EMORY | LAW

Emory Law Journal

Volume 68 | Issue 1

2018

Seeking Warrants for Unknown Locations: The Mismatch Between Digital Pegs and Territorial Holes

Diana Benton

SEEKING WARRANTS FOR UNKNOWN LOCATIONS: THE MISMATCH BETWEEN DIGITAL PEGS AND TERRITORIAL HOLES

ABSTRACT

Increasingly, criminal activity takes place over the Dark Net, a portion of the Internet that allows users to conceal their identities and locations. Law enforcement can observe Dark Net users committing crimes but cannot identify them for further investigation and prosecution without hacking into their computers. Such hacking is a search within the meaning of the Fourth Amendment, which means law enforcement must obtain a warrant beforehand.

However, the need to search the computers of Dark Net users presents law enforcement officers and courts with a problem that does not often arise in the traditional search warrant context. Because a judge does not have the authority to issue a warrant that will be executed outside her jurisdiction, police cannot apply for a warrant without first knowing where the computer to be searched is located. The nature of the Dark Net—a virtual space for criminal activity that is unmoored from the traditional territorial boundaries that define courts' authority—creates a dilemma for courts and law enforcement. How can a judge know whether she has authority to issue a warrant when the location to be searched is undiscoverable without the very warrant itself?

This Comment analyzes the Fourth Amendment implications of such warrants and recommends expanding statutory authority and procedural mechanisms to allow judges to issue warrants when the location to be searched remains unknown. This expansion would further the constitutional preference for warrants without violating constitutional principles governing territorial limitations on courts' jurisdiction.

INTRODUCTION

The Internet offers criminals an unparalleled opportunity to source, market, and sell illicit products and services in a nationwide or even global marketplace.[1] To evade law enforcement, criminals are increasingly shifting their online activity to the Dark Net,[2] which ordinary Internet users cannot access without specialized software or authorization from the network's host.[3] The Dark Net hosts vast black markets for child pornography,[4] illegal narcotics, toxic chemicals, illicit weapons, hacking software, and stolen credit card data.[5] Offenders coordinate heinous crimes over the Dark Net with terrible consequences for victims and society,[6] including hosting forums where pedophiles share tips for abusing children and exploitative videos,[7] selling powerful opioids that cause overdose deaths,[8] and even executing murder-for-hire schemes.[9]

---

[1] *See, e.g.*, Press Release, Dep't of Justice, U.S. Att'y's Office, S. Dist. of N. Y., Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015) (noting that the Silk Road, a large Dark Net marketplace, featured drug dealers located in over ten different countries providing illegal narcotics to buyers across the world).

[2] *See* Frank Miniter, *The Growing Force that Will Soon Reshape the Entire Internet*, FORBES (Dec. 30, 2017, 1:31 PM), https://www.forbes.com/sites/frankminiter/2017/12/30/the-growing-force-that-will-soon-reshape-the-entire-internet/#304254e31c88. The terms "Dark Net" and "Dark Web" are used interchangeably. *See, e.g.*, Press Release, Dep't of Justice, Office of Pub. Affairs, AlphaBay, the Largest Online 'Dark Market,' Shut Down (July 20, 2017) (using terms "dark net" and "dark web" interchangeably). One of the most prominent networks comprising the Dark Net is The Onion Router (TOR). *See* United States v. Jean, 207 F. Supp. 3d 920, 924 (W.D. Ark. 2016) (describing the origins of the TOR network).

[3] *See Jean*, 207 F. Supp. 3d at 924–25 (describing the dark web structure and access); United States v. Scanlon, No. 2:16-cr-73, 2017 WL 3974031, at *3–4 (D. Vt. Apr. 26, 2017) (describing how a Dark Net site required the host to authorize a user's account before granting access).

[4] *See, e.g.*, Leslie R. Caldwell, *Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation*, DEP'T OF JUST. BLOG ARCHIVES (Nov. 21, 2016), https://www.justice.gov/archives/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation (discussing Dark Net child pornography forums).

[5] *See, e.g.*, Press Release, Dep't of Justice, Office of Pub. Affairs, More than 400 .Onion Addresses, Including Dozens of 'Dark Market' Sites, Targeted as Part of Global Enforcement Action on TOR Network (Nov. 7, 2014), (describing Dark Net websites as the "Wild West of the Internet, where criminals can anonymously buy and sell all things illegal").

[6] *See* United States v. Levin, 874 F.3d 316, 319 (1st Cir. 2017) ("Child-pornography websites are a source of significant social harm.").

[7] Caldwell, *supra* note 4 ("Tens of thousands of pedophiles congregate on these sites to buy, sell and trade images and videos of abuse, and even to pay abusers to commit new abuses and to record and share them. Many of these same websites feature discussion groups where pedophiles can provide one another advice on how to groom young children for abuse, how to evade detection by caregivers and law enforcement and other ways to facilitate these vile crimes.").

[8] *See, e.g.*, U.S. Att'y's Office, S. Dist. of N. Y., *supra* note 1 (linking narcotics distributed on the Silk Road Dark Net marketplace to at least six overdose deaths).

[9] *See* United States v. Ulbricht, 79 F. Supp. 3d 466, 485–86 (S.D.N.Y. 2015) (discussing evidence that the operator of the Silk Road, a major Dark Net marketplace, was implicated in multiple murder-for-hire

Beyond the challenge of discovering and accessing these secret marketplaces, law enforcement must identify offenders to prosecute them.[10] However, Dark Net users are typically anonymous,[11] identified only by their self-designated screen names.[12] As one court explained, "[The Onion Router (TOR)] browser enables users to cloak their identities in darkness—like guests to a dimly lit masquerade ball using masks to conceal their faces."[13] Absent self-disclosure,[14] law enforcement must hack into users' computers to determine their identities.[15]

Because hacking into a computer is a search, the Fourth Amendment presumptively requires law enforcement to first obtain a warrant.[16] In the absence of a warrant, nothing that the search uncovers can be used as evidence at trial.[17] Yet law enforcement officers cannot apply for a warrant without first

---

schemes); Andy Greenberg, *Read the Transcript of the Silk Road's Boss Ordering 5 Assassinations*, WIRED (Feb. 2, 2015, 9:31 PM), https://www.wired.com/2015/02/read-transcript-silk-roads-boss-ordering-5-assassinations/.

[10] *See* United States v. Barnes, No. 3:15-CR-112-J-39PDB, 2017 U.S. Dist. LEXIS 136157, at *18–20 (M.D. Fla. May 8, 2017) (discussing how the FBI could not prosecute anonymous online distributors of child pornography without first determining their identities). *See generally* United States v. Scanlon, No. 2:16-cr-73, 2017 WL 3974031, at *2–3 (D. Vt. Apr. 26, 2017) (describing the steps required to access a child pornography marketplace on the Dark Net).

[11] United States v. Jean, 207 F. Supp. 3d 920, 924–25 (W.D. Ark. 2016).

[12] *See Scanlon*, 2017 WL 3974031, at *4 (describing how the FBI could observe users' actions on a Dark Net child pornography website but could not obtain their true identities from the scant information available on the Dark Net).

[13] *Jean*, 207 F. Supp. 3d at 924–25.

[14] In addition to criminal users' self-interest in anonymity, criminal forums may encourage anonymity. *See Scanlon*, 2017 WL 3974031, at *3 (noting that a Dark Net child pornography hub cautioned users not to post information that could be used to identify them).

[15] *See* United States v. Taylor, 250 F. Supp. 3d 1215, 1220–22, 1228 (N.D. Ala. 2017) (determining that the government could only identify a Dark Net user by hacking into the user's computer); *Jean*, 207 F. Supp. 3d at 928–29 (describing how the FBI hacked into a Dark Net user's computer to identify its IP address, which allowed the FBI to identify the user through an administrative subpoena to the internet service provider). The FBI refers to such hacking as a "Network Investigative Technique (NIT)." *Id.* at 926.

[16] *See, e.g.*, United States v. Horton, 863 F.3d 1041, 1047 (8th Cir. 2017) (holding that the FBI hacking into the defendant's personal computer was a search because he had a reasonable expectation of privacy in its contents, and therefore the government must obtain a search warrant); *Taylor*, 250 F. Supp. 3d at 1228 ("The NIT [hacking into a computer] is not akin to a police officer peering through broken blinds into a house; it is more like a police officer acquiring a key to the house and entering through the back door to secretly observe activity in the living room.").

[17] *See* Mapp v. Ohio, 367 U.S. 643, 648, 660 (1961) (holding that evidence seized in violation of the Fourth Amendment must be excluded from use in federal and state court). Even derivative evidence may be excluded when discovered as a result of earlier evidence found in an illegal search. Murray v. United States, 487 U.S. 533, 536–37 (1988). Although exceptions to the warrant requirement exist, they do not apply in this context. *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 351 (2009) (refining the conditions which permit a warrantless search of a vehicle incident to a recent occupant's arrest); United States v. Matlock, 415 U.S. 164, 171 (1974) (holding that no warrant is needed when a person with common authority over the premises to be searched consents); United States v. Robinson, 414 U.S. 218, 224 (1973) ("It is well settled that a search incident to a lawful arrest

knowing where the computer to be searched is located, because the location of the search will determine which court has authority to issue the warrant.[18] Courts face geographic limitations on their jurisdiction,[19] absent certain exceptions.[20] Therefore, if a court issues a warrant to search a computer at an unknown location, then the warrant may be void *ab initio* if the search reveals that the computer is physically located beyond the court's jurisdiction.[21] Because a void warrant cannot provide a legal basis for a search, the prosecution cannot rely on anything found in the search in a criminal trial.[22]

This Catch-22 prevents the government from investigating and prosecuting dangerous criminals; the Internet creates a virtual space for criminal activity unmoored from the traditional territorial boundaries that define courts' authority.[23] Hence, this Comment argues that when no other district is known to have jurisdiction, federal judges should have the authority to issue warrants for the search or seizure of property under the Fourth Amendment if the alleged crime could be prosecuted in their district. This approach bridges the disconnect between courts' jurisdiction, based on physical spaces, and crimes that take place in cyberspace.

This discussion is timely because a 2016 amendment to Rule 41 of the Federal Rules of Criminal Procedure provides a mechanism for federal courts to issue remote access warrants, which authorize law enforcement to hack into a

---

is a traditional exception to the warrant requirement of the Fourth Amendment . . . . [A] search may be made of the person of the arrestee . . . [and] of the area within the control of the arrestee.").

[18] *See* Weinberg v. United States, 126 F.2d 1004, 1006–07 (2d Cir. 1942) ("With very few exceptions, United States district judges possess no extraterritorial jurisdiction.")

[19] *See* United States v. Krueger, 809 F.3d 1109, 1124 (10th Cir. 2015) (noting that "a warrant issued in defiance of positive law's restrictions on the territorial reach of the issuing authority" will be invalid).

[20] For procedural exceptions, see FED. R. CRIM. P. 41(b). However, a statute must provide the court authority to use a procedural exception. *See Weinberg*, 126 F.2d at 1006 (holding that a warrant had no effect outside the district of the issuing court when no statute provided the court with such jurisdiction).

[21] *See Horton*, 863 F.3d at 1049 (holding that a warrant was void *ab initio* because it authorized searches outside the issuing court's jurisdiction, even though some searches pursuant to the warrant took place within the court's jurisdiction); United States v. Levin, 874 F.3d 316, 318 n.1, 320–21 (1st Cir. 2017) (affirming that the same warrant examined in *Horton* was void *ab initio* because it authorized searches outside the court's jurisdiction). *But see* United States v. Workman, 863 F.3d 1313, 1318–19 n.1 (10th Cir. 2017) (noting in dicta that while the same warrant examined in *Horton* was invalid when executed outside the issuing court's jurisdiction, the warrant was not void *ab initio* because the warrant was valid when executed within the issuing court's district).

[22] However, the court may allow the fruits of the illegal search to be admitted into evidence if the police acted in good faith reliance on an apparently valid warrant. *See Horton*, 863 F.3d at 1051–52 (holding that the good faith exception applied because law enforcement did not mislead the judge and reasonably relied on the warrant, although it was void *ab initio* due to territorial limitations on the judge's jurisdiction).

[23] *See* United States v. Jean, 207 F. Supp. 3d 920, 941 (W.D. Ark. 2016) ("Internet crime and surveillance defy traditional notions of place.").

computer to search for information.[24] The amendment was added because the proliferation of criminal activity on the Dark Net made these investigative techniques increasingly necessary.[25] Prior to the amendment, for example, a court had rejected the FBI's application for a warrant to hack into a cybercriminal's computer to determine its physical location because Rule 41, at the time, did not allow remote access warrants.[26] Although amended Rule 41 provides a procedural mechanism for such warrants, it does not address the question of constitutionality when the court issuing the warrant does not know *ex ante* whether the search will take place outside its district.[27] Anonymous Dark Net users may be located anywhere in the world.[28] While scholars have proposed practical frameworks to regulate government hacking to reduce conflicts with international law,[29] the constitutionality of these searches has not yet received detailed scrutiny in the context of the amendment to Rule 41 allowing remote access warrants.[30] The procedural framework for issuing these warrants is

---

[24] FED. R. CRIM. P. 41 advisory committee's note to 2016 amendments; FED. R. CRIM. P. 41(b)(6).

