NOTES

LAW ENFORCEMENT HACKING: DEFINING JURISDICTION

*Rachel Bercovitz**

Federal law enforcement's deployment of malware (Network Investigative Technique, or NIT) raises a jurisdictional question central to remote searches of electronic data: Where does the search occur?

Litigation arising from two prominent NIT searches—Operations Pacifier and Torpedo—illustrates the challenge courts confronted in defining the situs of a NIT search absent a clear territorial referent. The defined situs deserves attention, for it determines the territorial reach of law enforcement's legal authority to conduct operations—warrant jurisdiction—and the Fourth Amendment's applicability to nonresident aliens.

Recent circuit court opinions have raised the prospect that courts may deem invalid the 2016 amendment to Federal Rule of Criminal Procedure 41(b), which authorizes searches of the sort at issue in Operations Pacifier and Torpedo. Should this occur, the situs of a NIT search would again turn on jurisdiction-specific definitions. As this Note suggests, courts that define the situs as within the United States may enable nonresident alien search targets to claim the Fourth Amendment's protections. Litigants could draw from lower court precedent recognizing nonresident aliens' Fifth and Sixth Amendment rights when the alleged violation is said to occur domestically. Their ability to pursue constitutional remedies, however, would remain contingent on the reviewing court's jurisdictional definition, not on normatively consistent constitutional rationales.

This Note proposes that Congress standardize the situs of a NIT search by drawing from the amended Rule 41(b) and from circuit courts' interpretation of the situs of a wiretap under the federal Wiretap Act. This proposed definition would codify the amended Rule 41(b) and may guide (though it would not preempt) a court's analysis of a nonresident alien's Fourth Amendment claim. This Note concludes by urging a doctrinal shift toward extending the Fourth Amendment's protections to nonresident alien NIT search targets.

---

* J.D. Candidate 2021, Columbia Law School. The author would like to thank Professors Daniel Richman and Christina D. Ponsa-Kraus for their steadfast guidance and insight. The author also thanks the editors of the *Columbia Law Review* for their thoughtful and tireless editorial assistance.

INTRODUCTION

During oral argument in *United States v. Microsoft*, Justice Alito set forth a puzzle: how to define the situs of a search and seizure of electronic data.[1] *Microsoft* addressed whether a statutory warrant directing Microsoft to disclose customer data stored in Microsoft's data center in Dublin, Ireland, but accessible to Microsoft employees at Microsoft's headquarters in Redmond, Washington, entailed an extraterritorial search.[2] Though the

1. Transcript of Oral Argument at 52–53, United States v. Microsoft Corp., 138 S. Ct. 1186, 1187 (2018) (per curiam) (No. 17-2), 2018 WL 1383162.

2. See *Microsoft*, 138 S. Ct. at 1187.

stored information "physically exists on one or more computers somewhere," Alito began, "it doesn't have a presence anyplace . . . . The whole idea of territoriality is strained."[3]

This challenge—defining legal jurisdiction absent a clear territorial referent—is not new. During the late 1990s and early 2000s in particular, scholars considered how online communications and transactions challenged the traditional territorial link between "legally significant (online) phenomena and physical location," between conduct and effect.[4] Courts, in turn, confronted one practical application of this jurisdictional puzzle: how to define the situs of an "intercept" of communications within the meaning of the Wiretap Act when law enforcement is physically separated from the tapped device.[5] More recently, in *Microsoft*, Alito confronted the question in the context of Stored Communications Act (SCA) compelled disclosure orders, which direct third-party service providers to disclose stored customer data to law enforcement under specified conditions.[6]

With the rise of encryption technology and anonymizing software, however, this question has regained salience, particularly with regard to the government's use of malware to directly search a suspect's device or data.[7] Through tactics the government terms Network Investigative Techniques (NITs), law enforcement is able to circumvent encryption technology and anonymizing software that impede traditional investigative

---

3. Transcript of Oral Argument at 52–53, *Microsoft*, 138 S. Ct. 1186 (No. 17-2).

4. David R. Johnson & David Post, Law and Borders—The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367, 1370, 1378 (1996) (arguing that "[m]any of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct 'place' for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the 'real world'"); see also Patricia L. Bellia, Chasing Bits Across Borders, 2001 U. Chi. Legal F. 35, 44 (examining the treatment of remote cross-border searches under the Constitution and customary international law and arguing that any bilateral or multilateral agreement authorizing cross-border searches "must track Fourth Amendment requirements"); Paul Schiff Berman, Legal Jurisdiction and the Deterritorialization of Data, 71 Vand. L. Rev. En Banc 11, 13–15 (2018) [hereinafter Berman, Legal Jurisdiction] (reviewing this early scholarship on internet jurisdiction and territorial sovereignty); Jack L. Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignty, 5 Ind. J. Glob. Legal Stud. 475, 475 (1998) (arguing that "territorial regulation of the Internet is no less feasible and no less legitimate than territorial regulation of non-Internet transactions").

5. See, e.g., United States v. Rodriguez, 968 F.2d 130, 135–36 (2d Cir. 1992) (defining "intercept" within the meaning of Section 2518(3) of the Wiretap Act as both where "the contents of a wire communication are captured or redirected" and where "the redirected contents are first heard").

6. See *Microsoft*, 138 S. Ct. at 1187; Paul M. Schwartz, Legal Access to the Global Cloud, 118 Colum. L. Rev. 1681, 1714 (2018).

7. See Jonathan Mayer, Government Hacking, 127 Yale L.J. 570, 576–78 (2018). This Note focuses exclusively on federal law enforcement's use of malware-enabled searches, as the factual and legal records of these searches are substantially more developed at the federal level. See id. at 578, 580 n.29.

tools.[8] When a NIT search targets a device or data concealed by anonymizing software, however, officers do not know prior to the search where it will execute. The question, in turn, becomes: Where does this NIT search occur?

Prior to the 2016 amendment to the venue provisions of Federal Rule of Criminal Procedure 41(b), which regulate federal magistrate judges' authority to issue search warrants, the government defined the search by the location of the relevant government server and investigating officer.[9] In turn, courts presiding over challenges to two prominent NIT searches—Operations Pacifier and Torpedo—embraced divergent interpretations. Though numerous courts adopted a device-centric approach, defining the situs of the search by the location of the suspect's device,[10] others embraced the government's definition, analogizing the search to a tracking device authorized by Rule 41(b)(4).[11] Crucially, a device-centric definition laid the groundwork for courts to hold NIT searches that executed beyond the judicial district of the authorizing magistrate judge invalid under the unamended Rule 41(b) and the Federal Magistrates Act.

The amended Rule 41(b)(6)(A) departed from these single-factor approaches. Subsection (b)(6)(A) provides that "a magistrate judge with authority in any district where activities related to a crime may have occurred" may issue a remote search warrant when "the district where the media or information is located has been concealed through technological means."[12] In NIT searches executed since this Rule change, the government and courts have defined the "place to be searched" by the traditional Fourth Amendment framework—the location of the thing searched.[13]

---

8. The government has modified the terminology over time. What began as "a workbench project" evolved into the "computer and internet protocol address verifier" (CIPAV) before the 2012 adoption of what is believed to be the currently used term—NITs. See Zach Lerner, A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, 18 Yale J.L. & Tech. 26, 38 (2016).

9. See, e.g., Brief of the United States at 21, United States v. Darby, 721 F. App'x 304 (4th Cir. 2018) (No. 17-4212), 2017 WL 6015454 ("Under Rule 41's tracking-device provision, the NIT was installed when it was placed on the Playpen server in the Eastern District of Virginia, not when the NIT was retrieved from the Playpen server by a user logging onto Playpen or when the NIT ultimately disclosed the location-identifying information.").

10. See infra note 70.

11. See infra note 71.

12. Fed. R. Crim. P. 41(b)(6)(A). Subsection (b)(6)(A) provides:

> (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:
>
> > (A) the district where the media or information is located has been concealed through technological means . . . .

13. See infra note 48 and accompanying text.

This definition deserves attention, for the situs of the search is not merely technical. The definition determines the territorial reach of law enforcement's legal authority to conduct operations—warrant jurisdiction—and the applicability of the Fourth Amendment's protections.[14] In turn, the definition may determine the legality of the search and the Fourth Amendment rights of nonresident aliens[15] subject to a NIT search.[16]

First, if the amended Rule 41(b)(6)(A) is found invalid in light of the Federal Magistrates Act—a prospect the Second and Ninth Circuits have raised—magistrate judges would remain constrained by the Act's "independent territorial restrictions" on their authority to issue extra-district NIT searches.[17] In turn, courts would again confront the problem that arose under the unamended Rule 41(b): defining the situs of a NIT search that executes beyond the judicial district of the authorizing magistrate judge.

---

14. See Jennifer Daskal, The Un-Territoriality of Data, 125 Yale L.J. 326, 389 (2015) [hereinafter Daskal, The Un-Territoriality of Data] ("Whereas territoriality under the Fourth Amendment demarcates who is—and is not—entitled to basic privacy protections vis-à-vis the U.S. government, territoriality for purposes of warrant jurisdiction defines the geographic scope of court-approved law enforcement authority to act.").

15. A note on terminology: In this Note, "nonresident alien" refers to foreign nationals investigated by U.S. law enforcement for conduct that might be defined as occurring abroad.

Jurists and scholars have long employed the term "nonresident alien" when discussing whether or to what extent provisions of the Constitution apply to noncitizens located abroad. As scholars such as Kevin R. Johnson have noted, however, use of the term "alien" concretizes a notion of noncitizens as "'other,' different and apart from 'us.'" Kevin R. Johnson, "Aliens" and the U.S. Immigration Laws: The Social and Legal Construction of Nonpersons, 28 U. Miami Inter-Am. L. Rev. 263, 264 (1996). Indeed, President Biden's proposed immigration reform bill, the U.S. Citizenship Act of 2021, calls for "further recogniz[ing] America as a nation of immigrants" by replacing the term "alien" with "noncitizen" in U.S. immigration law. Fact Sheet: President Biden Sends Immigration Bill to Congress as Part of His Commitment to Modernize Our Immigration System, White House (Jan. 20, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/01/20/fact-sheet-president-biden-sends-immigration-bill-to-congress-as-part-of-his-commitment-to-modernize-our-immigration-system [https://perma.cc/EK2S-CVRY].

