § 1512(f)(1) (2012).

[98] *See, e.g.*, United States v. Risken, 788 F.2d 1361, 1369 (8th Cir. 1986) ("Proof of a violation of § 1503 requires proof of the defendant's knowledge of a pending judicial proceeding, which is expressly not an element of a violation of § 1512."). However, more recent cases have required a tighter "nexus element" between the proceeding and the obstructive conduct. *See, e.g.*, Arthur Andersen LLP v. United States, 544 U.S. 696, 707–08 (2005) (requiring that a proceeding be "foreseen"). The source of this requirement is unclear. *See* United States v. Aguilar, 515 U.S. 593, 612 (1995) (Stevens, J., concurring in part and dissenting in part) ("The Court does not indicate where its 'nexus' requirement is to be found within the words of the statute. Instead, it justifies its holding [by] . . . importing extratextual requirements . . . .").

home venues of the victims of such crimes only occasionally prove suitable. The judicially-developed substantial contacts test, which allows for the consideration of where the effects of a crime are felt in setting venue, could offer a promising solution, but it has not been widely adopted. Congress, however, could offer an ultimate solution by updating the cybercrime statutes to provide for venue in the place where the actual victims of a cybercrime experience its harm.