[25] *See* Letter from Mythili Raman, Acting Att'y Gen., to Reena Raggi, Honorable, Chair, Advisory Comm. on the Criminal Rules (Sept. 18, 2013), *in* ADVISORY COMM. ON CRIMINAL RULES, CRIMINAL RULES COMMITTEE MEETING 171–72 (2014) (describing the need for remote access warrants due to criminals' increasing use of "anonymizing technologies" online); Devin M. Adams, *The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, "Particularly" Speaking*, 51 U. RICH. L. REV. 727, 744 (describing the proposal and approval of the remote access warrant amendment).

[26] *In re* Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753, 761 (S.D. Tex. 2013) ("This is not to say that such a potent investigative technique [as remote access hacking] could never be authorized under Rule 41. And there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology.").

[27] *See* FED. R. CRIM. P. 41 advisory committee's note to 2016 amendments ("The amendment does not address constitutional questions . . . leaving the application of . . . constitutional standards to ongoing case law development.").

[28] *See* United States v. Workman, 863 F.3d 1313, 1315 (10th Cir. 2017) (observing the "paradox" the FBI faced when attempting to use a warrant to identify users of a Dark Net child pornography hub, who were spread throughout the United States); United States v. Scanlon, No. 2:16-cr-73, 2017 WL 3974031, at *5 (D. Vt. Apr. 26, 2017) (noting that a warrant to search for identifying information of anonymous computer users identified over 1,300 IP addresses of computers, including domestic and foreign users). During the last two months of 2017, 85% of computers accessing the Dark Net were located outside the United States. The Tor Project, *Top-10 Countries by Relay Users*, TOR METRICS, https://metrics.torproject.org/userstats-relay-table.html?start=2017-11-01&end=2017-12-31 (last visited Aug. 20, 2018).

[29] *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1124–28 (2017) (proposing an executive agency implementation scheme regulating government hacking).

[30] Scholars have analyzed territoriality of data in the context of whether the Fourth Amendment protects digital communications when the location of the data is unknown, and its owner remains anonymous. *Compare* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 383 (2015) (proposing applying a presumption that the Fourth Amendment protects all subjects of a search, which the government must rebut by establishing that none of the parties is a U.S. person), *with* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 303 (2015) (proposing that the government should be permitted to conduct warrantless monitoring of subjects whose Fourth Amendment rights are unknown under the good faith belief that the subject lacks sufficient connection with the United States to gain Fourth Amendment protection). The

already in place, but the issue of courts' constitutional authority to issue remote access warrants urgently needs to be resolved.

To provide the first steps toward defining the courts' constitutional authority to issue warrants where the district of the physical evidence is unknown, this Comment proceeds in three Parts. Part I explains how warrants are applied to digital data and the conundrum of investigating anonymous Internet users whose physical location is unknown. Part II proposes the solution of providing authority to federal judges to issue warrants based on the location where the crime under investigation may be prosecuted, and calls for an amendment to Rule 41 and federal statutes to accommodate the proposed changes. It also explains how the proposed exception comports with territorial constraints on courts' authority to issue warrants and constitutional limitations on extraterritorial application of their authority. Part III discusses immediate implications and the potential for expanding Fourth Amendment protections to allow the Warrant Clause to apply overseas.

I. TERRITORIALLY CONSTRAINED WARRANTS IN THE AGE OF THE INTERNET

Analyzing the Fourth Amendment's implications for anonymous Internet users of unknown locations requires a brief overview of how warrants apply to digital data in general. Section A below discusses the Fourth Amendment's application to digital data and section B describes the unique dilemma presented by Internet users who have masked their physical locations.

A. Digital Data and Warrants

The Fourth Amendment applies to searches for digital data in two important contexts: (1) warrants allowing law enforcement to search a user's computer;[31] and (2) warrants served upon third-party information service providers compelling them to provide stored user data.[32] This Comment addresses the first context.

---

data's location and owner's identity determine whether the subject has gained Fourth Amendment protection and whether police must obtain a search warrant. See United States v. Verdugo-Urquidez, 494 U.S. 259, 265, 274–75 (1990) (holding that the Fourth Amendment only protects persons who are part of the U.S. community or who have developed sufficient connection with the United States), discussed *infra* Section III.B. However, this Comment analyzes whether a warrant *can* be issued.

[31] *See, e.g.*, *Workman*, 863 F.3d at 1315 (discussing a warrant to search a computer by remotely hacking into it).

[32] *See, e.g.*, Microsoft Corp. v. United States, 829 F.3d 197, 200 (2d Cir. 2016) [hereinafter Microsoft II] (discussing a warrant compelling Microsoft to provide stored user data to law enforcement), *vacated as moot*, 138 S. Ct. 1186 (2018).

The Fourth Amendment protects against warrantless searches by government actors.[33] A search is a physical intrusion into constitutionally protected areas, including a person's effects,[34] or an invasion into an area where a person has a reasonable expectation of privacy.[35] Federal appellate courts agree that law enforcement searching a suspect's private computer by remotely hacking into it violates the suspect's reasonable expectation of privacy, requiring a warrant.[36] However, the warrant must be valid at the location where the search takes place.[37]

A search by remote hacking takes place where the suspect's computer is physically located, not at the government hacker's location.[38] The hacker sends a computer code into the target computer, where the code performs the search and sends the desired information back to the hacker.[39] Therefore, the relevant Fourth Amendment intrusion occurs at the location of the hacked computer.[40]

In contrast, a warrant compelling a third-party ISP to disclose customer data to law enforcement might be executed for purposes of the Fourth Amendment either where the ISP stores the data or where the ISP discloses the data to police

---

[33] Warrantless searches are presumptively unreasonable under the Fourth Amendment unless an exception applies. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). However, the warrant requirement only applies where warrants can be issued, such as within the United States. *See Verdugo-Urquidez*, 494 U.S. at 278 (Kennedy, J., concurring) (noting that a warrantless search overseas did not violate the Fourth Amendment because no U.S. judge had authority to issue a warrant for that location). For further discussion of this issue, see *infra* Section III.B.

[34] United States v. Jones, 565 U.S. 400, 404–05 (2012) (holding that the government's physical intrusion to place a tracking device on a vehicle was a search).

[35] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (characterizing the majority opinion as holding that a search occurs when the government intrudes into a space where a person has a reasonable expectation of privacy that society is prepared to recognize, and he has subjectively manifested an actual expectation of privacy in that place).

[36] *See, e.g.*, United States v. Horton, 863 F.3d 1041, 1046–47 (8th Cir. 2017) (holding that hacking into defendant's personal computer remotely required a warrant because the intrusion violated his reasonable expectation of privacy); *see also* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (holding that searching a cell phone's digital content required a warrant because such content did not fall into the exception for a search incident to arrest).

[37] *See, e.g.*, *Horton*, 863 F.3d at 1047–49 (holding that a warrant seeking to remotely search a computer to determine its physical location was invalid because the issuing judge had no authority over the computer's location, which is where the search took place).

[38] *See id.* at 1047–48 (holding that a search by remote access using hacking software took place where the hacked computer was physically located in Iowa, not in the FBI office in Virginia where law enforcement accessed the Internet to upload the hacking software).

[39] *See id.* at 1047 (describing the FBI hacking into a suspect's computer remotely).

[40] *See, e.g.*, *id.* at 1047–49 (holding that a judge issuing a warrant to remotely search a computer must have jurisdiction where the computer was physically located because that was where the search took place).

in the United States.[41] The Court declined to resolve this question in *United States v. Microsoft Corporation* (*Microsoft III*) because the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which passed after the case was litigated in lower courts, required ISPs to comply with the warrant regardless of the location where they stored the data, rendering the original dispute over the statute's scope moot.[42]

However, neither *Microsoft III* nor the CLOUD Act address warrants for remote searches of personal computers at unknown locations. Instead, they pertain to another type of warrant, one that compels an ISP to disclose user information stored on its servers.[43] This warrant's authority to demand action from the ISP arises from the courts' *in personam* jurisdiction over the ISP, which enables the court to enforce its orders to the ISP.[44] In contrast, a warrant allowing police to search a computer at an unknown location requires the court to have *in rem* jurisdiction over the computer itself.[45]

This distinction is important because when the computer's location is unknown, the courts' authority to issue a warrant to search it remains unresolved. A court issuing a remote access warrant cannot ascertain its jurisdiction over the

---

[41] *Compare* Microsoft II, 829 F.3d 197, 220 (2d Cir. 2016) (holding that a warrant compelling an ISP to disclose customer data was executed where the data was stored on a server in Ireland), *vacated as moot*, 138 S. Ct. 1186 (2018), *with In re* Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757 (BAH), 2017 WL 3445634, at *5, *13–14 (D.D.C. July 31, 2017) (observing that lower courts had nearly universally rejected the holding of *Microsoft I* and holding that such warrants were executed where the domestic ISP was located).

[42] 138 S. Ct. 1186, 1187–88 (2018) [hereinafter Microsoft III]. While the CLOUD Act provides statutory authority for such warrants, the constitutional authority remains undetermined because the recently passed Act has not yet faced challenge in court. *See* Pub. L. No. 115-141, 132 Stat. 348 (2018) (amending the Stored Communications Act, 18 U.S.C. § 2703 (2012)). This Comment's proposal will resolve potential challenges over courts' authority to issue to such warrants when they are to be executed for data stored overseas by providing courts with the authority to issue warrants regardless of the location of execution, as discussed in Part III.

[43] *See Microsoft III*, 138 S. Ct. at 1187–88.

[44] *See Microsoft II*, 829 F.3d at 200 (noting that Microsoft, a U.S. ISP, complied with the warrant to the extent that it compelled disclosure of data stored in the United States); *In re* Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156, at *2–4 (E.D. Wis. June 30, 2017) [hereinafter *In re* Two Email Accounts] (comparing warrants compelling an ISP to disclose data in its possession to ordinary search warrants that authorize police to search a particular location); *see also In re* Search of Content Stored at Premises Controlled by Google Inc., No. 16-mc-80263-RS, 2017 WL 3478809, at *5 (N.D. Cal. Aug. 14, 2017) (holding that a court could compel an ISP to comply with a Stored Communications Act (SCA) warrant because the court had "enforcement jurisdiction" over the ISP). The CLOUD Act has resolved questions over the scope of the courts' authority to issue such orders. *See* Pub. L. No. 115-141, 132 Stat. 348 (2018).

[45] *See* In re *Two Email Accounts*, at *2–4.

computer or its user until after the search occurs.[46] These problems posed by searches of computers at unknown locations will be discussed in detail below.

B. Anonymous Internet Users of Unknown Location

Applying the Fourth Amendment to anonymous computer users at unknown locales creates a dilemma for judges who must first ascertain their jurisdiction over the unknown location where the warrant will be executed.[47] This Comment proposes an exception that would extend jurisdiction when the location for the warrant's execution is unknown or no other U.S. district has jurisdiction over the target.

The 2016 amendments to Rule 41 allow law enforcement to request a warrant to hack into a target computer remotely and to search or copy digital information located within or outside the magistrate judge's district.[48] The purpose of remote access warrants is to facilitate law enforcement investigations of criminal activity by anonymous Internet users, an increasingly prevalent problem.[49] To obtain the computer's identifying information, including its physical location and potentially the user's identity,[50] law enforcement must hack into the target computer, which constitutes a search under the Fourth Amendment.[51] Without this identifying information, law enforcement cannot prosecute persons who conduct criminal transactions over the Dark Net because they cannot be identified.[52]

---

[46] *See, e.g.*, *Horton*, 863 F.3d at 1047–48; United States v. Scanlon, No. 2:16-cr-73, 2017 WL 3974031, at *12 (D. Vt. Apr. 26, 2017) (noting that the judge issuing a warrant for police to remotely hack into computers anonymously accessing a Dark Net child pornography hub could not determine the computers' physical locations *ex ante*).

[47] *See, e.g.*, *Horton*, 863 F.3d at 1047–48 (noting the paradox created when the judge could not know whether he had authority to issue a warrant until after the warrant was executed); *Scanlon*, 2017 WL 3974031, at *12.

[48] FED. R. CRIM. P. 41(b)(6) ("[A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been concealed through technological means.").

[49] *Supra* note 25.

[50] This information usually consists of the IP address. *See, e.g.*, United States v. McLamb, 880 F.3d 685, 688–89 (4th Cir. 2018) (describing how FBI hacked into a computer to obtain identifying information).

[51] *See Horton*, 863 F.3d at 1047 ("Even if a defendant has no reasonable expectation of privacy in his IP address, he has a reasonable expectation of privacy in the contents of his personal computer."); *McLamb*, 880 F.3d at 690–91 (holding that FBI hacking into computers to search for IP addresses "actually searched computers"). *But see* United States v. Jean, 207 F. Supp. 3d 920, 933 (W.D. Ark. 2016) (questioning whether government entry onto a private computer to obtain its IP address was a search under the Fourth Amendment).