16. See Jennifer Daskal, Borders and Bits, 71 Vand. L. Rev. 179, 185–86 (2018) [hereinafter Daskal, Borders and Bits] ("[T]he answers to these jurisdictional questions often determine not just government's ability to access or manage data, but the rights and protections that apply. In determining who gets to set the rules, the jurisdictional rules indirectly determine the scope of one's privacy, associational, and speech rights."); Daskal, The Un-Territoriality of Data, supra note 14, at 354–55, 383–86 (explaining that the territorial limits on a federal judge's authority to issue a search warrant depend on where the search is deemed to have occurred and arguing for the presumptive application of the Fourth Amendment "regardless of where the data or the target is located").

17. United States v. Eldred, 933 F.3d 110, 117 (2d Cir. 2019) (internal quotation marks omitted) (quoting United States v. Krueger, 809 F.3d 1109, 1121 (10th Cir. 2015) (Gorsuch, J., concurring)); see also United States v. Henderson, 906 F.3d 1109, 1115 n.5 (9th Cir. 2018); infra section II.A.

Law enforcement may avoid this warrant jurisdiction problem by submitting NIT warrant applications to *district* court judges, who are not subject to the Magistrates Act's territorial constraints.[18] But the jurisdictional question would remain relevant for nonresident alien search targets.[19]

Courts that define the situs by the location of the government server or investigating officer—*within* the authorizing magistrate judge's judicial district—may pave the way for nonresident aliens subject to NIT searches to challenge the search on Fourth Amendment grounds. Though Supreme Court doctrines generally foreclose Fourth Amendment challenges brought by foreign nationals for searches of their property abroad,[20] a nonresident alien might assert such a challenge by characterizing the NIT search as domestic, not extraterritorial, in nature.[21] A nonresident alien's ability to pursue remedies for Fourth Amendment violations, however, would remain contingent on the fortuity of the court's jurisdictional definition.

To address this incongruity, this Note proposes that lawmakers define the situs of a NIT search as part of a comprehensive bill regulating these remote searches.[22] The proposed definition should relate to the locations of the targeted device or data and the investigating officer. A definition tied to the location of the device or data searched would recognize but regulate law enforcement's execution of remote searches. In turn, a definition tied to the investigating officer may pave the way for nonresident aliens to assert Fourth Amendment challenges to unlawful NIT searches.

Part I of this Note introduces NIT searches and examines how judges have defined the situs of these searches prior to and following the amendment to Rule 41(b). Part II discusses circuit court opinions raising the prospect that the amended Rule 41(b)(6)(A) may be vulnerable to judicial

---

18. See Mayer, supra note 7, at 628.

19. For NIT searches that execute domestically, the defined situs of the search generally does not have a constitutional dimension. See 2 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 4.2(f) (6th ed. 2020) (noting that "contrary to the usual rule . . . the violation of a rule or statute may show that the Fourth Amendment requirement that warrants be issued by a 'neutral and detached magistrate' who is 'lawfully vested' with warrant-issuing authority has not been met"). Though the Fourth Amendment sets forth probable cause and warrant requirements, statutes and rules define the territorial scope of the authorizing judge's authority to issue search warrants. See id.

By contrast, in searches that may be said to execute extraterritorially, the situs may enable or foreclose Fourth Amendment claims by nonresident aliens depending on whether the situs of the search is found to be located within or beyond the United States. See infra section II.B.2. Further, as to U.S. citizens, the situs may determine whether the Fourth Amendment's traditional probable cause and warrant requirements, or its reasonableness test, applies. See infra note 118.

20. See infra section II.B.1.

21. See infra section II.B.2.

22. See infra Part III.

attack. This Part then suggests that defining the situs as within the magistrate judge's judicial district may enable nonresident aliens to assert Fourth Amendment challenges arising from unlawful NIT searches. As the pursuit of constitutional remedies would remain contingent on the presiding court's definition, Part III proposes that Congress define the situs of a NIT search by drawing from Rule 41(b) and the federal Wiretap Act.

I. THE JURISDICTIONAL PUZZLE

Data's abstract and intangible nature has long challenged efforts to define the situs of a data search. The chosen referent—the site of the device searched or the officer executing the search, for example—determines law enforcement's authority to execute the search (warrant jurisdiction) and the Fourth Amendment's applicability. Recent scholarship addressing the jurisdictional question in the context of compelled disclosure orders and NIT searches[23] has largely focused on warrant jurisdiction: the territorial reach of Stored Communications Act warrants,[24] and the geographic scope of a magistrate judge's authority to approve NIT searches that may be said to execute beyond the authorizing judge's judicial district.[25] Yet scholars have largely shifted attention from these

23. See, e.g., Berman, Legal Jurisdiction, supra note 4, at 20–21 (suggesting that prior scholarship on internet jurisdiction informs the contemporary jurisdictional question raised by electronic data, and advancing a "cosmopolitan pluralist conception of jurisdiction" that aims to "capture a middle ground between strict territorialism on the one hand and a system of complete universal jurisdiction on the other"); Zachary D. Clopton, Response, Data Institutionalism: A Reply to Andrew Woods, 69 Stan. L. Rev. Online 9, 9 (2016) (suggesting that though Woods's thesis against data exceptionalism "has much going for it, . . . it does not provide crisp answers to many of the challenging problems of transnational jurisdiction and conflict of laws"); Daskal, The Un-Territoriality of Data, supra note 14, at 390 ("The *Microsoft* case . . . pits the location of data against the location of access, requiring an answer as to which controls, at least for purposes of warrant jurisdiction under the SCA."); Shelli Gimelstein, A Location-Based Test for Jurisdiction Over Data: The Consequences for Global Online Privacy, 2018 U. Ill. J.L. Tech. & Pol'y 1, 4 (arguing that the Second Circuit's decision in *Microsoft* "illustrates the problem in relying on data location as a basis for determining where SCA search warrants can lawfully be executed"); Schwartz, supra note 6, at 1690 (arguing that "the legal significance of where cloud data is accessed versus where it is located—the source of much scholarly debate—cannot be answered without reference to specific cloud models"); Andrew Keane Woods, Against Data Exceptionalism, 68 Stan. L. Rev. 729, 734 (2016) (suggesting that, contrary to proponents of the "data exceptionalism" thesis, data stored in the cloud is not "fundamentally incompatible with existing territorial limits on jurisdiction").

24. See 18 U.S.C. § 2703 (2018); Schwartz, supra note 6, at 1714 (detailing the SCA's core provisions).

25. See, e.g., Mayer, supra note 7, at 625–26 (noting that Federal Rule of Criminal Procedure 41(b)(6) addressed the question of which court has authority to issue a search warrant when the target device's location has been concealed); Diana Benton, Comment, Seeking Warrants for Unknown Locations: The Mismatch Between Digital Pegs and Territorial Holes, 68 Emory L.J. 183, 192 (2018) ("Applying the Fourth Amendment to anonymous computer users at unknown locales creates a dilemma for judges who must first

questions following two developments. First, the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act[26]—an amendment to the SCA—resolved the immediate challenge presented in *Microsoft* by requiring service providers to disclose customer data without regard to whether it is "located within or outside of the United States."[27] Second, the 2016 amendment to Federal Rule of Criminal Procedure 41(b) appeared to resolve the jurisdictional challenge raised in two high-profile NIT searches—Operations Pacifier and Torpedo—by authorizing magistrate judges to issue warrants for extra-district NIT searches under certain circumstances.[28]

The significance of defining jurisdiction, however, remains. If courts find the amended Rule 41(b)(6)(A) insufficient to authorize extra-district NIT searches, magistrate judges would continue to lack authority under the Magistrates Act to issue warrants for searches executed beyond their judicial districts.[29] Even if Rule 41(b)(6)(A) is found to properly accord this authority, courts will be pressed to define the situs of searches that do not fall within this subsection.

Government training materials, including those disclosed pursuant to Freedom of Information Act (FOIA) litigation,[30] and NIT searches executed in routine investigations since the Rule 41(b) amendment,[31] have made clear law enforcement's continued use of malware searches in a range of investigations.[32] The prevalence and persistence of this investigative tool call for considered reflection on how courts define the situs of NIT searches.

This Part proceeds in three sections. Section I.A introduces law enforcement's use of NIT searches to circumvent anonymizing software and encryption technology, and sets forth why remote data searches

---

ascertain their jurisdiction over the unknown location where the warrant will be executed.").

26. Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018) (codified in scattered sections of 18 U.S.C.). The CLOUD Act requires U.S. based service providers to "preserve, backup, or disclose" electronic communications content relating to a customer or subscriber that are within the provider's "possession, custody, or control," even if the data is stored on a server located abroad. 18 U.S.C. § 2713. In so doing, the Act conditions regulatory jurisdiction on the location of the service provider, rather than of the stored data. See Jennifer Daskal, Privacy and Security Across Borders, 128 Yale L.J. Forum 1029, 1035–36 (2019).

27. 18 U.S.C. § 2713.

28. See infra section I.B.1; see also Daskal, Borders and Bits, supra note 16, at 205 (discussing the Rule change).

29. See infra section II.A.

30. See U.S. Hacking FOIA, Priv. Int'l, https://privacyinternational.org/taxonomy/term/571 [https://perma.cc/2F4J-3X3X] (last visited Jan. 31, 2021) (collecting materials disclosed by the Justice Department, the FBI, and other federal agencies pursuant to FOIA litigation).

31. See infra section I.C.

32. See Mayer, supra note 7, at 578 fig.1 (charting the increase in federal judicial opinions concerning government-deployed malware from 2001 to 2017).

challenge the traditional Fourth Amendment approach to defining the situs of a search. Sections I.B and I.C pivot to NIT searches. Section I.B examines how the government and courts defined the situs of NIT searches in litigation stemming from two child-exploitation investigations, Operations Pacifier and Torpedo, while section I.C discusses how this definition has evolved under the amended Rule 41(b)(6)(A).

A. *Introducing Terms*

1. *NITs: Law Enforcement Responds to the "Going Dark" Problem.* — Federal law enforcement has traditionally followed one of two routes to search data: (1) compel a service provider to disclose stored customer data, or (2) conduct a direct search by seizing the device and directly searching data stored in the device's memory.[33] Advancements in anonymizing software and encryption technology, however, have challenged law enforcement's ability to execute direct data searches, introducing a gap between officers' lawful authority to access digital evidence and their technical capacity to do so—the so-called "going dark" problem.[34] Anonymizing software and encryption technology pose distinct challenges. Software such as Tor and I2P[35] conceal a suspect's identifying information, such as

---

33. Id. at 590. This Note concerns law enforcement's access to "data at rest," or stored content, including data stored on devices (such as cell phones) and in the cloud. See Kristin Finklea, Cong. Rsch. Serv., R44481, Encryption and the "Going Dark" Debate 5–6 (2016), https://fas.org/sgp/crs/misc/R44481.pdf [https://perma.cc/HJ8M-Q3LR]. It does not concern law enforcement's interception of "data in motion," or real-time communication between a user and a web server (such as for online shopping) or between users (for example, over iMessage or Telegram). See id.; Richard M. Thompson II & Chris Jaikaran, Cong. Rsch. Serv., R44407, Encryption: Selected Legal Issues 2–3 (2016), https://fas.org/sgp/crs/misc/R44407.pdf [https://perma.cc/T98P-CS9N].

34. See Kristin Finklea, Cong. Rsch. Serv., R44827, Law Enforcement Using and Disclosing Technology Vulnerabilities 10 (2017), https://fas.org/sgp/crs/misc/R44827.pdf [https://perma.cc/6T9W-HT2H] [hereinafter Finklea, Using and Disclosing Vulnerabilities]; Alan Z. Rozenshtein, Surveillance Intermediaries, 70 Stan. L. Rev. 99, 111 & n.53 (2018) (noting the debate over whether "technological changes like widespread encryption have resulted in law enforcement 'going dark,' or whether the digitization of everyday life has instead led to a 'golden age of surveillance'").

35. Tor, short for The Onion Router, enables users to engage on the internet anonymously. See Kristin Finklea, Cong. Rsch. Serv., R44101, Dark Web 3–4 (2017), https://fas.org/sgp/crs/misc/R44101.pdf [https://perma.cc/MT9F-P957]. "Tor" describes both the software that users install on their devices to operate anonymously, id., and the collection of "volunteer-operated servers" that support the Tor network. Tor: Overview, Tor, https://2019.www.torproject.org/about/overview.html.en [https://perma.cc/4GV2-ACZ7] (last visited Jan. 19, 2021). Tor conceals a user's IP address by routing web traffic through a series of relays, or nodes, run by these servers. Information is encrypted between relays and takes on the IP address of the final "exit" relay. I2P, or the Invisible Internet Project, is another popular anonymous network. See Finklea, supra; Tor, supra.

Though Tor and I2P are often associated with marketplaces of contraband, illicit services, or child pornography that depend on anonymity, these anonymizing services also—importantly—enable users such as journalists, whistleblowers, dissidents, and others to operate anonymously, and users to access government-censored content. See Tor, supra.

the Internet Protocol (IP) address of their device, which law enforcement traditionally uses to identify and locate a suspect.[36] In turn, encryption technology impedes law enforcement's access to the contents of stored data.[37] When both tools are in use, law enforcement cannot use traditional search techniques to either identify the suspect (due to anonymizing software) or access the relevant evidence (due to encryption technology).

The government has in part responded to the "going dark" problem by leveraging vulnerabilities in software, hardware, or firmware to deploy malware onto a suspect's device—in other words, hacking. NITs enable law enforcement to bypass the anonymizing software or encryption technology impeding officers' ability to execute a traditional search.

Law enforcement has deployed NITs to investigate conduct ranging from loansharking to extortion to child pornography.[38] Agents employ two principal methods to deliver NITs: (1) "social-engineering," or phishing, attacks that target particular individuals, and (2) "watering-hole" attacks that reach *any* individual interacting in a specified manner with a particular "dark-web" site.[39] In a phishing attack, law enforcement sends the target an electronic communication containing an attachment or link embedded with a NIT; when the target takes the necessary step (generally, opening the attachment or link), the NIT deploys to "install software and collect identifying information."[40] In a watering-hole attack, agents seize

---

36. See Susan Hennessey, Hoover Inst., The Elephant in the Room: Addressing Child Exploitation and Going Dark 8 (2017), https://www.hoover.org/sites/default/files/research/docs/hennessey_webreadypdf.pdf [https://perma.cc/998X-LBKA]. "An IP address identifies a device communicating with a network . . . . When an IP is identified, law enforcement can discover the physical location of a computer accessing a particular website at a particular time." Id.

37. Id. at 7–8 (discussing challenges encryption technology poses for law enforcement investigations of child sexual abuse offenders).

38. Mayer, supra note 7, at 578.

39. Lerner, supra note 8, at 40–42. The term "watering hole" alludes to animal predators that hover near watering holes for an opportunity to catch prey. See ACLU, Elec. Frontier Found. & Nat'l Ass'n of Crim. Def. Laws., Challenging Government Hacking in Criminal Cases 1, 37 (2017), https://www.aclu.org/sites/default/files/field_document/malware_guide_3-30-17-v2.pdf [https://perma.cc/Q76U-K35M]; Eyal Aharoni, What Is a Watering Hole Attack and How to Prevent Them, Cymulate: Blog (Jan. 2, 2019), https://blog.cymulate.com/watering-hole-attack-dont-drink-water [https://perma.cc/BP7G-JEFG] (last updated Feb. 21, 2021).

The "dark web" refers to the thousands of websites that use anonymizing software, such as Tor or I2P, to conceal their IP addresses. See Andy Greenberg, Hacker Lexicon: What Is the Dark Web?, WIRED (Nov. 19, 2014), https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web [https://perma.cc/R5JV-F7GR].

40. Lerner, supra note 8, at 40–41. An agent might act undercover, maintaining communication with the suspect throughout the social-engineering attack. Or an agent may pose as a third party to induce the suspect to click a link or open an attachment. Id. In one high-profile example of the latter method, the FBI impersonated the Associated Press (AP) by sending a NIT-embedded fake AP article to a suspect believed to have made a bomb threat against a Seattle high school. When the suspect clicked the link, the NIT exploited a vulnerability in the suspect's web browser to deploy malware, which identified the suspect's

and install a NIT onto a server hosting a given dark-web site. Agents continue to operate the server with the embedded NIT, which deploys onto the device of each user visiting the compromised website.[41] The FBI has deployed watering-hole attacks to investigate visitors of dark-web sites selling illicit services or contraband, most notably in Operations Pacifier and Torpedo.[42]

While the SCA regulates compelled disclosure orders,[43] there is no analogous statute for NIT searches—the Fourth Amendment is the only backstop.[44] Yet courts that have considered the question have not uni-

---

IP address. See id.; Ellen Nakashima & Paul Farhi, FBI Lured Suspect with Fake Web Page, but May Have Leveraged Media Credibility, Wash. Post (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/fbi-lured-suspect-with-fake-web-page-but-may-have-leveraged-media-credibility/2014/10/28/e6a9ac94-5ed0-11e4-91f7-5d89b5e8c251_story.html (on file with the *Columbia Law Review*).

41. See Lerner, supra note 8, at 40–41; Mayer, supra note 7, at 584–85.

42. See Finklea, Using and Disclosing Vulnerabilities, supra note 34, at 3–6 (discussing law enforcement's investigations of child pornography websites through Operation Pacifier, Operation Torpedo, and the seizure of Freedom Hosting, and law enforcement's investigation of illicit marketplaces through Operation Onymous, including one of the most prominent such marketplaces, Silk Road 2).

43. See Richard M. Thompson II & Jared P. Cole, Cong. Rsch. Serv., R44036, Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA) 2–7 (2015), https://fas.org/sgp/crs/misc/R44036.pdf [https://perma.cc/RH87-PSQN] (outlining the SCA's principal provisions). The SCA is one of three main titles comprising the 1986 Electronic Communications Privacy Act (ECPA). The SCA, or ECPA Title II, sets forth different forms of compulsory process based in part on the type of information stored (content or non-content information, or metadata) and the duration of storage. Title I of ECPA amended the Wiretap Act, or Title III of the Omnibus Crime Control and Safe Streets Act of 1968, to regulate electronic communications in addition to oral and wire communications. See id. at 3.

To access the contents of communication stored for 180 or fewer days, the government must obtain a warrant supported by probable cause. 18 U.S.C. § 2703(a) (2018); Stephen P. Mulligan, Cong. Rsch. Serv., R45173, Cross-Border Data Sharing Under the CLOUD Act 5–6 (2018), https://fas.org/sgp/crs/misc/R45173.pdf [https://perma.cc/B7FB-MH6B]. If the content data has been in storage for more than 180 days, the government may either obtain a court order under Section 2703(d), which issues pursuant to a lesser burden of proof, or secure an administrative subpoena. See 18 U.S.C. § 2703(b)(1)(B); Mulligan, supra, at 5–6.

44. Congress enacted the SCA to fill gaps exposed by Supreme Court doctrines limiting Fourth Amendment protection of searches of electronic data stored by third-party service providers. See Alan Z. Rozenshtein, Fourth Amendment Reasonableness After *Carpenter*, 128 Yale L.J. Forum 943, 944 (2019) ("[A]lthough the SCA is often framed as a grant of power to law enforcement, its main impetus was the opposite: Congress was chiefly concerned about digital privacy, and thus went to great lengths to specify workable, privacy-protecting rules governing law enforcement's ability to access certain categories of digital information."). The Court's so-called third-party doctrine provides that an individual does not have a "legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743–44 (1979). In turn, law enforcement's access to data that users have voluntarily shared with third-party service providers has traditionally not been a search under the Fourth Amendment. See Rozenshtein, supra, at 944 & n.7. But see Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (holding the

formly found that a NIT deployed to collect a device's IP address implicates the Fourth Amendment,[45] meaning this common form of NIT search may presently evade judicial review.[46]

In searches found to implicate the Fourth Amendment, law enforcement must generally obtain from a neutral magistrate judge a warrant supported by probable cause to believe that officers will "find evidence of crime in the place being searched."[47] This warrant requirement, however, raises a threshold jurisdictional question: Which magistrate judge has authority to issue the warrant? In other words, in which judicial district is the NIT search said to occur?

2. *Location Independence and the Fourth Amendment.* — According to traditional Fourth Amendment doctrine, the search or seizure occurs at the site of the person or thing searched or seized.[48] Yet in NIT searches, the law enforcement officer conducting the search is physically removed from the targeted device or data. As scholar Jennifer Daskal has described it, there is "location independence" between the government officer and the search target.[49]

Courts have occasionally confronted this problem of defining jurisdiction notwithstanding location independence in the context of tangible searches and seizures—most prominently, in cross-border shootings and drone strikes.[50] Nearly all courts have drawn from the traditional Fourth

---

government's acquisition of Timothy Carpenter's cell-site location information from a third party was a search within the meaning of the Fourth Amendment).