[52] *See* United States v. Barnes, No. 3:15-CR-112-J-39PDB, 2017 U.S. Dist. LEXIS 136157, at *18–20 (M.D. Fla. May 8, 2017) (discussing how the FBI could not prosecute anonymous online distributors of child

To obtain a remote access warrant, law enforcement must show that the district where the data is located has been "concealed through technological means."[53] However, there is no guarantee that the data is located within the district issuing the warrant, or even within the United States.[54] When proposing the 2016 amendment allowing remote access warrants, the Department of Justice argued that the amendment would not authorize the search of computers on foreign soil.[55] However, the amendment could be construed to enable remote searches outside U.S. boundaries.[56]

Under current territorial limitations on judges' authority, a warrant for an anonymous computer cannot be valid when the issuing judge does not know whether it would be executed within or outside the United States.[57] Law enforcement would not know whether the search took place outside the United States until the search had already been executed.[58] The computer's masked location creates a chicken-and-egg conundrum: The judge cannot determine whether the warrant will be a valid exercise of her jurisdiction until the warrant has already been executed.[59] For example, investigators executing a warrant authorizing remote hacking of computers accessing child pornography on the Dark Net inadvertently searched computers in Denmark, Greece, and Chile, in

pornography without first determining their identities). *See generally Scanlon*, 2017 WL 3974031, at *2–3 (describing the steps required to access a child pornography marketplace on the Dark Net).

[53] FED. R. CRIM. P. 41(b)(6).

[54] *See* United States v. Workman, 863 F.3d 1313, 1315 (10th Cir. 2017) (observing the "paradox" the FBI faced when attempting to use a warrant to identify users of a Dark Net child pornography hub, who were spread throughout the United States); *Scanlon*, 2017 WL 3974031, at *5 (noting that a warrant to search for identifying information of anonymous computer users identified over 1,300 IP addresses of computers, including domestic and foreign users); The Tor Project, *supra* note 28.

[55] Letter from Mythili Raman, Acting Att'y Gen., to Reena Raggi, Honorable, Chair, Advisory Comm. on the Criminal Rules (Sept. 18, 2013), *in* ADVISORY COMM. ON CRIMINAL RULES, CRIMINAL RULES COMMITTEE MEETING 171–74 (2014) The Department of Justice argued that the presumption of extraterritoriality would apply, although the rule amendment was the result of administrative rule-making instead of legislative action. *Id.*

[56] *See* Center for Democracy & Technology, Written Statement Before the Judicial Conference Advisory Comm. on Criminal Rules, at 3 (Oct. 24, 2014), https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0009&attachmentNumber=1&disposition=attachment&contentType=pdf (stating that amending Rule 41 to allow remote access warrants "would authorize extraterritorial searches that circumvent the [Mutual Legal Assistance Treaty (MLAT)] process and may violate international law").

[57] *See* United States v. Horton, 863 F.3d 1041, 1049 (8th Cir. 2017) (holding that a warrant was void *ab initio* because it authorized searches outside the issuing court's jurisdiction, even though some searches pursuant to the warrant took place within the court's jurisdiction); United States v. Levin, 874 F.3d 316, 318, 320–21 (1st Cir. 2017) (affirming that the same warrant examined in *Horton* was void *ab initio* because it authorized searches outside the court's jurisdiction). *But see Workman*, 863 F.3d at 1318–19 n.1 (noting in dicta that while the same warrant examined in *Horton* was invalid when executed outside the issuing court's jurisdiction, the warrant was not void *ab initio* because the warrant was valid when executed within the issuing court's district).

[58] *See, e.g.*, *Scanlon*, 2017 WL 3974031, at *12.

[59] *See, e.g.*, *Horton*, 863 F.3d at 1047–48; *Scanlon*, 2017 WL 3974031, at *12.

addition to U.S. computers located outside the district where the warrant was issued.[60]

Even if the warrant is ultimately executed within the United States, the possibility of its execution outside the United States imperils its validity. Some courts have declared a warrant "wholly void or void *ab initio*" because it authorized searches outside the judge's jurisdiction, even though some searches pursuant to the warrant took place within the judge's district.[61] Therefore, a warrant to search a Dark Net user's computer may be declared void even when the warrant is executed within the United States, merely because the warrant could have been executed outside the United States where U.S. courts currently lack authority to issue warrants. This problem requires a solution enabling courts to issue warrants to investigate criminal activity over the Dark Net without risking invalidation for lack of jurisdiction.

II. PROPOSED SOLUTION

As the conundrum described above shows, the current territorial principle governing judges' authority to issue warrants does not function well in the context of cybercriminals who have masked their location through the Dark Net. The age of the Internet demands a new rule better suited to the challenges that law enforcement and society face. Yet there must be some limiting principle on judges' authority to issue warrants. Rather than the outmoded focus on geographical territory, a judge's authority should hinge on whether the crime could be prosecuted in that court.

When no other district is known to have jurisdiction, a federal judge should have the authority to issue warrants for the search or seizure of property based on whether the alleged crime could be prosecuted in his district. To be valid, a warrant requires (1) statutory authority,[62] (2) a procedural mechanism for

---

[60] EUROPEAN PARLIAMENT, LEGAL FRAMEWORKS FOR HACKING BY LAW ENFORCEMENT: IDENTIFICATION, EVALUATION, AND COMPARISON OF PRACTICES 29 (2017), http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2017)583137. The warrant did not authorize searches outside the issuing district because it was issued before the 2016 amendment to Rule 41 providing for remote access warrants. *Horton*, 863 F.3d at 1047 & n.2, 1048.

[61] *See Horton*, 863 F.3d at 1049; *Levin*, 874 F.3d at 318 n.1, 320–21. *But see Workman*, 863 F.3d at 1318–19 n.1 (noting in dicta that while the same warrant examined in *Horton* was invalid when executed outside the issuing court's jurisdiction, the warrant was not void *ab initio* because the warrant was valid when executed within the issuing court's district).

[62] *See* Weinberg v. United States, 126 F.2d 1004, 1006 (2d Cir. 1942) (holding that a warrant had no effect outside the district of the issuing court when no statute provided the court with such jurisdiction).

issuance,[63] and (3) constitutional compliance.[64] Therefore, statutes authorizing warrants and Rule 41 must be amended to reflect this exception. This Comment proposes that Congress amend Rule 41 as follows to add this necessary exception:[65]

> A magistrate judge with authority in the district may issue a warrant to search for and seize property located outside the district if:
>
> A) no other district is known to have jurisdiction;[66] and
>
> B) the district is reasonably likely to have jurisdiction over the crime underlying the probable cause in the warrant.[67]

This exception to the territorial limitations on warrants would comport with existing restrictions on courts' authority, as discussed below in section II.A. Further, this exception would not violate constitutional constraints, as examined in section II.B. But it would apply to searches for physical objects as well as digital data, for the reasons discussed in section II.C.

A. Territorial Limitations on Warrants and Courts

The proposed exception does not impede the constitutional purposes behind territorial constraints on warrants, as analyzed below in section II.A.1. Further, as discussed in section II.A.2., the Constitution does not prohibit courts from issuing warrants outside their geographic jurisdictions. Finally, the practical reasons for the proposed exception strongly resemble the justifications for existing exceptions allowing federal courts to issue warrants outside their districts, as explained in section II.A.3.

---

[63] *See, e.g.*, *Levin*, 874 F.3d at 321 (1st Cir. 2017) (discussing a warrant that was void due to lack of procedural authorization under Rule 41 and lack of statutory authority under the Federal Magistrates Act, 28 U.S.C. § 636 (2012)).

[64] *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 239 (1983) (determining the probable cause standard that the Fourth Amendment requires for warrants).

[65] The proposed text is formatted as an amendment to Rule 41(b). *See* FED. R. CRIM. P. 41(b).

[66] Warrant applicants must demonstrate a good faith effort to determine whether another federal court may have jurisdiction. For an anonymous Internet user, law enforcement could readily demonstrate compliance due to the difficulty of obtaining information on such users.

[67] The standard of "reasonably likely" would be measured based on information available to law enforcement at the time of the warrant application.

1. Constitutional Purposes for Territorial Constraints

Warrants face geographic limitations based on the authority of the issuing court.[68] A warrant is only valid if the issuing court had authority to issue it.[69] A warrant has no effect in territory where the court has no authority.[70] Under the Federal Magistrates Act, magistrate judges have jurisdiction within their federal district and "elsewhere as authorized by law."[71] Therefore, expansion of magistrate judges' authority requires amending the statutes conferring authority and the Federal Rules of Criminal Procedure to provide a mechanism for warrant issuance, as proposed above. An amendment to the Federal Rules of Criminal Procedure is valid if the extension of authority does not violate constitutional principles.[72] To determine the permissible scope of an extension of magistrate judges' authority to issue warrants, one must consider what constitutional principles are served by the territorial restrictions and what might violate those principles. This section will examine these constitutional principles in the context of both search warrants and arrest warrants because of the limited use of search warrants in early American jurisprudence.[73]

The district-based limitations on federal courts' jurisdiction serve federalism principles by dividing the federal judiciary geographically and by preventing centralized concentration of power, a major concern of some of the Founders.[74] Geographic alignment of districts with states also furthers states' rights by

---

[68] *See* FED. R. CRIM. P. 41(b); United States v. Krueger, 809 F.3d 1109, 1124 (10th Cir. 2015) (noting that "a warrant issued in defiance of positive law's restrictions on the territorial reach of the issuing authority" will not be valid).

[69] *Krueger*, 809 F.3d at 1124 (citing United States v. Lefkowitz, 285 U.S. 452, 464 (1932)).

[70] *See* Weinberg v. United States, 126 F.2d 1004, 1006 (2d Cir. 1942) (holding that a warrant had no effect outside the district of the issuing court when no statute provided the court with such jurisdiction).

[71] 28 U.S.C. § 636(a) (2012).

[72] *See, e.g.*, FED. R. CRIM. P. 41 advisory committee's note to 2016 amendments (commenting on search warrants allowing law enforcement to remotely access target computers in another district). For statutes that provide authority coextensive with the Federal Rules of Criminal Procedure, amending the Federal Rules of Criminal Procedure would modify the statute as well. *Cf.* Microsoft II, 829 F.3d 197, 208 (2d Cir. 2016) (noting that the SCA provides statutory authority coextensive with Rule 41), *vacated as moot*, 138 S. Ct. 1186, 1187–88 (2018).

[73] *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 628 (1999) (discussing search warrants' original use to recover stolen property instead of obtain evidence for criminal prosecution).

[74] *See Krueger*, 809 F.3d at 1125 (Gorsuch, J., concurring) ("[O]ur whole legal system is predicated on the notion that good borders make for good government, that dividing government into separate pieces bounded both in their powers and geographic reach is of irreplaceable value when it comes to securing the liberty of the people. . . . Congress has repeatedly displayed a preference for geographically divided power in its treatment of the federal judiciary. . . .").

ensuring that federal judges have meaningful connections to their districts.[75] The division of the federal judiciary into districts prevents one state from infringing on another's jurisdiction, thus protecting each state's sovereignty.[76] In a modern-day context, this geographical division, when coupled with requirements for personal and subject matter jurisdiction, also constrains forum shopping by parties, such as by police applying for warrants.[77]

The proposed exception to territorial limitations does not imperil these federalism concerns because the exception will only apply in situations where no other district court has apparent jurisdiction. Therefore, the solution will preserve the geographical division of the federal judiciary, thus preventing concentration of power geographically and avoiding federalism concerns.[78] Further, allowing federal courts to extend their authority outside U.S. territory would not threaten the states' rights protected by a geographically-rooted federal judiciary because the court would not infringe on another district's jurisdiction.[79]

An alternative solution authorizing a "national warrant" to be issued by a single court might risk the concentration of power that the establishment of the geographically aligned district courts sought to avoid. First, in practice, this solution would encourage law enforcement to forum shop for a sympathetic judge.[80] Second, restraining forum-shopping by assigning the responsibility to a

---

[75] *See* Sharon E. Rush, *Federalism, Diversity, Equality, and Article III Judges: Geography, Identity, and Bias*, 79 MO. L. REV. 119, 131 (2014).

[76] *See id.* at 131 ("It would be unthinkable for a state to have no federal district court judges. . . . It would be unimaginable to have a Kansas resident sitting as a federal judge in Nebraska. . . ."). The system of federalism was not only concerned with the federal government's power over the states, but also larger, more powerful states dominating others. *See* Thomas B. Colby, *In Defense of the Equal Sovereignty Principle*, 65 DUKE L.J. 1087, 1104–06 (2016) (discussing the "equal footing principle").

[77] *See* People v. Fleming, 631 P.2d 38, 44 (Cal. 1981) (holding that limiting a magistrate's jurisdiction to issue search warrants for property in other counties to cases where the crime would likely be prosecuted locally addressed defendant's fears that officers might "forum shop" for favorable magistrates); *see also* United States v. Leon, 468 U.S. 897, 918 (1984) (noting that deterring police from "magistrate shopping" when applying for search warrants "promotes the ends of the Fourth Amendment"); Castillo v. State, 810 S.W.2d 180, 184 (Tex. Crim. App. 1990) (en banc) (holding that interpreting a wiretapping statute too broadly would allow a search anywhere in the state to be authorized by a judge in any district, allowing forum shopping and "effectively destroying the [statute's] territorial restrictiveness"), *superseded by statute*, TEX. CRIM. PROC. CODE ANN. art. 18.20, § 3(b) (West 2018).

[78] *See Krueger*, 809 F.3d at 1125 (Gorsuch, J., concurring).

[79] *See* Rush, *supra* note 75, at 131–32, 163 (noting that geographic organization of federal courts serves state interests by ensuring judges identify with a state as a "territorial community"). Requirements for judges to reside in their own district instead of another state and the state-based nominee selection process ensure judges have a geographic connection to their states. *Id.* at 130.

[80] *See Fleming*, 631 P.2d at 44 (holding that limiting a magistrate's jurisdiction to issue search warrants for property in other counties to cases where the crime would likely be prosecuted locally addressed defendant's fears that officers might "forum shop" for favorable magistrates); *Leon*, 468 U.S. at 918 (noting that deterring police from "magistrate shopping" when applying for search warrants "promotes the ends of the Fourth

single court would inundate that court with a workload pertaining to matters outside its geographic jurisdiction,[81] raising the very concerns about states' rights discussed above.[82]

One way to avoid the problems of geographic concentration of power would be for the D.C. Circuit to issue search warrants when no federal district is known to have jurisdiction. The D.C. Circuit already has special statutory jurisdiction over certain types of cases[83] and is composed of judges from diverse parts of the country.[84] However, the D.C. Circuit does not issue warrants and deals with far fewer criminal cases than other circuits,[85] which potentially inhibits the development of circuit case law and expertise in that field.[86] Therefore, limiting the proposed exception to the court which has jurisdiction over the underlying crime provides a better solution by keeping the warrant-issuing authority co-located with the court having the most interest in resolving the prosecution of the underlying crime.

In addition to federalism concerns, dividing the federal judiciary into state-based districts also facilitates two constitutional rights granted to persons accused of crimes: (1) Article III, Section 2 of the Constitution requires that criminal trials be held in the state where the crime was committed,[87] and (2) the Sixth Amendment provides the accused with the right to a jury composed of the residents of the state and district in which the crime was committed.[88] While

---

Amendment"); *Castillo*, 810 S.W.2d at 184 (en banc) (holding that interpreting a wiretapping statute too broadly would allow a search anywhere in the state to be authorized by a judge in any district, allowing forum shopping and "effectively destroying the [statute's] territorial restrictiveness"), *superseded by statute*, TEX. CRIM. PROC. CODE ANN. art. 18.20, § 3(b) (West 2018).

[81] A single investigation led to cases in forty-four districts across the country. United States v. Taylor, 250 F. Supp. 3d 1215, 1222–23 (N.D. Ala. 2017) (collecting cases).

[82] *Supra* note 76.

[83] *See* Eric M. Fraser et al., *The Jurisdiction of the D.C. Circuit*, 23 CORNELL J.L. & PUB. POL'Y 131, 144–50 (2013) (compiling statutory expansion of D.C. Circuit jurisdiction).

[84] *See id.* at 136 (noting that the President may nominate someone from any part of the country for the D.C. Circuit, and local senators do not exist to influence the nomination process). This lack of geographic tie to one area dispels the geographic bias discussed *supra* note 76. The D.C. Circuit's statutory workload mostly consists of administrative appeals from federal agencies located in the nation's capital. *See* Fraser, *supra* note 83, at 142–43.

[85] *See* Fraser, *supra* note 83, at 138 (observing that the D.C. Circuit is "an outlier" because criminal cases occupy "less than 10% of its docket, or just over a third of the national rate").

[86] *See* Paul R. Gugliuzza, *Rethinking Federal Circuit Jurisdiction*, 100 GEO L.J. 1437, 1465–66 (2012) (arguing that the Federal Circuit fails to develop expertise that would positively influence its development of patent law because the Circuit hears few commercial disputes).

[87] U.S. CONST. art. III, § 2, cl. 3. Locations for trials for crimes "not committed within any state" are set by federal statute. *Id.*

[88] U.S. CONST. amend. VI ("In 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 . . . .").

these rights dictate the location of a criminal trial, they do not affect which court may issue a warrant, and thus they would not be endangered by an expansion of the magistrate judges' authority to issue warrants.[89]

2. Absence of Constitutional Prohibitions on Expansion of Authority

While dividing the judiciary into districts advances federalism, there is no clear constitutional prohibition against judges issuing search warrants outside their districts. Indeed, the Constitution's text provides little guidance on government searches.[90] The Founders' intent regarding police investigative activity is difficult to discern because policing looked very different in their time.[91] The Fourth Amendment was originally intended to rein in the federal government, which at the time did not provide federal law enforcement jurisdiction over common law crimes such as burglary or murder.[92] Further, proactive criminal investigations did not exist, due to the lack of a modernized, professionalized police force.[93] The government mainly conducted searches to locate stolen property rather than to collect evidence, because forensic science had not yet developed to use evidence to solve crimes.[94] The first evidentiary search warrants did not appear until the twentieth century and were not condoned by the Supreme Court until 1967.[95]

Instead of having their role defined directly by the Framers, evidentiary search warrants inherited their geographic limitations from arrest warrants, which did exist at the time the Fourth Amendment was written.[96] Early American cases demonstrate that territorial limitations on arrest warrants stemmed from jurisdictional limitations on the authority of the Executive Branch.[97] Police could not execute an arrest warrant outside their jurisdiction,

---

[89] At trial, the defendant may challenge the constitutionality of the warrant regardless of which court issued it. *See* Alderman v. United States, 394 U.S. 165, 171–72 (1969) (holding that defendants whose Fourth Amendment rights were violated have standing to suppress evidence).

[90] *See* George C. Thomas III, *Stumbling Toward History: The Framers' Search and Seizure World*, 43 TEX. TECH L. REV. 199, 199 (2010) (noting that the Constitution's text "does not provide a workable metric for a general theory of the appropriate limits on government searches and seizures").

[91] *See id.* at 200.

[92] *Id.* at 208.

[93] Davies, *supra* note 73, at 620; Thomas III, *supra* note 90, at 201.

[94] Davies, *supra* note 73, at 627.

[95] *Compare* Gouled v. United States, 255 U.S. 298, 309 (1921) (holding that search warrants may not be used to merely search for evidence, but only to seize stolen property), *with* Warden v. Hayden, 387 U.S. 294, 300–01 (1967) (holding that the Fourth Amendment permitted evidentiary warrants).

[96] Davies, *supra* note 73, at 552.

[97] *See, e.g.*, Lawson v. Buzines, 3 Del. 416, 416–17 (1842) (holding that constable of Wilmington had no authority outside city limits, despite having an arrest warrant); York v. Commonwealth, 82 Ky. 360, 364 (1884) (holding that county sheriff could not authorize deputy to arrest someone pursuant to warrant issued in another

whether it was a municipality or county, because their own authority was confined to their jurisdiction.[98] The legislature also had no authority to give the executive power to conduct arrests outside the legislature's own territorial limits.[99] However, these early cases dealt with local police belonging to a specific county or municipality.[100] Today's federal law enforcement agents are not limited to a federal district, but instead operate nationwide and occasionally on foreign territory.[101] Further, law enforcement conduct searches using search warrants extending outside the issuing court's district pursuant to several exceptions discussed below.[102]

3. Existing Exceptions

Exceptions to the geographic limitations on federal courts' authority already exist without running afoul of constitutional concerns. Rule 41, which provides that "a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district,"[103] has been amended multiple times in the last three decades to authorize federal magistrate judges to issue warrants that will be executed outside of their districts in certain situations.[104] These exceptions seek to provide law enforcement with a mechanism to obtain warrants across district boundaries when government investigations necessarily implicate the Fourth Amendment.

---

county); Copeland v. Islay, 19 N.C. 505, 508 (1837) (holding that county constable has no right to arrest person pursuant to warrant issued in another county).

[98] *See, e.g.*, *Lawson*, 3 Del. at 416–17 (holding that constable for Wilmington city has no authority outside city limits despite having an arrest warrant); *York*, 82 Ky. at 364 (holding that county sheriff cannot authorize deputy to arrest someone pursuant to warrant issued in another county); *Copeland*, 19 N.C. at 508 (holding that county constable has no right to arrest person pursuant to warrant issued in another county).

[99] *See* Butolph v. Blust, 5 Lans. 84, 88–89 (N.Y. Gen. Term 1871) (holding that city council has no authority to give police the authority to arrest someone outside of city limits).

[100] *See, e.g.*, *Lawson*, 3 Del. at 416–17 (holding that constable for Wilmington city has no authority outside city limits despite having an arrest warrant); *York*, 82 Ky. at 364 (holding that county sheriff cannot authorize deputy to arrest someone pursuant to warrant issued in another county); *Copeland*, 19 N.C. at 508 (holding that county constable has no right to arrest person pursuant to warrant issued in another county).

[101] *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 262, 274–75 (1990) (holding that U.S. officials' search of a house in Mexico did not violate the Fourth Amendment); Kevin L. Perkins, Assistant Dir., Criminal Investigative Div., FBI, Statement Before the Commission on Wartime Contracting in Iraq and Afghanistan, FBI: TESTIMONY (May 24, 2010), https://archives.fbi.gov/archives/news/testimony/the-fbis-efforts-to-combat-international-contract-corruption (discussing investigations by U.S. contracting officers during military operations).

[102] *See* FED. R. CRIM. P. 41(b).

[103] *Id.* at (b)(1).

[104] For a history of the amendments to Rule 41, see FED. R. CRIM. P. 41 advisory committee's notes to 1989, 1990, 1993, 2002, and 2006 amendments.

For example, Congress amended Rule 41 in 1990 to allow federal magistrate judges to issue search warrants for property within the district that may move outside the district prior to the warrant's execution.[105] Two obstacles motivated this exception: first, the "inevitable delays" between application for a warrant and its execution; and second, the need to provide a "practical tool" so that law enforcement would not have to seek warrants in several districts for the same property or rely on an exception to the warrant requirement.[106]

Technological advances have also motivated exceptions to the geographical limitations on magistrate judges' authority. The Court held in *United States v. Karo* that monitoring a target's movement with a tracking device could implicate the Fourth Amendment as a search.[107] However, at the time, no federal procedure expressly allowed law enforcement to request a warrant to monitor a tracking device that might cross district lines, despite the inherently mobile nature of such investigations.[108] To fill this gap between the Fourth Amendment's requirements and judges' authority, an exception was added to Rule 41 in 2006 allowing magistrates to issue warrants to monitor tracking devices that might leave the district.[109] The tracking device exception exists because law enforcement lacks knowledge of where the suspect or evidence may be located at the time the tracking device facilitates the search.[110] Similarly, this Comment's proposed exception allows the magistrate judge to issue a warrant when law enforcement cannot determine where the search will be executed.[111]

---

[105] FED. R. CRIM. P. 41(b)(2); FED. R. CRIM. P. 41 advisory committee's note to 1990 amendments. The Judicial Conference of the United States' Advisory Committee on Criminal Rules prepares recommended changes and accepts public input in the administrative notice-and-comment procedure. *See* Adams, *supra* note 25, at 745–46 (describing the process for amending the Federal Criminal Rules of Procedure). Afterwards, if in favor of the changes, the Supreme Court approves amendments and provides the proposed changes to Congress for final approval. *Id.* at 749.

[106] FED. R. CRIM. P. 41 advisory committee's note to 1990 amendments; FED. R. CRIM. P. 41(b)(2).

[107] 468 U.S. 705, 716 (1984) (holding that government monitoring of the location of a person or object with an electronic device may be Fourth Amendment activity requiring a warrant).

[108] *See* FED. R. CRIM. P. 41 advisory committee's note to 2006 amendments. The Advisory Committee did not rely on the exception allowing a search of an item that may move prior to execution, which did not exist when *Karo* was decided, but instead provided detailed instructions for application and execution of tracking device warrants. *See id.*; FED. R. CRIM. P. 41 advisory committee's note to 1990 amendments.

[109] FED. R. CRIM. P. 41(b)(4); FED. R. CRIM. P. 41 advisory committee's note to 2006 amendments (recommending limiting the exception to federal judges because the tracking activity may cross state lines).

[110] United States v. Jean, 207 F. Supp. 3d 920, 942 (W.D. Ark. 2016) ("The whole point of seeking authority to use a tracking device is because law enforcement does not know where a crime suspect—or evidence of his crime—may be located.")

[111] *See id.* (applying the tracking device exception to a remote access warrant where the location of the computer to be searched was unknown, due to the similarity in principles).