45. To determine whether a Fourth Amendment search or seizure has occurred, courts apply either the *Katz* reasonableness test or the common-law trespassory test. Under *Katz*'s two-part inquiry—drawn from Justice Harlan's *Katz* concurrence—courts inquire, first, whether an individual has "exhibited an actual (subjective) expectation of privacy," and second, whether this subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); see also *Carpenter*, 138 S. Ct. at 2213 (outlining the reasonableness and physical trespass tests).

46. See Mayer, supra note 7, at 582, 661–62. As of 2017, the government maintained that the Fourth Amendment does not regulate NIT searches for which "no content is being searched nor . . . any computer code executed locally on that machine." Affidavit in Support of an Application for a Search Warrant at 24–25 ¶59, In re Search of: The Use of a Network Investigative Technique for a Computer Accessing Email Accounts: weknow@hotdak.net, iama.skank@yandex.com, and weknow@mail2actor.com, No. 6:17-mj-00519 (W.D.N.Y. filed Jan. 31, 2017) [hereinafter W.D.N.Y. Search Warrant].

47. Ronald Jay Allen, William J. Stuntz, Joseph L. Hoffmann, Debra A. Livingston, Andrew D. Leipold & Tracey L. Meares, Comprehensive Criminal Procedure 417, 443 (4th ed. 2016).

48. See, e.g., Daskal, The Un-Territoriality of Data, supra note 14, at 343 (noting that in the Supreme Court's extraterritorial Fourth Amendment case United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), "[w]hat mattered was the location of the *property* being searched, not the location of the property's owner or the agent performing the search").

49. Id. at 369–70.

50. Id. at 369–71.

Amendment framework, defining the situs in cross-border shootings[51] and drone strikes[52] by the location of the person seized, rather than of the law enforcement officer executing the seizure.

Though infrequent in searches of tangible persons or things, location independence is increasingly a touchstone of data searches. *Microsoft*, for example, presented location independence between the customer data stored in Dublin, Ireland, and Microsoft's headquarters in Redmond, Washington.[53] In *Microsoft*, the Second Circuit defined the situs of the seizure by the location of the stored data in Dublin,[54] not, as the magistrate

---

51. In two factually similar cases, each involving a U.S. border patrol agent that fatally shot a Mexican national across the United States–Mexico border, the Ninth and Fifth Circuits diverged as to whether the plaintiff was entitled to pursue a Fourth Amendment *Bivens* claim against the federal officer.

An en banc Fifth Circuit panel defined Mexico as the situs of the seizure, finding the claim entailed the extraterritorial application of the Fourth Amendment. See Hernandez v. Mesa, 885 F.3d 811, 814 (5th Cir. 2018), aff'd, 140 S. Ct. 735 (2020) (declining to extend a *Bivens* remedy where "[t]he transnational aspect of the facts presents a 'new context' under *Bivens*, and numerous 'special factors' counsel against federal courts' interference with the Executive and Legislative branches").

By contrast, the Ninth Circuit appeared to define the situs of the seizure by the site of the border patrol agent in Arizona—at least to the extent necessary to distinguish the facts from *Verdugo-Urquidez*, the 1990 Supreme Court case restricting the circumstances under which nonresident aliens may claim the Fourth Amendment's protections. See Rodriguez v. Swartz, 899 F.3d 719, 731 (9th Cir. 2018), vacated, 140 S. Ct. 1258 (2020) (mem.) ("[U]nlike the American agents in *Verdugo-Urquidez*, who acted on Mexican soil, [agent] Swartz acted on American soil. Just as Mexican law controls what people do there, American law controls what people do here."). The Ninth Circuit affirmed the district court's denial of Swartz's motion to dismiss the case on qualified immunity grounds and authorized the plaintiff to pursue a Fourth Amendment *Bivens* claim. Id. at 748.

Granting certiorari in *Hernandez*, the Supreme Court resolved this circuit split by affirming the judgment of the en banc Fifth Circuit panel that declined to extend a *Bivens* remedy. *Hernandez*, 140 S. Ct. 735, 749–50 (2020) ("In sum, this case features multiple factors that counsel hesitation about extending *Bivens*, but they can all be condensed to one concern—respect for the separation of powers." (citing Ziglar v. Abbasi, 137 S. Ct. 1843, 1857–58 (2017))). Following *Hernandez*, the Court granted certiorari and vacated judgment in *Swartz*, remanding the case to the Ninth Circuit for further proceedings. Swartz v. Rodriguez, 140 S. Ct. 1258 (2020) (mem.), remanded to 800 F. App'x 535 (9th Cir. 2020) (mem.).

52. See Daskal, The Un-Territoriality of Data, supra note 14, at 370.

53. See id at 371–72.

54. In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 220 & n.27 (2d Cir. 2016), vacated and remanded sub nom. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam) ("[I]t is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized [in Dublin] by Microsoft, acting as an agent of the government."). The court reasoned, pursuant to the presumption against extraterritoriality, "that legislation of Congress 'is meant to apply only within the territorial jurisdiction of the United States,' unless a contrary intent clearly appears." Id. at 210 (quoting Morrison v. Nat'l Austl. Bank, 561 U.S. 247, 255 (2010)). The court first determined the SCA's warrant provisions were not meant to apply extraterritorially, id. at 210–16, and that the "focus" of the warrant provisions was "user privacy." Id. at 216–20. The court then found the privacy invasion would occur where the electronic communications

judge found, by the location where "the information is reviewed in the United States."[55]

B. *Pre–Rule 41(b)(6)(A) NIT Searches*

In Operations Pacifier (2015) and Torpedo (2012), courts implicitly defined the situs of the search by either the targeted device or the relevant government server and law enforcement officer executing the search. In each operation, officers sought and obtained one search warrant from one magistrate judge authorizing the deployment of a NIT onto *all* devices accessing each dark-web site—devices later discovered to be located beyond the authorizing magistrate judge's judicial district.[56] Officers seized and continued to operate the server hosting the relevant child pornography sites at a government facility.[57]

Because target visitors had used anonymizing software, the government was unable to specify in its warrant applications the precise devices to be searched. Instead, the government drew from the doctrine of "anticipatory" warrants,[58] which provides that a magistrate judge may authorize

---

are accessed—in Dublin. In turn, the court found that "execution of the Warrant would constitute an unlawful extraterritorial application of the Act." Id. at 220–22; see also Daskal, Borders and Bits, supra note 16, at 187–88 (summarizing the Second Circuit's reasoning).

55. In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 468, 472 (S.D.N.Y. 2014), rev'd and remanded, 829 F.3d 197 (2d Cir. 2016), vacated and remanded sub nom. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam). Following passage of the CLOUD Act in 2018, the government obtained a new warrant. In turn, the Supreme Court dismissed *Microsoft* as moot and vacated the judgment on review. *Microsoft*, 138 S. Ct. at 1188.

56. See Mirja Gutheil, Quentin Liger, Aurélie Heetman, James Eager & Max Crawford, European Parliament Policy Department C: Citizens' Rights and Constitutional Affairs, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation, and Comparison of Practices 29 (2017), https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf [https://perma.cc/JP5Q-CDKJ] (citing reports that the FBI searched more than 1,000 computers, including those of persons located in Denmark, Greece, and Chile); Kevin Poulsen, The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users, WIRED (Dec. 16, 2014), https://www.wired.com/2014/12/fbi-metasploit-tor [https://perma.cc/FC8T-5TBB] (noting that Operation Torpedo was "the first time—that we know of—that the FBI deployed such code broadly against every visitor to a website, instead of targeting a particular suspect").

57. See ACLU et al., supra note 39, at 6–7. Law enforcement deployed NITs to obtain the IP addresses and other identifying information of visitors to specified child pornography dark-web sites. Id. Officers drew upon this identifying information to connect the anonymized visitors to individuals, information that they in turn used to support warrant applications for physical searches of the suspects' homes. See, e.g., United States v. Hammond, 263 F. Supp. 3d 826, 828–29 (N.D. Cal. 2016), aff'd, 740 F. App'x 573 (9th Cir. 2018) (Operation Pacifier); United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *3–4 (D. Neb. Aug. 5, 2016) (Operation Torpedo).

58. See United States v. Grubbs, 547 U.S. 90, 96 (2006) ("Anticipatory warrants . . . require the magistrate to determine (1) that it is *now probable* that (2) contraband, evidence of a crime, or a fugitive *will be* on the described premises (3) when the warrant is executed.").

a search "subject to defined conditions that trigger the warrant's execution."[59] In Operation Pacifier, for example, the search warrant application provided that the NIT would deploy onto the devices of those that logged in to the child pornography site Playpen.[60] In Operation Torpedo, the search warrant application for dark-web site "Hidden Service A" conditioned deployment of the NIT on users accessing specific pages or privately communicating through the site.[61]

Defendants indicted as part of Operations Pacifier and Torpedo moved to suppress evidence obtained as a result of the NIT searches, arguing in part that the search warrants were invalid under the Federal Magistrates Act and Federal Rule of Criminal Procedure 41(b).[62] These defendants argued that the authorizing magistrate judges lacked jurisdiction to issue the NIT warrants to search computers beyond their judicial districts.[63]

1. *Two Sources of Authority: Rule 41 and the Federal Magistrates Act.* — These challenges implicated the two sources of law that define where a magistrate judge may issue a search warrant: the Federal Magistrates Act and Federal Rule of Criminal Procedure 41(b). Section 636 of the Magistrates Act sets forth magistrate judges' powers and geographically limits where they may be exercised.[64] Rule 41(b), in turn, sets forth one substantive power—the authority to issue search warrants for property located within a magistrate judge's judicial district[65] unless one of the now-five enumerated exceptions applies.[66] The fifth exception, subsection (b)(6), took effect in December 2016.[67] Subsection (b)(6)(A) expressly authorizes magistrate judges to issue warrants for searches of the sort at

59. Mayer, supra note 7, at 620–24 & n.183 (explaining the doctrine and its use in NIT searches).

60. See Attachment A to Application for a Search Warrant at 3, In re Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015), https://www.eff.org/files/2016/08/25/nit_warrant.pdf (on file with the *Columbia Law Review*). The government defined the "place to be searched" in its warrant application as these "activating computers," or "those of any user or administrator who logs into the target website." Id.

61. See Attachment A to Search and Seizure Warrant at 28, In re Search of Computers that Access the Website "Hidden Service A" Which Is Located at oqm66m6lyt6vxk7k.onion, No. 8:12-mj-00360 (D. Neb. filed Nov. 20, 2012), *in* United States v. Cottom, No. 8:13-cr-00108-JFB-TDT, 2015 WL 9308226 (D. Neb. Dec. 22, 2015), ECF No. 122-2, aff'd, 679 F. App'x 518 (8th Cir. 2017); Mayer, supra note 7, at 584 n.41 (collecting the three warrant applications in Operation Torpedo).

62. 28 U.S.C. § 636(a) (2018); Fed. R. Crim. P. 41(b). Operation Pacifier defendant Robert Clay Eldred's challenge is illustrative. See United States v. Eldred, 933 F.3d 110, 114 (2d Cir. 2019).

63. See *Eldred*, 933 F.3d at 114–15.

64. 28 U.S.C. § 636(a).

65. Fed. R. Crim. P. 41(b)(1).

66. Fed. R. Crim. P. 41(b)(2)–(6).

67. See Fed. R. Crim. P. 41 advisory committee's note on 2016 amendments; Mayer, supra note 7, at 626.

issue in Operations Pacifier and Torpedo—when the district in which the data is located "has been concealed through technological means."[68]

Because this exception was not available when the magistrate judges issued the warrants in Operations Pacifier and Torpedo, the government argued in litigation arising from these operations that the warrant had properly issued under one of the existing Rule 41(b) exceptions.[69]

2. *Operations Pacifier and Torpedo.* — In litigation arising from Operation Pacifier, numerous courts defined the situs of the search by the Fourth Amendment's traditional framework, finding the search occurred at the site of each "activating computer" onto which the NIT deployed.[70] Others, however, implicitly defined the search by the site of the government server and investigating officer.[71] These courts adopted the government's argument that the NIT was akin to a tracking device, finding the warrant valid under Rule 41(b)(4)'s tracking device exception. As one district court explained, the NIT "'installed' at the site of the Playpen server when the [d]efendant connected to the Playpen site in the Eastern District of Virginia" and, "through the 'exploit,' was able to travel to, and track the location of, the [d]efendant's computer."[72]

In Operation Torpedo, the FBI conducted a watering-hole attack similar to that deployed in Operation Pacifier to investigate visitors of three child pornography dark-web sites.[73] Comparatively few Operation Torpedo defendants have challenged the authorizing magistrate judge's jurisdictional authority to issue the NIT warrant.[74] Yet as in Operation

---

68. Fed. R. Crim. P. 41(b)(6)(A).

69. See infra section I.B.2.

70. See United States v. Austin, 230 F. Supp. 3d 828, 832 (M.D. Tenn. 2017) (collecting cases).

71. See, e.g., id. 832–33; United States v. Jones, 230 F. Supp. 3d 819, 825 (S.D. Ohio 2017), aff'd, No. 18-3743, 2019 WL 3764628 (6th Cir. June 27, 2019); United States v. Sullivan, 229 F. Supp. 3d 647, 655 (N.D. Ohio 2017); United States v. Bee, No. 16-00002-01-CR-W-GAF, 2017 WL 424905, at *4 (W.D. Mo. Jan. 13, 2017), R. & R. adopted, No. 16-00002-01-CR-W-GAF, 2017 WL 424889 (W.D. Mo. Jan. 31, 2017); United States v. McLamb, 220 F. Supp. 3d 663 (E.D. Va. 2016), aff'd 880 F.3d 685 (4th Cir. 2018); United States v. Lough, 221 F. Supp. 3d 770, 778 (N.D. W. Va. 2016), aff'd per curiam, 721 F. App'x 291 (4th Cir. 2018); United States v. Jean, 207 F. Supp. 3d 920, 942 (W.D. Ark. 2016), aff'd, 891 F.3d 712 (8th Cir. 2018); United States v. Eure, No. 2:16-cr-00043, 2016 WL 4059663 (E.D. Va. July 28, 2016), aff'd per curiam, 723 F. App'x 238 (4th Cir. 2018); United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016); United States v. Darby, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016), aff'd per curiam, 721 F. App'x 304 (4th Cir. 2018).

72. *Austin*, 230 F. Supp. 3d. at 833. Rule 41(b)(4) authorizes the issuance of a warrant "to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." Fed. R. Crim. P. 41(b)(4).

73. For background on the Operation, see United States v. Reibert, No. 8:13CR107, 2015 WL 366716, at *4–6 (D. Neb. Jan. 27, 2015); ACLU et al., supra note 39, at 6–7.

74. Though Operation Torpedo (2012) predated Operation Pacifier (2015), defendants did not challenge the magistrate judge's warrant on jurisdictional grounds until after defendants indicted in connection with Operation Pacifier began to do so. The timeline

Pacifier, at least one district court has upheld the warrant under Rule 41(b)(4)'s tracking device exception.[75] This court appeared to agree with the many Operation Pacifier courts that the search occurred at the site of the activating computers. But the court found that the computer "in essence travelled into the district of Nebraska to communicate with the website located in Nebraska."[76] In so doing, the court implicitly defined the situs of the search by *both* the site of the investigating officer and the device searched.

C. *Post–Rule 41(b)(6)(A) NIT Searches*

The 2016 amendment to Rule 41(b) minimized the immediate importance of defining the situs of a NIT search. Rule 41(b) provides that in situations in which the location of the target "media or information" has been concealed, a magistrate judge may issue a NIT warrant in any district "where activities related to a crime may have occurred."[77]

Two unsealed NIT warrants issued under the amended Rule 41(b)(6)(A) illustrate that magistrate judges have authorized NIT warrants without regard to whether the devices or data to be searched are located within their judicial districts. In each search warrant application, law enforcement continued to draw upon the doctrine of anticipatory warrants to describe the "location to be searched" by the then-unknown location of the target device or dark-web accounts associated with the search target.[78]

In an investigation of computer crimes and stalking in the Western District of New York (W.D.N.Y.), law enforcement applied for and obtained a NIT search warrant in 2017 to aid in identifying the search target and

---

suggests that Torpedo defendants drew from arguments raised by Pacifier defendants, and perhaps explains why Operation Pacifier, not Operation Torpedo, has been the principal subject of commentary on this jurisdictional question even though both operations present the puzzle.

This timeline may also reflect the involvement of the ACLU, the Electronic Frontier Foundation (EFF), or other legal nonprofit organizations that, public filings suggest, were not involved in Operation Torpedo litigation. See, e.g., ACLU et al., supra note 39, at 9–21 (outlining legal strategies to aid criminal defense attorneys representing NIT search targets); Mark Rumold, Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation, Elec. Frontier Found. (Sept. 15, 2016), https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation [https://perma.cc/DN65-Z2R2] (introducing a blog series on the "significant legal questions" raised by Operation Pacifier).

75. See United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *6 (D. Neb. Aug. 5, 2016).

76. Id.

77. Fed. R. Crim. P. 41(b)(6).

78. See In re Search of Information Associated with Multiple Accounts that Are Stored on the Server Hosting Tor Hidden Service AlphaBay, No. 1:17-mj-00208 (D.D.C. filed Apr. 6, 2017) [hereinafter AlphaBay Search Warrant]; W.D.N.Y. Search Warrant, No. 6:17-mj-00519 (W.D.N.Y. filed Jan. 31, 2017).

the associated device.[79] The warrant application defined the "location to be searched" as "the portion of any computer accessing (target emails)" that would deploy the NIT.[80]

In another investigation in the District of Columbia, law enforcement obtained a NIT warrant to investigate the vendor of bomb threat emails on the now-defunct dark-web marketplace AlphaBay.[81] The warrant authorized the FBI to deploy a NIT onto the computer server operating AlphaBay and to search the AlphaBay accounts of the suspected perpetrator, in order to obtain evidence about the suspect and identify customers and additional victims.[82] As in the W.D.N.Y. search, the warrant application defined the place to be searched by the thing searched—the AlphaBay accounts tied to specified usernames.[83]

These warrants make clear that subsection (b)(6)(A) has functioned as intended. Yet they also suggest that if the amended Rule were held invalid or found inapplicable to these searches, courts would confront the same question as had arisen in Operations Pacifier and Torpedo litigation: Where did the search occur?

II. CONSTITUTIONAL REMEDIES AND A TERRITORIALLY UNROOTED FOURTH AMENDMENT

Though the 2016 amendment to Rule 41(b) purported to authorize NIT searches that execute beyond the judicial district of the authorizing magistrate judge, several circuit courts to have considered the amended Rule have questioned its validity in light of the Federal Magistrates Act's own territorial restrictions.[84] As section II.A discusses, these opinions raise

---

79. Affidavit to Application for a Search Warrant at 27–29, *W.D.N.Y. Search Warrant*, No. 6:17-mj-00519 (describing the mechanics and purpose of the NIT search).

80. Attachment A at 1, *W.D.N.Y. Search Warrant*, No. 6:17-mj-00519.

81. Affidavit to Application for a Search Warrant at 7–9 ¶¶ 20–21, 15–16 ¶¶ 36–37, *AlphaBay Search Warrant*, No. 1:17-mj-00208. It is unclear how this NIT search, authorized in April 2017, relates to the joint international operation (Operation Bayonet) announced in July 2017, which led to the takedown of servers operating AlphaBay, the arrest of the AlphaBay administrator, and the seizure of tens of millions in cryptocurrency and assets. See Off. of Inspector Gen., DOJ, Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities 6 (2020), https://oig.justice.gov/sites/default/files/reports/21-014.pdf [https://perma.cc/2GM4-9NNR]; Press Release, AlphaBay, the Largest Online "Dark Market," Shut Down, DOJ (July 20, 2017), https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down [https://perma.cc/P373-F662].

Though the Justice Department discussed Operation Bayonet in a 2020 audit of the FBI's dark-web strategy, the government has not disclosed whether this takedown involved the deployment of a NIT. See Off. of Inspector Gen., supra.

82. See Affidavit to Application for a Search Warrant at 15–16 ¶¶ 36–37, *AlphaBay Search Warrant*, No. 1:17-mj-00208; Attachment B at 2, *AlphaBay Search Warrant*, No. 1:17-mj-00208.