The increased significance of terrorism investigations after the 9/11 attacks gave rise to an exception for terrorism investigations.[112] The difficulty of obtaining warrants for searches that might be executed in multiple districts impeded investigations of potential terrorists.[113] To evade surveillance by law enforcement, terrorists changed cell phones frequently and routed email through different servers.[114] Recognizing that "technology ha[d] dramatically outpaced our statutes," the Attorney General called for procedural and statutory amendments allowing courts to issue warrants outside their territorial jurisdiction for terrorism investigations.[115] The 2002 exception allowed federal magistrates to issue warrants for persons or property "within or outside" their district when activities related to terrorism may have occurred in their district.[116]

By providing a procedure to obtain warrants in situations where warrants are deemed necessary yet geographical limitations would otherwise constrain magistrate judges, these exceptions "further[] the constitutional preference for warrants."[117] Enabling law enforcement to obtain warrants "encourages reliance on warrants" instead of merely on the Fourth Amendment's reasonableness requirement.[118] These repeated amendments to Rule 41 demonstrate that where the Fourth Amendment requires a search warrant, a mechanism should be developed to authorize judges to issue one. The constitutional preference for warrants combined with the practicality concerns discussed above outweigh potential concerns such as federalism.

B. Extraterritoriality Concerns

In addition to comporting with the constitutional purposes of territorial limits on courts' authority, the proposed exception also complies with constraints on extraterritorial jurisdiction.[119] Regardless of any geographic limitations on search warrants, Congress can lawfully regulate or criminalize conduct on

---

[112] FED. R. CRIM. P. 41(b)(3); FED. R. CRIM. P. 41 at advisory committee's note to 2002 amendments.

[113] *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the H. Comm. on the Judiciary*, 107th Cong. (2001) (testimony of John Ashcroft, Att'y Gen. of the United States); *id.* (statement of F. James Sensenbrenner, Jr., Chairman of the House Committee on the Judiciary) (stating the need for legislation to "allow the FBI to obtain a search warrant from one court to investigate crimes of terrorism rather than requiring them to waste precious investigative time going to 94 different federal judicial districts").

[114] *Id.* (testimony of John Ashcroft, Att'y Gen. of the United States).

[115] *Id.* ("We're not asking the law to expand, just to grow as technology grows.").

[116] FED. R. CRIM. P. 41(b)(3); FED. R. CRIM. P. 41 advisory committee's note to 2002 amendments.

[117] FED. R. CRIM. P. 41 advisory committee's note to 1990 amendments.

[118] *Id.*; *see* U.S. CONST. amend. IV ("The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated . . . .").

[119] These concerns are further minimized by the limitations on the warrant's authority, as discussed in Section III.A. below.

foreign soil when the Constitution grants Congress such authority.[120] For example, Congress may prohibit U.S. citizens or permanent residents from engaging in illicit sexual conduct in a foreign country based on the Foreign Commerce Clause.[121] Congress also may regulate activity by foreign entities overseas when the activity affects the United States.[122]

Criminalizing extraterritorial conduct sometimes leads to criminal investigation and prosecution of persons residing overseas, resulting in U.S. courts extending authority outside the United States.[123] The United States may request extradition of the accused when he is overseas,[124] a grand jury may issue subpoenas for witnesses and information located overseas,[125] and a court may impose punitive measures upon a defendant whose only connection to the United States may be the offense he committed.[126] When so many aspects of criminal investigation and prosecution already reach overseas, it is odd that magistrate judges lack the requisite statutory authority and procedural mechanisms to issue search warrants for evidence that may be located abroad.[127]

---

[120] *See, e.g.*, RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2103 (2016) (holding that the Racketeer Influenced and Corrupt Organizations Act applies to some foreign racketeering activity); United States v. Yunis, 924 F.2d 1086, 1090 (D.C. Cir. 1991) (holding that the federal Hostage Taking Act provided jurisdiction over a defendant found outside the United States); *see also* Naomi Harlin Goodno, *When the Commerce Clause Goes International: A Proposed Legal Framework for the Foreign Commerce Clause*, 65 FLA. L. REV. 1139, 1144 (2013) (collecting federal laws governing U.S. citizens' conduct abroad).

[121] *See* United States v. Bollinger, 798 F.3d 201, 214–15 (4th Cir. 2015) (holding that Congress can criminalize sexual activity overseas under the Foreign Commerce Clause). The Foreign Commerce Clause provides that "Congress shall have the power . . . [t]o regulate commerce with foreign nations." U.S. CONST. art. I, § 8, cl. 3.

[122] *See, e.g.*, *RJR Nabisco, Inc.*, 136 S. Ct. at 2105 (holding that the Racketeer Influenced and Corrupt Organizations Act applies to foreign entities engaging in foreign enterprises when they affect commerce involving the United States).

[123] *See, e.g.*, United States v. Knowles, 197 F. Supp. 3d 143, 147, 152 (D.C. Cir. 2016) (holding that a U.S. statute criminalized a Jamaican citizen's conspiracy to distribute narcotics using an aircraft with U.S. connections, resulting in the defendant's extradition from Colombia for prosecution in the United States).

[124] *See* William Magnuson, *The Domestic Politics of International Extradition*, 52 VA. J. INT'L L. 839, 845 (2012) (discussing history of international extradition).

[125] *See* United States v. First Nat'l City Bank, 396 F.2d 897, 900–01 (2d Cir. 1968) (holding that a court may compel production of items if it has personal jurisdiction over the possessor).

[126] *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990) (upholding the conviction of a Mexican national "with no voluntary attachment to the United States," who resided in Mexico and was only brought into the United States in custody for criminal prosecution).

[127] For federal offenses where relevant conduct occurs partly or entirely on foreign soil, relevant evidence may lie outside the United States. *See id.* at 262, 274–75 (holding that U.S. officials' search of a house in Mexico did not violate the Fourth Amendment); Perkins, *supra* note 101; DRUG ENF'T ADMIN., *supra* note 101. The Federal Rules of Criminal Procedure have been amended to reflect the possible need for warrants that may be executed overseas, as discussed in Section I.A. *See* FED. R. CRIM. P. 41 advisory committee's note to 1990 amendments (noting that amendments are intended to clarify procedures for obtaining a warrant for an extraterritorial search).

Although various statutes criminalize conduct that occurs in foreign countries, courts interpret them under a presumption against extraterritoriality to avoid inadvertently causing international discord.[128] Courts assume that "Congress generally legislates with domestic concerns in mind."[129] However, a clear, affirmative indication that Congress intended extraterritorial application rebuts that presumption.[130] Without such an indication, the court must determine whether applying the statute in this case would be an impermissible extraterritorial application.[131] "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application, even if other conduct occurred abroad . . . ."[132] However, if conduct relevant to the focus occurred in a foreign country, then the case is an extraterritorial application, regardless of any other domestic conduct.[133]

If the statute applies extraterritorially, such application must not violate due process under the Fifth Amendment.[134] Lower courts are split on the proper test for due process in such cases.[135] Some circuits require that a nexus must exist between the defendant and the United States, such that applying the statute extraterritorially would not be arbitrary or fundamentally unfair.[136] This nexus may include (1) the defendant's U.S. citizenship or residency, (2) the location of the acts giving rise to the offense, (3) the intended effect the defendant had on or within the United States, and (4) the effect on significant U.S. interests.[137] Under such reasoning, a foreign national could face federal charges of assault

---

[128] RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2100 (2016).

[129] *Id.* (applying the presumption against extraterritorially "regardless of whether there is a risk of conflict between the American statute and a foreign law" because the presumption "reflects the . . . 'commonsense notion that Congress generally legislates with domestic concerns in mind'").

[130] *See* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255, 265 (2010).

[131] *Id.* at 266.

[132] *RJR Nabisco, Inc.*, 136 S. Ct. at 2101.

[133] *Id.* Prior to *Morrison*, the Charming Betsy canon of statutory construction recommended that "an act of [C]ongress ought never to be construed to violate the law of nations, if any other possible construction remains." Weinberger v. Rossi, 456 U.S. 25, 32 (1982) (quoting Murray v. The Charming Betsy, 6 U.S. (2 Cranch) 64, 118 (1804)).

[134] United States v. Brehm, 691 F.3d 547, 552 (4th Cir. 2012) ("Though a criminal statute having extraterritorial reach is declared or conceded substantively valid under the Constitution, its enforcement in a particular instance must comport with due process.").

[135] Dan E. Stigall, *International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law*, 35 HASTINGS INT'L & COMP. L. REV. 323, 347 (2012).

[136] *See, e.g.*, United States v. Davis, 905 F.2d 245, 248–49 (9th Cir. 1990) ("In order to apply extraterritorially a federal criminal statute to a defendant consistently with due process, there must be a sufficient nexus between the defendant and the United States so that such application would not be arbitrary or fundamentally unfair.") (citation omitted).

[137] *Brehm*, 691 F.3d at 552–53 (holding that pervasive U.S. influence on a NATO military base, even when the defendant and his victim were both foreign citizens, established sufficient nexus to satisfy due process).

for stabbing another foreign national on a NATO base in Afghanistan, due to (1) the pervasive U.S. influence on the base, (2) the significant U.S. interest in maintaining discipline and readiness on the base, and (3) the defendant's presence on the base working for a U.S. contractor.[138]

However, other circuits do not require a nexus to satisfy due process, but instead require that prosecution must be neither arbitrary nor fundamentally unfair.[139] Various circuits apply this alternate test differently, even when applying the same statute,[140] examining whether (1) the defendant had notice that his activities may subject him to criminal prosecution in the United States;[141] or (2) U.S. jurisdiction comported with international law principles.[142]

Even when application of the statute to foreign conduct comports with due process requirements, the court still must have jurisdiction to try the case.[143] For crimes that are not committed within any state, Congress may provide statutory authority for jurisdiction.[144] Accordingly, many statutes contain a jurisdictional hook enabling prosecution in a certain federal district when the criminal activities took place outside U.S. territory.[145]

---

[138] *Id.*

[139] United States v. Ballestas, 795 F.3d 138, 148 (D.C. Cir. 2015) ("The ultimate question under the Due Process Clause is not nexus, but is whether application of the statute to the defendant would be arbitrary or fundamentally unfair.") (internal brackets omitted).

[140] *Compare id.* (holding that applying the U.S. Maritime Drug Law Enforcement Act (MDLEA) to a drug smuggler on the high seas comported with due process because he was aware that the smuggling organization deliberately evaded U.S. law enforcement), *with* United States v. Cardales, 168 F.3d 548, 553 (1st Cir. 1999) (holding that applying MDLEA to a drug smuggler on the high seas comported with due process because the territorial and protective principles of international law allowed jurisdiction).

[141] *See Ballestas*, 795 F.3d at 148 (holding that applying U.S. criminal statutes to a drug smuggler on the high seas satisfied due process because he was aware that the smuggling organization deliberately evaded U.S. law enforcement).

[142] *See Cardales*, 168 F.3d at 553 (holding that U.S. jurisdiction over a drug smuggler on the high seas comported with due process because the territorial and protective principles of international law allowed jurisdiction); United States v. Ibarguen-Mosquera, 634 F.3d 1370, 1379 (11th Cir. 2011) (holding that U.S. jurisdiction over drug smugglers on the high seas satisfied due process because "international law permits any nation to subject stateless vessels on the high seas to its jurisdiction").

[143] *See* 28 U.S.C. § 636(a) (2012) (providing federal magistrate judges with authority within their district "and elsewhere as authorized by law"). Congress extended the power of magistrate judges beyond their districts to "elsewhere as authorized by law" based on problems identified after Hurricane Katrina, which impeded operation of the federal courts in Louisiana. *See* United States v. Krueger, 809 F.3d 1109, 1121 (10th Cir. 2015) (Gorsuch, J., concurring) (discussing history of 28 U.S.C. § 636(a) (2000)); *see also* 28 U.S.C. § 48(e) (2012).

[144] U.S. CONST. art. III, § 2, cl. 3 (stating that for crimes "not committed within any State, the Trial shall be at such Place or Places as the Congress may by law have directed").

[145] *See, e.g.*, 21 U.S.C. § 959(c) (2012) (establishing extraterritorial jurisdiction in the federal district where the offender enters the United States or, alternately, the district court for the District of Columbia, for certain drug offenses). Statutes providing jurisdiction in the D.C. Circuit as an alternate forum support the

C. Physical and Non-Physical Searches

One possibility to further minimize potential conflicts resulting from extraterritorial application of authority would be to limit this exception to digital data. However, limitations based on digital data would cause uncertainty and may become outdated as technology outpaces the law.[146] This Comment recommends applying the exception to Rule 41 proposed above not only to purely digital searches but also to physical searches conducted by law enforcement in person at the site of the object to be searched. This should occur for two important reasons. First, even a digital search has physical components. Second, creating separate rules for data will create problems defining what items are sufficiently intangible for their physical location to be immaterial under the law.