83. Attachment A at 1, *AlphaBay Search Warrant*, No. 1:17-mj-00208.

84. 28 U.S.C. § 636(a) (2018); see also United States v. Eldred, 933 F.3d 110, 118 (2d Cir. 2019) ("[T]he Fourth Amendment issues raised by [defendant] Eldred could recur, but

the prospect that courts may deem the amended Rule 41(b) insufficient to authorize extra-district NIT searches, reviving the jurisdictional question that arose in connection with Operations Pacifier and Torpedo. As section II.B argues, districts that define the situs of a NIT search by the location of the government server or investigating officer—within the authorizing magistrate judge's judicial district—may enable nonresident aliens to raise Fourth Amendment claims, but render their pursuit of constitutional remedies contingent on the presiding judge's jurisdictional definition.

A. *Rule 41(b)(6)(A) May Conflict with the Federal Magistrates Act*

As section I.B.1 discusses, when the magistrate judges in Operations Pacifier and Torpedo issued the relevant NIT warrants, Rule 41(b) had limited magistrate judges to issuing warrants for searches executed within their judicial districts unless one of the then-four exceptions applied. The fifth exception, subsection (b)(6), authorizes the issuance of warrants for NIT searches when "the district where the media or information is located has been concealed through technological means."[85] As the Third Circuit noted when presiding over one Operation Pacifier challenge, "Rule 41(b)(6) . . . went into effect in December 2016 to authorize NIT-like warrants."[86]

Yet the Second and Ninth Circuits—drawing from a Tenth Circuit concurrence by then-Judge Gorsuch—have raised doubts about whether Rule 41(b)(6)(A) indeed accords this power.[87] Though the new Rule confers on magistrate judges the authority to issue warrants for extra-district searches under certain circumstances, the Magistrates Act, these circuits offer, may impose "independent territorial restrictions" on magistrate judges' jurisdiction that Rule 41(b)(6)(A) cannot supersede.[88] These courts suggest that Rule 41(b)(6)(A) leaves magistrate judges with no

---

now pursuant to § 636(a) alone."); United States v. Henderson, 906 F.3d 1109, 1115 n.5 (9th Cir. 2018) ("[E]ven if the government is correct that the magistrate did not exceed her statutory authority as a result of the Rule 41(b) violation, such action may still have *independently* violated § 636's similar territorial restrictions." (citing United States v. Krueger, 809 F.3d 1109, 1121 (10th Cir. 2015) (Gorsuch, J., concurring))).

85. Fed. R. Crim. P. 41(b)(6)(A).

86. United States v. Werdene, 883 F.3d 204, 218 (3d Cir. 2018).

87. See *Eldred*, 933 F.3d at 117 ("Several of the nine sister circuits to have addressed the NIT warrant here have noted that the situation that arose in this case will not recur due to the passage of the 2016 amendments to Rule 41(b) . . . . But even this point is not beyond doubt."); *Henderson*, 906 F.3d at 1115 ("The Federal Magistrates Act . . . defines the scope of a magistrate judge's authority, imposing jurisdictional limitations on the power of magistrate judges that cannot be augmented by the courts."); *Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring) ("The Federal Magistrates Act identifies only three geographic areas in which a federal magistrate judge's powers are effective . . . . The problem in this case is that a magistrate judge purported to exercise power in none of these places.").

88. *Eldred*, 933 F.3d at 117 (internal quotation marks omitted) (quoting *Krueger*, 809 F.3d at 1121 (Gorsuch, J., concurring)); see also *Henderson*, 906 F.3d at 1115 n.5.

more authority than they possessed prior to this rule change: the power to issue warrants within their judicial districts unless one of four statutorily codified exceptions applies.[89]

As Gorsuch argued, the Magistrates Act both defines a magistrate judge's powers[90] and geographically limits to three contexts *where* these powers may be exercised: (1) "within the district in which sessions are held by the court that appointed the magistrate judge"; (2) "at other places where that court may function"; and (3) "elsewhere as authorized by law."[91] Rule 41(b), which defines under what conditions a magistrate judge has authority to issue a search warrant,[92] sets forth one of the magistrate judge's "powers and duties"[93] consistent with the Magistrates Act: the authority to issue such warrants.

According to this interpretation—cited but not elaborated upon by the Second and Ninth Circuits—Rule 41(b)(6)(A) does not fall within any of these three geographic contexts.[94] A NIT warrant of the sort issued in Operations Pacifier and Torpedo would very likely reach at least some search targets beyond the authorizing magistrate judge's judicial district—and perhaps beyond the United States[95]—in contravention of the first two contexts ("the district in which sessions are held" and "other places where that court may function").[96] Nor, under this interpretation, would Rule 41(b)(6)(A) qualify as a "law," as the third context provides.[97] As Gorsuch advanced, a plain reading of the Magistrates Act states "'elsewhere as authorized by law'—not 'elsewhere as authorized by law or *rule*.'"[98]

---

89. See Mayer, supra note 7, at 627 ("[I]n a plain reading of the statutory text, the Federal Rules of Criminal Procedure can only create new powers and duties for magistrate judges *within their district*. The Federal Rules cannot create extra-district powers or duties.").

90. 28 U.S.C. § 636(a)(1) (2018) (according judges "all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure").

91. Id. § 636(a).

92. See Fed. R. Crim. P. 41(b); Brian L. Owsley, Beware of Government Agents Bearing Trojan Horses, 48 Akron L. Rev. 315, 319 (2015).

93. 28 U.S.C. § 636(a)(1).

94. See id. § 636(a) ("Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law . . . .").

95. See Daskal, Borders and Bits, supra note 16, at 206 n.94 (noting that "the vast majority of Tor users are foreign based," such that at least in some cases, "remote searches of Tor-users' devices will yield the search of a device located in a foreign territory"). In the one-year period beginning January 1, 2020, an estimated 25.88% of mean daily users directly connected to Tor from the United States. See Top-10 Countries by Relay Users, Tor Metrics, https://metrics.torproject.org/userstats-relay-table.html?start=2020-1-01&end=2021-01-01 [https://perma.cc/6SKJ-FZVY] (last visited Jan. 28, 2021).

96. 28 U.S.C. § 636(a).

97. See supra text accompanying note 91.

98. United States v. Krueger, 809 F.3d 1109, 1120 (10th Cir. 2015) (Gorsuch, J., concurring) (quoting 28 U.S.C. § 636).

Gorsuch reinforced this textualist construction with an argument sounding in congressional intent, noting that the Magistrates Act elsewhere distinguishes between laws and rules when it details the scope of a magistrate judge's powers, a distinction suggesting that Congress intentionally declined to permit geographic expansions of a magistrate judge's jurisdiction by federal rules of procedure.[99] Historical practice lends support to Gorsuch's interpretation: Congress has statutorily codified each of the four prior exceptions to Rule 41(b) that empower magistrate judges to issue warrants for extra-district searches.[100]

If, as Gorsuch advanced and the Second and Ninth Circuits cited, Rule 41(b)(6)(A) is not a "law" within the meaning of the Magistrates Act, its authorization of extra-district searches is in conflict with the Act's territorial restriction on where magistrate judges may exercise their statutorily defined powers. The Rules Enabling Act, which authorizes the Supreme Court to promulgate federal rules of "practice and procedure" like Rule 41, states that "[a]ll laws in conflict with" promulgated rules are "of no further force or effect."[101] The Supreme Court has affirmed this doctrine of later-in-time supersession for both civil and criminal rules of procedure.[102] Yet, supersession applies only to rules of "practice and procedure" that do not "abridge, enlarge or modify any substantive right."[103]

Though Gorsuch does not address the issue, his analysis—that the Magistrates Act governs notwithstanding the later-in-time amendment to Rule 41(b)—would imply that the venue provisions of Rule 41(b) are not rules of "practice and procedure" to which the Rules Enabling Act's displacement provision applies.[104] If so, the Magistrates Act would continue

---

99. Id.

100. See Mayer, supra note 7, at 627–28.

101. 28 U.S.C. § 2072(a)–(b). The Rules Enabling Act and subsequent amendments describe the procedure by which rules are introduced and promulgated. Five subject-specific advisory committees evaluate proposals for rules amendments. After considering public comments, an advisory committee submits a proposed amendment to the Standing Committee. The Standing Committee independently reviews the advisory committee's findings before recommending the amendment to the Judicial Conference. The Conference may then submit the proposed amendment to the Supreme Court. If the Court approves the change, it will promulgate the rule to take effect within the year unless Congress enacts legislation to "reject, modify, or defer the pending rules." How the Rulemaking Process Works, U.S. Cts., https://www.uscourts.gov/rules-policies/about-rulemaking-process/how-rulemaking-process-works [https://perma.cc/K6MF-ZCLU] (last visited Jan. 13, 2021).

102. See Henderson v. United States, 517 U.S. 654, 656 (1996) (Federal Rules of Civil Procedure); Davis v. United States, 411 U.S. 233, 241–42 (1973) (Federal Rules of Criminal Procedure).

103. 28 U.S.C. § 2072(a)–(b); see also United States v. Isaacs, 351 F. Supp. 1323, 1328 (N.D. Ill. 1972) ("The provision that 'laws in conflict with such rules shall be of no further force or effect' does no more than provide that the rules of pleading, practice and procedure prescribed by the Supreme Court supercede [sic] those rules . . . in effect at the time the legislation became effective.").

104. See, e.g., United States v. Eldred, 933 F.3d 110, 117–18 (2d Cir. 2019) ("[T]he recent amendments to Rule 41 may not alone be sufficient to answer the question whether

to impose "independent territorial restrictions" on magistrate judges' authority to issue warrants for NIT searches beyond their judicial district, notwithstanding the amended Rule 41(b).[105]

A NIT defendant located beyond the authorizing magistrate judge's judicial district might assert that the warrant issued in violation of the Magistrates Act. The defendant would define the situs of the NIT search by the location of the device or data, arguing that the search reached beyond the magistrate judge's district to the district in which the defendant's device or data was located. That the Second and Ninth Circuits questioned whether Rule 41(b)(6)(A) sufficed to authorize extra-district searches suggests that at least some courts may hold for NIT defendants, concluding that the Magistrates Act's own territorial restrictions bind magistrate judges absent a statute codifying Rule 41(b)(6)(A).

This holding would pave the way for a NIT defendant to invoke the Fourth Amendment's exclusionary rule to suppress evidence obtained from the search.[106] Yet, invalidation of Rule 41(b)(6)(A) would also revive the jurisdictional question that arose prior to the 2016 amendment to the Rule. Should this occur, litigation stemming from Operations Pacifier and Torpedo suggests that courts would continue to adopt divergent definitions of the situs of a NIT search.

B. *Domesticating Nonresident Aliens' Fourth Amendment Claims*

Courts that define a NIT search by the location of the government server or investigating officer may enable nonresident alien search targets to claim the Fourth Amendment's protections. Litigants would draw upon lower court precedent that recognizes nonresident aliens' Fifth and Sixth Amendment rights when the alleged violation is said to occur within the United States.

1. *Supreme Court Doctrine Limiting Nonresident Aliens' Fourth Amendment Rights.* — Supreme Court case law governing the applicability of constitutional provisions beyond the borders of the United States has evolved from

---

a *magistrate judge*, as opposed to a district court judge, has authority to issue NIT-style warrants pursuant to the amended Rule."); United States v. Henderson, 906 F.3d 1109, 1115 n.5 (9th Cir. 2018) ("[E]ven if the government were correct in asserting that Rule 41(b) was not violated or that such Rule is merely a technical venue provision, the government fails to grapple with the independent territorial limitations imposed upon a magistrate judge's jurisdiction by § 636 *itself*."); United States v. Krueger, 809 F.3d 1109, 1122 (10th Cir. 2015) (Gorsuch, J., concurring) ("Section 636(a)'s territorial restrictions are *jurisdictional* limitations on the power of magistrate judges and the Supreme Court has long taught that the violation of a statutory jurisdictional limitation—quite unlike the violation of a more prosaic rule or statute—is *per se* harmful.").

105. *Krueger*, 809 F.3d at 1121.

106. But see *Eldred*, 933 F.3d at 116–17 (questioning "whether a venue requirement exists as a matter of Fourth Amendment law" and providing that even assuming "a constitutional dimension to *some* cases in which a warrant might exceed territorial limits . . . it is not clear that *all* such cases present viable Fourth Amendment claims").

a strictly territorial approach to one guided by citizenship and geographic distinctions.[107] These distinctions continue to embody the so-called "compact theory" of constitutional extraterritoriality.[108] Under this view, the Constitution's criminal procedure provisions do not necessarily bind law enforcement when it operates beyond the territorial United States, for the Constitution "was written to provide sound government to a particular nation—and not to bestow rights to all people across the globe."[109] Rather, this theory provides that "international law, diplomacy, and policy choices of the political branches" historically constrained the executive's authority to exercise enforcement authority abroad.[110]

Prior to the mid-twentieth century, constitutional rights were not available—to citizens or noncitizens—beyond the borders of the United States or its territories.[111] In the 1957 decision *Reid v. Covert*, a plurality of the Court departed from this strict territorial limitation on the constitutional provisions applicable to citizens located abroad.[112] Yet the Court's doctrines have largely preserved territorial-based limitations as to the

---

107. For a comprehensive account of the Court's jurisprudence on the constitutional rights of nonresident citizens and aliens, see generally Karen Nelson Moore, Aliens and the Constitution, 88 N.Y.U. L. Rev. 801 (2013).

108. See Jose A. Cabranes, Our Imperial Criminal Procedure: Problems in the Extraterritorial Application of U.S. Constitutional Law, 118 Yale L.J. 1660, 1665–67 (2009) (outlining the compact theory); see also In re Ross, 140 U.S. 453, 464 (1891) ("By the Constitution a government is ordained and established 'for the United States of America,' and not for countries outside of their limits . . . . The Constitution can have no operation in another country.").

109. Cabranes, supra note 108, at 1698.

110. Andrew Kent, A Textual and Historical Case Against a Global Constitution, 95 Geo. L.J. 463, 505 (2007).

111. In the *Insular Cases*, a series of cases decided at the turn of the twentieth century, the Court cabined the Constitution's application to the then-newly acquired territories. It set forth a tiered doctrine of constitutional incorporation: The Constitution's provisions applied in full in "incorporated" territories, or territories expected to become states, but only partly in the "unincorporated" territories—those, such as Puerto Rico, that the United States had claimed but had not made "destined for statehood." See Boumediene v. Bush, 553 U.S. 723, 757–59 (2008) (discussing the *Insular Cases*). The Court has not overturned this tiered distinction. See Gerald Neuman, Understanding Global Due Process, 23 Geo. Immigr. L.J. 365, 366 (2009). According to Neuman, the *Insular Cases* reflect that "the Constitution as such applies to the U.S. government wherever it acts." Id.

112. 354 U.S. 1, 5 (1957) (plurality opinion) (Black, J.) (holding that U.S. civilian dependents living on military bases abroad are entitled to the Fifth and Sixth Amendment rights to indictment by a grand jury and trial by jury in capital cases); see also Christina Duffy Burnett, A Convenient Constitution? Extraterritoriality After *Boumediene*, 109 Colum. L. Rev. 973, 996 (2009); Neuman, supra note 111, at 367–68. The *Reid* plurality did not expressly overrule *In re Ross*, an 1891 decision holding that the Constitution's criminal procedure rights do not extend to U.S. citizens prosecuted beyond the United States. *Reid*, 354 U.S. at 11–12 (citing *In re Ross*, 140 U.S. at 453). But the plurality dismissed the *Ross* Court's "approach," advancing that "[a]t best, the *Ross* case should be left as a relic from a different era." Id. at 12; see also Moore, supra note 107, at 828 (elaborating on the *Reid* plurality opinion).

rights of noncitizens when the conduct relevant to investigation and prosecution occurs abroad.[113]

In the post–World War II case *Johnson v. Eisentrager*, the Court declined to extend the Fifth Amendment's protections to German nationals convicted by a U.S. military tribunal in China and detained in Allied-occupied Germany.[114] *Eisentrager*'s precise holding has remained a matter of dispute, however, as the *Eisentrager* Court reasoned on separate grounds that the German nationals had been detained abroad and had committed wartime actions against the United States.[115]

The Court drew upon *Eisentrager*'s first rationale, premised on a territorially restricted view of the Constitution's reach, in its 1990 decision *United States v. Verdugo-Urquidez*.[116] The *Verdugo-Urquidez* Court held that the Fourth Amendment does not apply to nonresident aliens in searches and seizures conducted beyond the United States.[117] Speaking for himself and Justices White, O'Connor, and Scalia, Chief Justice Rehnquist reasoned that the Constitution's reach depended on whether an alien had "come within the territory of the United States and developed substantial connections with this country."[118] In so reasoning, Rehnquist

---

113. See Moore, supra note 107, at 823. A different line of precedent governs the rights of aliens in immigration proceedings, which are civil in nature. Id. at 823–24. However, the Court has long accorded Fifth Amendment Due Process protection to nonresident aliens in civil proceedings, enabling defendants to challenge a court's exercise of personal jurisdiction under the court's Due Process–rooted "minimum contacts" test. See Gary A. Haugen, Personal Jurisdiction and Due Process Rights for Alien Defendants, 11 B.U. Int'l L.J. 109, 115–17 (1993) (discussing the challenge of applying *Verdugo-Urquidez*'s "substantial connections" test to defendants challenging personal jurisdiction, for defendants who lack such connection to the United States "need the 'minimum contacts' test the most . . . [but] under *Verdugo-Urquidez*, cannot claim this constitutional protection"); Austen L. Parrish, Sovereignty, Not Due Process: Personal Jurisdiction over Nonresident Alien Defendants, 41 Wake Forest L. Rev. 1, 37 (2006) (commenting on the apparent incongruity between "the Court's current due process formulations in the jurisdictional context . . . [and] its approach to U.S. constitutionalism in other contexts").

114. 339 U.S. 763, 765–67, 784–85 (1950); see also Moore, supra note 107, at 826–30.

115. *Eisentrager*, 339 U.S. at 783–85; see also Moore, supra note 107, at 827.

116. 494 U.S. 259 (1990). *Verdugo-Urquidez* arose from the criminal prosecution of Mexican national Rene Martin Verdugo-Urquidez. Pursuant to a United States–obtained arrest warrant, Verdugo-Urquidez had been transported to the United States and incarcerated pending trial. Thereafter, federal agents in concert with Mexican officials conducted a warrantless search of Verdugo-Urquidez's Mexican residences. At trial, Verdugo-Urquidez invoked the Fourth Amendment's exclusionary rule to suppress the evidence seized. Id. at 262–63; see also Moore, supra note 107, at 836–37.

117. *Verdugo-Urquidez*, 494 U.S. at 274–75.

118. Id. at 271; see also Duffy Burnett, supra note 112, at 1015 ("A majority of the Court held that the Fourth Amendment did not apply to searches of noncitizens' homes abroad. Although Kennedy joined Chief Justice William Rehnquist's opinion for the Court, the reasoning in his concurrence was not consistent with Rehnquist's."); Moore, supra note 107, at 836–37 (explaining that "[f]our Justices accepted the view that aliens must be within the United States and have 'substantial connections' in order to qualify for Fourth Amendment protections, while Justice Kennedy offered mixed support for the substantial connections prong of this two-part test").

distinguished between the Fourth and Fifth Amendments. Whereas a violation of the Fifth Amendment right against self-incrimination "occurs only at trial," "a violation of the [Fourth] Amendment is 'fully accomplished' at the time of an unreasonable governmental intrusion."[119] The Court defined the situs of the search as the location where officers seized evidence in Mexicali and San Felipe, Mexico, rather than where Mexican national Verdugo-Urquidez was detained or where prosecutors sought to admit evidence into the record at trial—in California.[120]

Justice Kennedy, writing in concurrence, departed from Rehnquist's "substantial connections" test,[121] which Rehnquist grounded in territorial- and citizenship-based distinctions. Kennedy advanced that the Fourth Amendment's applicability depended not on such distinctions but on the practicality of extending constitutional protections abroad.[122] Drawing on Justice Harlan's "impracticable and anomalous" test as set forth in Harlan's *Reid* concurrence,[123] Kennedy concluded that applying the Fourth Amendment to searches of nonresident aliens or their property

---

The Supreme Court has not spoken as to U.S. citizens' Fourth Amendment rights abroad. Three lower courts have concluded that law enforcement officers' searches of U.S. persons or property abroad are subject to the Fourth Amendment's reasonableness test but not its warrant and probable cause requirements. A circuit split has developed between the Ninth Circuit on the one hand and the Second and Seventh Circuits on the other as to the reasonableness test to be applied. While the Second and Seventh Circuits apply a standard balancing test, weighing the government's need for information against the subject's comparative privacy interest, the Ninth Circuit defines the reasonableness of the search pursuant to the local law of the country wherein the search is conducted. Compare United States v. Stokes, 726 F.3d 880, 893 (7th Cir. 2013) ("Whether a search is reasonable under the Fourth Amendment . . . requires the court to weigh the intrusion on individual privacy against the government's need for information and evidence."), and In re Terrorist Bombings of U.S. Embassies in E. Afr. (Fourth Amendment Challenges), 552 F.3d 157, 172 (2d Cir. 2008) ("To determine whether a search is reasonable . . . we examine the 'totality of the circumstances' to balance 'on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" (quoting Samson v. California, 547 U.S. 843, 848 (2006))), with United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987) ("[T]he law of the foreign country must be consulted at the outset as part of the determination whether or not the search was reasonable.").