Under the law, a digital search takes place in a physical location, on the target computer.[147] Although police physically remain at their desks when remotely searching a computer that is located in another state or country, the search itself invades the computer.[148] Therefore, a purely digital search may infringe on the jurisdiction of the state or country where the computer is located, requiring authorization from local authorities.[149] While a digital invasion by foreign law enforcement may be less intrusive than a physical invasion, the host nation may still have rights it wishes to assert.[150] A rule that provides solely for digital searches still must recognize the importance of coordinating with the jurisdiction that contains the computer to be searched, when feasible, to reduce conflict between sovereigns and to preserve comity.[151] Of course, law enforcement

---

alternate solution discussed in Section II.A.1. of using the D.C. Circuit for warrants where no other court is known to have jurisdiction.

146 *See In re* Two Email Accounts, No. 17-M-1235, 2017 WL 2838156, at *1 (E.D. Wis. June 30, 2017) ("As technology continues to change beyond bounds even imagined three decades ago . . . the law might again be called 'hopelessly out of date.'").

147 *See* United States v. Horton, 863 F.3d 1041, 1047–48 (8th Cir. 2017) (holding that a search by remote access using hacking software took place where the computer was physically located, not at the physical site where law enforcement uploaded the software onto the internet).

148 *Id.*

149 *See* Brief for Ireland as Amicus Curiae in Support of Neither Party at 1, Microsoft III, 138 S. Ct. 1186 (2018) (No. 17-2), 2017 WL 6492481, at *1 (expressing Ireland's "genuine and legitimate interest in potential infringements by other states of its sovereign rights with respect to its jurisdiction over its sovereign territory" when U.S. law enforcement attempted to compel a U.S. ISP to disclose digital data stored in Ireland, even though any intrusion by U.S authorities or their agents into Ireland would be solely digital instead of physical).

150 *See id.*

151 *See id.* at *1–2; Bert-Jaap Koops & Morag Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law* 8–9 (Tilburg Law Sch. Legal Studies Research Paper Series, No. 05/2016), https://ssrn.com/abstract=2698263 (discussing how the disconnect between traditional international norms of jurisdiction based on territoriality and cybercrimes which transcend

cannot coordinate with that jurisdiction until the computer's location has been identified through a search.[152] The international norms for handling such investigations are still evolving.[153] In the United States, the CLOUD Act, which was passed in 2018, addresses such concerns in the context of warrants compelling ISPs to disclose customer data by requiring courts to consider comity before issuing the warrant.[154]

Another problem with creating a separate rule for data is that such an exception would imply that data is not subject to jurisdiction based on its physical location, but rather subject to jurisdiction based on the location of whoever can access the data. Such a rule would fail to protect the interests of the nation or state hosting the data.[155] Further, relying on data's "exceptional" nonphysical properties ignores the fact that other intangible, movable property, such as money, is subject to jurisdiction based on its physical location.[156] Creating a separate rule for data also introduces the problem of what counts as data; for example, funds in bank accounts may be "data" under such a rule.[157] This Comment's proposed solution avoids creating an unnecessary and confusing disparity by treating all items for search or seizure the same and simply focusing on where the underlying crime can be prosecuted.

III. IMPLICATIONS

While providing federal judges the authority to issue warrants for search or seizure of property based on their jurisdiction over the underlying crime does not violate constitutional principles, this proposed exception will affect various parties, as discussed in section III.A. Further, this solution may open a window for expanding the territorial limitations on the Fourth Amendment's protection beyond U.S. soil, as analyzed below in section III.B.

---

physical borders can lead one nation's law enforcement to infringe on another's national sovereignty during cyber investigations).

[152] Law enforcement would not know whether the search took place outside the United States until the search had already been executed. *See Horton*, 863 at 1047–48 (holding that a warrant seeking to remotely search a computer to determine its physical location was invalid because the issuing judge had no authority over the location where the warrant was ultimately executed); United States v. Scanlon, No. 2:16-cr-73, 2017 WL 3974031, at *12 (D. Vt. Apr. 26, 2017).

[153] *See* Koops & Goodwin, *supra* note 151.

[154] Pub. L. No. 115-141, 132 Stat. 348 (2018) (amending the Stored Communications Act, 18 U.S.C. § 2703 (2012)).

[155] *See supra* note 149 and accompanying text.

[156] *See* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 756–58 (2016) (comparing digital data to other intangible assets such as stock or debts).

[157] *See id.*

A. Immediate Implications

The proposed solution will impact multiple parties and must be carefully tailored to avoid infringing on complex issues of international comity. Because this exception would be limited to federal courts, its effect would be limited to situations where law enforcement could obtain a federal warrant. The expanded warrant authority will affect defendants, law enforcement, and third-party information providers such as ISPs by providing a mechanism for obtaining warrants in situations when such authority was questioned in the past, as section A.1. discusses. Section A.2. explains that this proposed expansion of jurisdiction will not harm international comity because the U.S. warrant will only provide authority under U.S. laws and will explicitly state that any necessary host nation authority must also be obtained.

1. Defendants, Law Enforcement, and Third-Party Information Providers

The expansion of federal courts' jurisdiction to issue warrants will benefit law enforcement, defendants, and third-party information providers by clarifying courts' authority and providing the protection of a warrant.[158] It will not significantly affect individual user privacy, as discussed below.

Providing a mechanism to seek search warrants furthers the constitutional preference for warrants,[159] serving the interests of defendants and law enforcement. Currently, when no court has jurisdiction to issue a warrant, a search must only satisfy the Fourth Amendment's Reasonableness Clause.[160] Warrants serve the Fourth Amendment's purpose better because they allow *ex ante* judicial examination of the constitutionality of searches, preventing unnecessary violations of defendants' rights.[161] In the absence of a warrant process, a court will not examine a search's constitutionality until criminal charges are filed and the defendant challenges admission of evidence the search

---

[158] Intelligence and national security operations will not be affected, since exceptions already exist for them. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 292 (1990) (Brennan, J., dissenting).

[159] *See* United States v. Ventresca, 380 U.S. 102, 105–06 (1965) ("[T]he informed and deliberate determinations of magistrates empowered to issue warrants are . . . to be preferred over the hurried actions of officers . . . . The reasons for this rule go to the foundations of the Fourth Amendment.") (citation omitted).

[160] U.S. CONST. amend. IV ("The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated . . . ."); *see* United States v. Odeh, 552 F.3d 157, 171 (2d Cir. 2008) (holding that because the Warrant Clause did not apply overseas, searches of persons protected by the Fourth Amendment were only governed by the Reasonableness Clause).

[161] *See Ventresca*, 380 U.S. at 106 (noting that the Fourth Amendment requires inferences about probable cause to be "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime").

produced.[162] Disputing the search afterwards does not undo police violations of the defendant's privacy.[163] Further, *ex post* judicial assessments of searches are less efficient from a law enforcement perspective because police have already committed finite resource towards an entire investigation, all of which may become inadmissible as fruit of an original unconstitutional search.[164] In contrast, the warrant process allows a court to rule on the search's constitutionality before the defendant has suffered a violation and before the police have expended resources on a lengthy investigation.[165]

Although this exception authorizes warrants for overseas searches, it is possible that courts will continue to apply the Reasonableness Clause[166] instead of the Warrant Clause[167] to searches that take place in foreign territory. However, the benefits of *ex ante* judicial approval for searches and the difficulty

---

[162] *See Odeh*, 552 F.3d at 170–71 (examining reasonableness of a warrantless search by U.S. officials overseas).

[163] *See* Linkletter v. Walker, 381 U.S. 618, 637 (1965) ("[T]he ruptured privacy of the victims' homes and effects cannot be restored. Reparation comes too late."); *see also* William C. Heffernan, *The Fourth Amendment Exclusionary Rule as a Constitutional Remedy*, 88 GEO. L.J. 799, 800 (2000) ("According to the Court, once a government official interferes with the privacy the Fourth Amendment protects, the harm someone has suffered as a result cannot be repaired; privacy wrongs, the Court reasons, are irreversible and so irreparable.").

[164] In the absence of a warrant, nothing that the search uncovers can be used as evidence at trial. *See* Mapp v. Ohio, 367 U.S. 643, 648, 660 (1961) (holding that evidence seized in violation of the Fourth Amendment must be excluded from use in federal and state court). Even derivative evidence may be excluded when discovered as a result of earlier evidence found in an illegal search. Murray v. United States, 487 U.S. 533, 536–37 (1988). Although exceptions to the warrant requirement exist, they do not apply in this context. *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 351 (2009) (refining the conditions which permit a warrantless search of a vehicle incident to a recent occupant's arrest); United States v. Matlock, 415 U.S. 164, 171 (1974) (holding that no warrant is needed when a person with common authority over the premises to be searched consents); United States v. Robinson, 414 U.S. 218, 224 (1973) ("It is well settled that a search incident to a lawful arrest is a traditional exception to the warrant requirement of the Fourth Amendment . . . [A] search may be made of the person of the arrestee . . . [and] of the area within the control of the arrestee.").

[165] *See Ventresca*, 380 U.S. at 106 (noting that the Fourth Amendment requires inferences about probable cause to be "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime").

[166] When no court has jurisdiction to issue a warrant, a search must only satisfy the Fourth Amendment's Reasonableness Clause. U.S. CONST. amend. IV ("The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated . . . ."); *see Odeh,* 552 F.3d at 171 (holding that because the Warrant Clause did not apply overseas, searches of persons protected by the Fourth Amendment were only governed by the Reasonableness Clause).

[167] U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."). Where the Warrant Clause applies, warrantless searches are presumptively unreasonable unless an exception applies. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). However, the warrant requirement only applies where warrants can be issued, such as within the United States. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 278 (Kennedy, J., concurring) (noting that a warrantless search overseas home of alien nonresident did not violate the Fourth Amendment because no U.S. judge had authority to issue a warrant for that location).

of applying the reasonableness standard to overseas searches[168] may incentivize law enforcement agencies to adopt policies favoring warrants.[169] Further, the availability of a warrant process enables defendants to raise the absence of a warrant under a reasonableness inquiry when challenging the admissibility of evidence.[170]

This exception will not expand authority for physical searches within the United States, since a warrant authorizing a physical search must describe the location to be searched to satisfy the particularity requirement of the Fourth Amendment.[171] When the physical location within the United States is known, law enforcement may seek a warrant from a court whose jurisdiction embraces the place to be searched, and therefore this proposed exception will not apply. Physical searches on foreign soil are discussed in section III.A.2.

For domestic ISPs, this rule will clarify that they are not violating U.S. laws when they comply with warrants for data stored on remote servers overseas.[172] The application of this rule to foreign ISPs will depend on whether a U.S. court has personal jurisdiction over that ISP.[173] However, an ISP will have no standing

---

[168] *See Verdugo-Urquidez*, 494 U.S. at 278 (Kennedy, J., concurring) (noting the difficulty of establishing reasonableness of overseas searches due to "the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad").

[169] Warrants invoking the proposed exception will likely support complex, resource-intensive investigations for complex cybercriminal schemes or serious international crimes. *See* United States v. Workman, 863 F.3d 1313, 1315–16 (10th Cir. 2017) (describing elaborate FBI efforts to investigate recipients of child pornography by taking over a Dark Net forum and disseminating code to unwitting users allowing the FBI to remotely hack into their computers in search of identifying information, then obtaining warrants for physical searches of individual users' computers). In such investigations, law enforcement has high incentives to avoid errors such as unconstitutional searches that will cause key evidence to be excluded.

[170] *See Verdugo-Urquidez*, 494 U.S. at 278 (Kennedy, J., concurring) (noting that extending the Warrant Clause to noncitizens' foreign property was "impracticable" partly due to the lack of means for U.S. magistrates to issue warrants for such property).

[171] *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched . . . .'"). In contrast, a digital search may satisfy the particularity requirement by describing the computers accessing a certain website as the place to be searched. *See* United States v. Jean, 207 F. Supp. 3d 920, 935–36 (W.D. Ark. 2016) (holding that a warrant authorizing a remote search by hacking satisfied particularity requirements); *see generally* Adams, *supra* note 25, at 762–64 (discussing the application of the Fourth Amendment's particularity clause in remote digital searches).

[172] *See* Microsoft II, 829 F.3d 197, 211 (2d Cir. 2016) (discussing potential conflicts of laws caused by allowing U.S. statutory authority for warrants to extend to data stored overseas), *vacated as moot*, 138 S. Ct. 1186 (2018). The Court declined to address this issue in *Microsoft III*. 138 S. Ct. 1186, 1187–88 (2018).

[173] Even to enforce a subpoena *duces tecum*, the court must have enforcement jurisdiction over the party. *See, e.g.*, *In re* Grand Jury Subpoena Directed to Marc Rich & Co., 707 F.2d 663, 665–67 (2d Cir. 1983) (holding that a district court could enforce a subpoena *duces tecum* against a foreign corporation based on personal jurisdiction over its subsidiary located in the United States, even when the materials sought were located overseas and production violated the host nation's laws).

as a third party to challenge the introduction of evidence in the criminal case.[174] Therefore, ISPs litigating disclosure of customer data provide imperfect stand-ins for the defendant's Fourth Amendment rights. Further, individual users might have difficulty establishing standing because they have shared the data with a third party, the ISP, potentially diminishing their reasonable expectation of privacy in the data.[175] Thus, individual users who wish to keep their data out of the reach of the U.S. government may still seek to store it on servers hosted by foreign ISPs.[176] However, these measures may not meaningfully increase user privacy because the host nation will still have territorial jurisdiction over the data, as discussed below.[177]

This Comment's proposed exception to territorial restrictions will not significantly reduce individual user privacy because many nations already have the legal framework to access data stored overseas.[178] Ten developed nations, including the United States, require cloud data service providers to disclose customer data for government investigations.[179] All but two of these nations have laws requiring ISPs to comply with government requests for data located in another country.[180] Despite popular belief, the United States provides

---

[174] *See* Alderman v. United States, 394 U.S. 165, 171–72 (1969) (holding that suppression of a Fourth Amendment violation can be sought "only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of damaging evidence").

[175] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that a defendant could not claim a legitimate expectation of privacy in information revealed to a third party, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed" (quoting United States v. Miller, 425 U.S. 435, 443 (1976))). *But see* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.") (citations omitted).

[176] *See* Brief of the Government of the United Kingdom of Great Britain and Northern Ireland as Amicus Curiae in Support of Neither Party at 4, *Microsoft III*, 138 S. Ct. at 1186 (No. 17-2), 2017 WL 6398769, at *4 (discussing dangers of "offshore 'data haven' countries that would block legitimate access by foreign nations' law enforcement authorities, and help wrongdoers evade investigators").

[177] WINSTON MAXWELL & CHRISTOPHER WOLF, A GLOBAL REALITY: GOVERNMENTAL ACCESS TO DATA IN THE CLOUD 2 (2012), http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf (examining different nations' legal regimes providing government access to user data stored by third-party service providers).

[178] *Id.* at 13.

[179] *Id.* (examining laws and practices in Australia, Canada, Denmark, France, Germany, Ireland, Japan, Spain, United Kingdom, and the United States).

[180] *Id.* (noting that all ten countries require a cloud provider to disclose customer data in the course of a government investigation, but in circumstances where the cloud service provider stores data on servers in another country, only Germany and Japan require cooperation from the other country's government).

relatively stronger privacy protection than many other nations.[181] For example, of the ten, all but the United States and Japan allow a cloud data service provider to voluntarily disclose customer data to the government in response to an informal request instead of requiring a formal legal request.[182]

Other countries already allow government investigators to hack into private computers to identify anonymous users.[183] For example, the United Kingdom's Investigatory Powers Act 2016 authorizes law enforcement to hack into computers with a warrant.[184] A European Parliament study found that four out of six countries studied had adopted specific legislative provisions authorizing government hacking, and the remaining two were in the legislative process to enact such provisions.[185] However, of the six countries studied, only the Netherlands legally permitted the hacking of devices whose location was unknown.[186] Australia and Israel also allow warrants authorizing law enforcement hacking.[187]

This Comment's proposed exception for territorial limitations on federal courts' authority to issue warrants provides further protection to individual privacy by requiring that the court issuing the warrant have jurisdiction over the underlying crime.[188] This stipulation limits law enforcement's ability to shop for a favorable forum to issue the warrant[189] and ensures that the court issuing the

---

[181] *Id.* at 1 ("[E]ven European countries with strict privacy laws also have anti-terrorism laws that allow expedited government access to Cloud data. . . . France's anti-terrorism laws make the Patriot Act look 'namby-pamby' by comparison.").

[182] *Id.* at 13.

[183] *See, e.g.*, Investigatory Powers Act 2016, c. 25, Part 5 (Eng.) (authorizing "targeted equipment interference" warrants).

[184] *Id.* (authorizing "targeted equipment interference" warrants).

[185] EUROPEAN PARLIAMENT, *supra* note 60, at 42–44, 48 (finding that France, Germany, Poland, and the United Kingdom had specific laws authorizing government hacking). Italy and the Netherlands were scheduled to adopt such provisions. *Id.* All six countries required *ex ante* judicial authorization. *Id.* at 11.

[186] *Id.* at 11. Further, if the device turned out to be in another jurisdiction, Dutch police must apply for Mutual Legal Assistance to search it. *Id.*

[187] *Id.* at 49.

[188] Jurisdiction over the crime will depend on the authorization provided by the criminal statute, as discussed in Section II.B.

[189] *See* People v. Fleming, 631 P.2d 38, 44 (Cal. 1981) (holding that limiting a magistrate's jurisdiction to issue search warrants for property in other counties to cases where the crime would likely be prosecuted locally addressed defendant's fears that officers might "forum shop" for favorable magistrates); *see also* United States v. Leon, 468 U.S. 897, 918 (1984) (noting that deterring police from "magistrate shopping" when applying for search warrants "promotes the ends of the Fourth Amendment"); Castillo v. State, 810 S.W.2d 180, 184 (Tex. Crim. App. 1990) (en banc) (holding that interpreting a wiretapping statute too broadly would allow a search anywhere in the state to be authorized by a judge in any district, allowing forum shopping and "effectively destroying the [statute's] territorial restrictiveness"), *superseded by statute*, TEX. CRIM. PROC. CODE ANN. art. 18.20, § 3(b) (West 2018).

warrant has a cognizable interest in the matter. However, many federal crimes can be prosecuted in multiple places.[190] The difficulty of demonstrating where the crime may be prosecuted may provide an insurmountable practical impediment for cybercrime investigations when perpetrators' physical locations remain unknown.

Law enforcement may be able to demonstrate the courts' jurisdiction to issue a warrant based on victims' citizenship or the destinations of trafficked items.[191] However, issuing warrants without first demonstrating that the crime can be prosecuted in a particular district risks the possibility that law enforcement might discover after further investigation that *no* U.S. district has jurisdiction to prosecute it.[192] Without a criminal prosecution, the person whose computer was searched will have limited opportunity to contest the invasion of his privacy, since the primary tool for addressing Fourth Amendment violations, the exclusion of evidence, only operates at trial.[193]

2. Foreign Nations

Because the proposed exception allowing warrants to be issued when no U.S. court is known to have jurisdiction will include overseas searches, warrants will expressly state that they only provide authority under U.S. law. When required, law enforcement still must take the additional step of obtaining approval from host nation authorities. This requirement protects comity between sovereigns and reduces the potential conflict with foreign laws.[194] In practice, this constraint will have limited effect on remote searches but will prevent significant

---

[190] *See, e.g.*, 21 U.S.C. § 959(c) (2012) (establishing extraterritorial jurisdiction in the federal district where the offender enters the United States or, alternately, the district court for the District of Columbia, for certain drug offenses).

[191] *See, e.g.*, Stigall, *supra* note 135, at 333 (discussing countries assuming jurisdiction over crimes based on the victims' nationalities rather than the location of the offense); United States v. Davis, 905 F.2d 245, 248–49 (9th Cir. 1990) (discussing MDLEA, which provided U.S. courts jurisdiction over drug transactions "aimed at causing criminal acts within the United States").

[192] For a discussion on the jurisdiction to criminalize conduct, see cases cited *supra* note 120 and accompanying text.

[193] *See* Mapp v. Ohio, 367 U.S. 643, 652–53 (1961) (noting "[t]he obvious futility" of relying on remedies other than the exclusionary rule). Although individuals may bring private actions against the police for invasion of civil rights, many Fourth Amendment violations do not satisfy the requirements for such claims. *See* Herring v. United States, 555 U.S. 135, 153 (2009) (Ginsburg, J., dissenting) (arguing that "[t]he exclusionary rule . . . is often the only remedy effective to redress a Fourth Amendment violation"); *see also* Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1388–89 (1983) (discussing the limitations of alternative remedies to the exclusionary rule).

[194] *See supra* note 151.

expansion of authority to conduct physical searches overseas, as discussed below.

Remote searches with no physical intrusion into the country where the data is hosted may still infringe upon the host nation's sovereignty, as discussed in section II.C.,[195] although to a lesser degree than physical searches.[196] For example, some countries consider U.S. digital incursions to obtain data that U.S. ISPs store within their borders as "potential infringements" on their sovereignty,[197] although those same countries may be willing to conduct such incursions themselves.[198] Therefore, even for remote searches, law enforcement must consider the host nation's authority.

When hacking remotely into a suspect's computer, law enforcement must consider the host nation's laws because the U.S. warrant will only authorize the search under U.S. law and will provide no guarantee that the search complies with foreign law. However, law enforcement will not know whether the search potentially implicates a foreign nation's laws until they have already conducted an initial search under the warrant to identify the computer's location.[199] Therefore, if the host nation considers remote searches by foreign law enforcement an invasion of its sovereignty, the searchers will already have

---

[195] *See* United States v. Horton, 863 F.3d 1041, 1047–48 (8th Cir. 2017) (holding that a search by remote access using hacking software took place where the computer was physically located, not at the physical site where law enforcement uploaded the software onto the internet); Brief for Ireland as Amicus Curiae in Support of Neither Party at 1, Microsoft III, 138 S. Ct. 1186 (2018) (No. 17-2), 2017 WL 6492481, at *1 (expressing Ireland's "genuine and legitimate interest in potential infringements by other states of its sovereign rights with respect to its jurisdiction over its sovereign territory" when U.S. law enforcement attempted to compel a U.S. ISP to disclose digital data stored in Ireland, even though any intrusion by U.S authorities or their agents into Ireland would be solely digital instead of physical); *supra* Section III.C.

[196] *See* Microsoft I, 15 F. Supp. 3d 466, 475–76 (S.D.N.Y. 2014) (noting that because digital investigations do not require the "deployment of American law enforcement personnel abroad," they do not raise the same concerns about extraterritorial extension of judicial authority), *rev'd in part*, 829 F.3d 197 (2d Cir. 2016), *vacated as moot*, 138 S. Ct. 1186 (2018).

[197] *See supra* note 149. Ireland preferred using the MLAT process instead of relying solely on a U.S. warrant to compel disclosure. *See id.* at 2.

[198] Ireland noted that under some circumstances, its own highest court accepted the need for an Irish court to order production of records from an Irish entity on foreign soil. *Id.* at 6–7.

[199] For a discussion on the anonymity of the Dark Net, see United States v. Jean, 207 F. Supp. 3d 920, 924–25, 928–29 (W.D. Ark. 2016) (describing how the FBI hacked into a Dark Net user's computer to identify its IP address, which allowed the FBI to identify the user through an administrative subpoena to the internet service provider); United States v. Scanlon, No. 2:16-cr-73, 2017 WL 3974031, at *4 (D. Vt. Apr. 26, 2017) (describing how the FBI could observe users' actions on a Dark Net child pornography website but could not obtain their true identities from the scant information available on the Dark Net and noting that a Dark Net child pornography hub cautioned users not to post information that could be used to identify them); United States v. Taylor, 250 F. Supp. 3d 1215, 1220–22, 1228 (N.D. Ala. 2017).

committed an intrusion.[200] Once law enforcement agents learn that the computer they are searching is located overseas, they should cease further searching and determine whether the host nation requires further approval. At this stage, sharing their investigation with host nation law enforcement agents may provide the best means of ensuring the suspect is prosecuted.[201] Host nation authorities will have greater access to legal mechanisms to investigate the suspect, including gathering physical evidence on site, interviewing witnesses, and arresting the suspect.[202]

Due to the borderless nature of cybercrime, many cyber investigations already involve international cooperation, particularly those over the Dark Net.[203] The Budapest Convention, signed by fifty-five parties, including the United States, facilitates cooperative efforts in combating cybercrime by requiring that members adopt laws to empower law enforcement to compel submission of computer data within their territories.[204] When investigating the Dark Net marketplace Silk Road, for example, U.S. law enforcement worked with sixteen countries operating under Europol's European Cybercrime Centre.[205] Some cooperative investigations initiate when foreign authorities

---

[200] *Cf. supra* note 149 (asserting Ireland's "legitimate interest in potential infringements by other states of its sovereign rights with respect to its jurisdiction over its sovereign territory" when the United States attempted to enforce a warrant to remotely search a U.S. corporation's data center located in Ireland).

[201] *See, e.g.*, Press Release, FBI, International Cooperation Disrupts Multi-Country Cyber Theft Ring (Oct. 1, 2010) (describing cooperation among local and federal U.S. law enforcement and police in the Netherlands, Ukraine, and United Kingdom to investigate cybercrime stealing from online bank accounts using a botnet attack); Press Release, FBI, FBI, International Law Enforcement Disrupt International Organized Cyber Crime Ring Related to Butterfly Botnet (Dec. 11, 2012), https://archives.fbi.gov/archives/news/pressrel/press-releases/fbi-international-law-enforcement-disrupt-international-organized-cyber-crime-ring-related-to-butterfly-botnet (describing FBI cooperation with foreign law enforcement to arrest individuals from Europe, New Zealand, Peru, and the United States in an investigation of cyber theft).

[202] *See* U.N. Office on Drugs & Crime, Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime 20 (2012), http://www.unodc.org/documents/organized-crime/Publications/Confiscation_Manual_Ebook_E.pdf (discussing the importance of international cooperation when seeking evidence located in a foreign country); *id.* at 21 (describing local German authorities collecting evidence from a German company for U.S. prosecution).

[203] *See, e.g.*, AlphaBay, *supra* note 2 (describing an international investigation by the United States, Thailand, Canada, and European police to shut down a Dark Net criminal marketplace).

[204] Council of Europe Convention on Cybercrime art. 18.1(a), Nov. 23, 2001, S. Treaty Doc. No. 11, 2296 U.N.T.S. 167 ("Each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order . . . a person in its territory to submit specified computer data in that person's possession or control . . . ."). However, the Convention on Cybercrime requires consent for cross-border investigations when computer systems are not open source. *Id.* at art. 32.

[205] Office of Pub. Affairs, More than 400 .Onion Addresses, *supra* note 5 (describing an investigation of Dark Net markets trafficking in firearms, drugs, stolen credit card data, counterfeit currency, and fake identity documents). The European Cybercrime Centre facilitates investigation across international boundaries. *European Cybercrime Centre – EC3*, EUROPOL, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last visited August 20, 2018).

inadvertently hack into Dark Net users' computers located in the United States.[206] For countries without cooperation agreements, the increasing prevalence of cyber investigations may compel such agreements.[207]

Where no agreement or host nation laws on cyber-intrusions exist, it may be unclear whether a digital investigation infringes on the host nation's rights unless the host nation objects.[208] However, if the host nation is unwilling to investigate or prosecute the suspect, U.S. authorities may need to request extradition or simply abandon the investigation.[209]

For physical searches conducted overseas, the availability of a U.S. warrant will provide benefits even though U.S. officials still must obtain host nation authorization. The requirement for host nation approval for physical searches restrains the practical effects of the expansion of U.S. courts' authority. Therefore, using a U.S. warrant will not increase the frequency or intrusiveness of physical searches overseas by U.S. officials because they already have to operate under the host nation's constraints and the Fourth Amendment's Reasonableness Clause.[210] However, defendants and law enforcement will gain the benefits of *ex ante* judicial examination of a search's constitutionality.[211] The host nation cannot necessarily be relied upon to provide such benefit because foreign laws may not require an impartial magistrate to determine probable cause prior to a search.[212] Further, U.S. law enforcement conducting a search overseas may reasonably rely on a foreign warrant or a foreign court's

---

[206] Joseph Cox, *Australian Authorities Hacked Computers in the U.S.*, MOTHERBOARD (Aug. 15, 2016, 10:10 AM) https://motherboard.vice.com/en_us/article/mg79nb/australian-authorities-hacked-computers-in-the-us (describing Australian police remotely hacking Dark Net users as part of a child pornography investigation and providing information to the FBI on U.S.-based users uncovered in the investigation).

[207] *See* Brief of the Government of the United Kingdom of Great Britain and Northern Ireland as Amicus Curiae in Support of Neither Party, *supra* note 176, at 7, 11–12 (discussing a proposed treaty between the United States and United Kingdom as an alternative process to improve investigations requiring requests for digital data).

[208] *See* Ghappour, *supra* note 29 (discussing foreign relations risks posed by law enforcement conducting remote searches of computers physically located in another country).

[209] *See Examples of International Investigations – Fiscal Year 2017*, IRS, https://www.irs.gov/compliance/criminal-investigation/examples-of-international-investigations-fiscal-year-2017 (describing extradition of a suspect from Peru for defrauding people out of approximately $65 million) (last updated Apr. 30, 2018).

[210] *See* U.S. CONST. amend. IV ("The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated . . ."); *see* United States v. Odeh, 552 F.3d 157, 171 (2d Cir. 2008) (holding that because the Warrant Clause did not apply overseas, searches of persons protected by the Fourth Amendment were only governed by the Reasonableness Clause).

[211] *See supra* Section III.A.1.

[212] *See, e.g.*, David Tate Cicotte, Saudi Search and Seizure Law Compared with the Fourth Amendment 4 (May 1, 2014) (unpublished law school student scholarship) (on file with Seton Hall University eRepository).

assessment that a warrant is unnecessary, even if the foreign standard does not provide the same protection as the Fourth Amendment.[213]

Therefore, foreign searches under this expansion of courts' jurisdiction will not damage international comity. Such searches will be limited to joint investigations where foreign authorities have approved U.S. law enforcement activities or digital investigations where law enforcement need not physically enter the host nation.

B. Potential Implications for the Fourth Amendment's Territorial Limitations

In addition to affecting parties controlled by statutory warrant requirements, this Comment's proposal may provide an opportunity for expansion of Fourth Amendment protection. Under current law, when a criminal statute extends to a person or conduct located outside the United States, the Fourth Amendment might not extend to the target of the criminal investigation.[214] The proposed mechanism—allowing federal courts to issue search warrants when no other U.S. court has jurisdiction—may allow courts to reexamine the territorial limits of Fourth Amendment protections. A deeper exploration of this subject is better suited for a separate paper, but this Comment will discuss such implications briefly.

In 1990, the Court held in *United States v. Verdugo-Urquidez* that the Fourth Amendment only protects "the people," a class of persons who are part of the national community or who have otherwise developed sufficient connection with the United States to be considered part of that community.[215] *Verdugo-Urquidez* involved U.S. agents' search and seizure of property in Mexico owned by a nonresident alien.[216] Writing for the majority, Justice Rehnquist reasoned

---

[213] *See* United States v. Peterson, 812 F.2d 486, 491–92 (9th Cir. 1987) (upholding a search that U.S. officials conducted in the Philippines under the good faith exception because local police represented that the search complied with Philippine laws); United States v. Stokes, 710 F. Supp. 2d 689, 702–03 (N.D. Ill. 2009) (holding a search conducted by U.S. officials in Thailand as reasonable when Thai officials informed U.S. law enforcement that the search would comply with Thai law because "U.S. law enforcement officers who reasonably rely on a foreign authority's representations of applicable foreign law have not engaged in any culpable police misconduct").

[214] United States v. Verdugo-Urquidez, 494 U.S. 259, 272–75 (1990) (holding that the Fourth Amendment did not extend to a Mexican citizen's property located outside the United States even when he was located within the United States at the time of the search); *see also* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *2–3 (W.D. Wash. May 23, 2001) (holding that the Fourth Amendment did not apply when the FBI hacked into Russian computers remotely because the computers were located outside the United States and belonged to a foreigner with insufficient ties to the U.S. to gain the protection of the Fourth Amendment).

[215] 494 U.S. at 265.

[216] *Id.* at 262.

that the Fourth Amendment's history suggests that the Founders intended to protect the people of the United States against their government by restricting federal searches and seizures domestically.[217] Further, not every constitutional provision applies to governmental activity, even in territories where the United States has sovereign power.[218] Extending Fourth Amendment rights further would carry significant practical consequences, by hindering foreign policy actions such as military activities that might result in searches or seizures,[219] or allowing "aliens with no attachment" to the United States to bring actions for damages for claimed violations of the Fourth Amendment in foreign countries or international waters.[220]

Justice Kennedy, concurring in the opinion, disagreed that the restrictions on the Fourth Amendment's reach arose from the text referring to "the people."[221] Instead, he relied on case law holding that the Court "must interpret constitutional protections in light of the undoubted power of the United States to take actions to assert its legitimate power and authority abroad."[222] He explained that extending the Warrant Clause to protect aliens' foreign property was "impracticable" because of the lack of U.S. judges in those jurisdictions to issue warrants, the differing concepts of reasonableness abroad, and the need to cooperate with foreign officials.[223] In a separate concurrence, Justice Stevens argued that the Warrant Clause had no application to searches of noncitizens' homes in foreign jurisdictions because American magistrates have no power to authorize such searches.[224]

Justice Brennan dissented, arguing that because the U.S. government holds foreigners criminally liable for violation of federal laws on foreign soil, the Fourth Amendment's protections should also cover them.[225] Because the Constitution provides Congress' authority to criminalize conduct, including the "enormous expansion" of federal criminal jurisdiction beyond U.S. territorial

---

217 *Id.* at 266.

218 *Id.* at 268.

219 *Id.* at 273–74. *But see id.* at 292 (Brennan, J., dissenting) (observing that exigency exceptions to the warrant requirement would reduce tension between the Fourth Amendment and the Executive's foreign affairs power).

220 *Id.* at 274 (majority opinion) (discussing the risk of aliens bringing *Bivens* actions against federal agents) (citing Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) (holding that a plaintiff injured by government agents' violation of the Fourth Amendment may sue for damages in federal court)).

221 *Id.* at 275–76 (Kennedy, J., concurring).

222 *Id.* at 277.

223 *Id.* at 278.

224 *Id.* at 279 (Stevens, J., concurring); *see also id.* (Brennan, J., dissenting).

225 *Id.* at 279–81 (Brennan, J., dissenting).

limitations, the Constitution also limits the government's authority to investigate such conduct.[226] He also noted that doctrinal exceptions to the Warrant Clause, such as exigent circumstances, would frequently apply abroad, lessening potential tension between foreign policy goals and constitutional constraints by reducing requirements to the reasonableness standard.[227] Further, the constitutionality of the Executive Branch's actions abroad would only be challenged in court when the Executive Branch brought a criminal prosecution introducing evidence seized abroad—meaning that most foreign policy actions would not be implicated.[228]

After *Verdugo-Urquidez*, the protections of the Fourth Amendment hinge on two factors: the location of the search and the target's identity.[229] For searches and seizures occurring inside the United States, the Fourth Amendment applies.[230] For searches and seizures taking place outside the United States, aliens without sufficient connection to the United States enjoy no Fourth Amendment protections.[231] For searches that occur in other nations, U.S. citizens and aliens with sufficient connection to the United States to count among "the people" protected by the Fourth Amendment receive the protection of the Reasonableness Clause but not the Warrant Clause, because of the difficulties discussed above with obtaining a warrant for property located overseas.[232]

This Comment's proposal addresses Justice Kennedy's and Justice Stevens's concerns about the unavailability of warrants for overseas searches. If Congress adopts the proposed exception and warrants become available for overseas searches, the Court could reconsider limitations of Fourth Amendment protections to "the people."

---

226 *Id.*

227 *Id.* at 292.

228 *Id.* at 293. The exclusionary rule remains the primary remedy for Fourth Amendment violations. *See* Mapp v. Ohio, 367 U.S. 643, 652–53 (1961) (noting "[t]he obvious futility" of relying on remedies other than the exclusionary rule). Although individuals may bring private actions against the police for invasion of civil rights, many Fourth Amendment violations do not satisfy the requirements for such claims. *See* Herring v. United States, 555 U.S. 135, 153 (2009) (Ginsburg, J., dissenting) (arguing that "[t]he exclusionary rule . . . is often the only remedy effective to redress a Fourth Amendment violation"); Stewart, *supra* note 193.

229 *See* 494 U.S. at 274–75 (holding that the Fourth Amendment did not extend to a search that took place outside the United States because the subject lacked sufficient connection to the United States).

230 *Id.* at 266.

231 *Id.*

232 *See* United States v. Odeh, 552 F.3d 157 (2d Cir. 2008).

CONCLUSION

Criminals now carry out a staggering volume of illegal activity online, ranging from drug trafficking to child pornography, simply by masking their identities. Law enforcement can watch criminals buy and sell illicit narcotics, child pornography, and stolen credit card numbers in Dark Net marketplaces but are powerless to stop them.

This Comment proposes a solution that will allow law enforcement to use the warrants available for traditional searches in remote access searches of anonymous criminals over the Internet. When no other district is known to have jurisdiction, a federal judge should have the authority to issue warrants for search or seizure of property based on whether the alleged crime could be prosecuted in the judge's district. This solution will require amending Rule 41 to provide a clearer procedural mechanism and statutory authority for issuing such warrants. This change will resolve the jurisdictional conundrum that courts face when issuing warrants to search computers of Internet users who have concealed their locations and identities. Further, this change will facilitate the rights of defendants and the authority of law enforcement by affording a mechanism for warrants overseas, furthering the constitutional preference for warrants.

Finally, this change opens the possibility for extending the protections of the Fourth Amendment's Warrant Clause into foreign territory. The 2016 amendment to Rule 41, which provides for remote access warrants, has already built a foundation for extending warrant authority overseas. The broader implications for the Fourth Amendment's territorial scope would provide a worthwhile topic for future scholarly research. However, until statutes and procedural rules bridge the current disconnect between territorial constraints on jurisdiction and the reality of modern cybercrime, criminals will continue to operate with impunity on the Dark Net.

DIANA BENTON*

* Notes & Comments Editor, *Emory Law Journal*, Volume 68; Emory University School of Law, J.D., 2019; Stanford University, B.A., 2007. I extend gratitude and appreciation to my faculty advisor, Associate Dean Kay Levine, for her excellent advice. To my colleagues at Emory Law, I would like to thank you for creating a wonderful environment for pursuing a legal education.