119. *Verdugo-Urquidez*, 494 U.S. at 264 (citing United States v. Leon, 468 U.S. 897, 906 (1984); United States v. Calandra, 414 U.S. 338, 354 (1974); Kastigar v. United States, 406 U.S. 441, 453 (1972)).

120. Id. at 261–63 ("The question presented by this case is whether the Fourth Amendment applies to the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country."); id. at 272 ("We do not think the applicability of the Fourth Amendment to the search of premises in Mexico should turn on the fortuitous circumstance of whether the custodian of its nonresident alien owner had or had not transported him to the United States at the time the search was made.").

121. See Duffy Burnett, supra note 112, at 1015 (noting that Rehnquist's reasoning has come to be known by this shorthand).

122. *Verdugo-Urquidez*, 494 U.S. at 276–78 (Kennedy, J., concurring).

123. Id. at 277–78 (quoting Reid v. Covert, 354 U.S. 1, 74 (1957) (Harlan, J., concurring)).

would be "impracticable and anomalous," given the "absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conditions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials."[124] Though Kennedy reasoned that Verdugo-Urquidez would have had a colorable Fourth Amendment claim "[i]f the search had occurred in a residence within the United States," because officers executed the search in Mexico, the search did not implicate the Fourth Amendment.[125]

Nearly two decades later, in 2008, Kennedy brought this analysis into the majority in *Boumediene v. Bush*, reasoning that under certain circumstances, the Constitution's provisions apply to aliens located beyond the borders of the United States.[126] In *Boumediene*, the Court held that aliens detained at Guantánamo Bay, Cuba, are entitled to the privilege of the writ of habeas corpus, in part because it would not be "impracticable or anomalous" to apply the Constitution's Suspension Clause to Guantánamo.[127]

Commentators have suggested that *Boumediene* has implications beyond the Suspension Clause, insofar as it lays the groundwork for nonresident aliens to assert constitutional claims even when the individual resided and the alleged violation occurred abroad.[128] Yet most lower courts evaluating the Fourth Amendment claims of nonresident aliens have continued to regard *Verdugo-Urquidez*, not *Boumediene*, as controlling.[129]

2. *Asserting Fourth Amendment Claims.* — Lower courts have generally cabined the applicability of the Constitution's criminal procedure provisions for violations said to occur beyond the territorial borders of the United States. In recent years, however, some courts have worked within

---

124. Id. at 276–78.

125. Id. at 278.

126. 553 U.S. 723, 771 (2008).

127. Id. at 769–71 (internal quotation marks omitted) (citing *Reid*, 354 U.S. at 74 (Harlan, J., concurring)). The Suspension Clause provides: "The Privilege of the Writ of Habeas Corpus shall not be suspended, unless when in cases of rebellion or invasion the public safety may require it." U.S. Const. art. I, § 9, cl. 2.

128. See, e.g., Moore, supra note 107, at 829 ("[P]articularly after *Boumediene*'s rejection of formalistic analysis of the Constitution's extraterritorial application . . . *Reid*'s recognition of the extraterritorial application of the Fifth and Sixth Amendments to citizens arguably suggests the possibility of similar treatment for aliens that the United States reaches out to punish criminally."); Neuman, supra note 111, at 398–99 ("Although the Court could have written a narrow decision relying on factors unique to Guantanamo as a U.S. quasi-territory, Kennedy chose to frame the issue within the wider perspective of extraterritoriality as discussed in *Reid v. Covert* and his *Verdugo* concurrence . . . .").

129. See, e.g., United States v. Larrahondo, 885 F. Supp. 2d 209, 221–22 (D.D.C. 2012) (denying nonresident alien defendant's motion to suppress evidence from a wiretap in Colombia, because "*Verdugo* forecloses the claim under the Fourth Amendment"); see also Daskal, The Un-Territoriality of Data, supra note 14, at 342 & n.44 (collecting lower court opinions holding, based on *Verdugo-Urquidez*, that nonresident aliens without "substantial connections" to the United States are not entitled to the Fourth Amendment or other "individual" rights).

the Court's doctrines by redefining the violation as taking place domestically.

Federal courts in the Second, Fourth, and Ninth Circuits have drawn on the Court's doctrines that categorize constitutional criminal procedure rights as either freestanding rights—attaching at the time of the alleged violation, or trial rights—attaching upon the commencement of court proceedings.[130] The Court has found that the Fifth Amendment right against self-incrimination and the Sixth Amendment right to counsel are "trial" rights.[131] By contrast, the *Verdugo-Urquidez* Court defined the Fourth Amendment right to be free from "unreasonable searches and seizures" as a freestanding right violated at the time of the alleged search or seizure.[132]

Based on these distinctions, courts addressing Fifth[133] and Sixth[134] Amendment claims asserted by nonresident aliens have found the claims

---

130. See supra note 119 and accompanying text.

131. See Kansas v. Ventris, 556 U.S. 586, 592 (2009) (finding the Sixth Amendment right to counsel "is a right to be free of uncounseled interrogation, and is infringed at the time of the interrogation"); Chavez v. Martinez, 538 U.S. 760, 767 (2003) ("Statements compelled by police interrogations of course may not be used against a defendant at trial . . . but it is not until their use in a criminal case that a violation of the Self–Incrimination Clause occurs." (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990); Brown v. Mississippi, 297 U.S. 278, 286 (1936))); *Verdugo-Urquidez*, 494 U.S. at 264 (stating that violation of the Fifth Amendment privilege against self-incrimination "occurs only at trial," even though "conduct by law enforcement officials prior to trial may ultimately impair that right").

132. See *Verdugo-Urquidez*, 494 U.S. at 264.

133. See In re Terrorist Bombings of U.S. Embassies in E. Afr. (Fifth Amendment Challenges), 552 F.3d 177, 201 (2d Cir. 2008) ("[W]e hold that foreign nationals interrogated overseas but tried in the civilian courts of the United States are protected by the Fifth Amendment's self-incrimination clause."); United States v. Osorio-Arellanes, No. 4:11-cr-00150-TUC-DCB, 2019 WL 357933, at *3 (D. Ariz. Jan. 29, 2019), rev'd on recons., No. 4:11-cr-00150-TUC-DCB, 2019 WL 417039 (D. Ariz. Jan. 31, 2019) ("The Fifth Amendment privilege against self-incrimination applies when U.S. agents question a suspect in a foreign country." (citing *In re Terrorist Bombings*, 552 F.3d at 198–201)); United States v. Jefferson, 594 F. Supp. 2d 655, 670 (E.D. Va. 2009) ("[T]here is no doubt that the witnesses [residing in Nigeria] have a privilege against self-incrimination under the Fifth Amendment . . . . This conclusion holds regardless of whether the depositions take place in the United States or in Nigeria." (citing *In re Terrorist Bombings*, 552 F.3d at 199)).

134. In *United States v. Osorio-Arellanes*, the district court noted that the Sixth Amendment right to counsel "commences upon indictment and guarantees a defendant the right to have counsel present at all 'critical' stages of the criminal proceedings." No. CR-11-00150-004-TUC-DCB (BPV), 2019 WL 357933, at *4 (quoting Montejo v. Louisiana, 556 U.S. 778, 786 (2009)). The post-indictment interrogation of Mexican national Heraclio Osorio-Arellanes therefore constituted "a critical confrontational stage." Id. at *5. Accordingly, the court found that defendant Osorio-Arellanes was entitled to move to suppress statements made during the interrogation in alleged violation of his Sixth Amendment right to counsel, even though the defendant was a foreign national interrogated abroad. Id.

The court initially held that the government had violated Osorio-Arellanes's Sixth Amendment right to counsel, but reversed on reconsideration. United States v. Osorio-

domestic, not extraterritorial, in nature. In so holding, these courts have enabled the claims to proceed under the Court's precedent that accords nonresident aliens constitutional criminal procedure rights for violations defined as occurring within the United States,[135] rather than precedent—embodied in *Eisentrager* and *Verdugo-Urquidez*—that limits the rights of nonresident aliens for violations said to occur abroad.[136]

For example, in a 2008 Second Circuit opinion arising from the 1998 bombings of the U.S. embassies in Kenya and Tanzania, the court held that nonresident aliens interrogated abroad and subsequently tried within the United States were entitled to the Fifth Amendment right against self-incrimination.[137] The court drew on *Verdugo-Urquidez*'s distinction between *where* and *when* Fourth and Fifth Amendment violations occur.[138] Citing *Verdugo-Urquidez*, the court reasoned that unlike a Fourth Amendment violation, which requires "an analysis of the extraterritorial application of the Fourth Amendment," "[n]o such analysis is necessary" for asserted violations of the right against self-incrimination, because "that provision governs the admissibility of evidence at U.S. trials, not the conduct of U.S. agents investigating criminal activity."[139] Accordingly, "regardless of the origin—*i.e.,* domestic or foreign—of a statement, it cannot be admitted at trial in the United States if the statement was 'compelled,'" whether or not the defendant is a U.S. citizen.[140]

* * *

A nonresident alien subject to an unlawful NIT search might draw from this precedent to assert a Fourth Amendment challenge, notwithstanding the Court's doctrines limiting application of the Constitution's provisions to nonresident aliens. Pursuit of this challenge, however, would depend on whether the court defines the situs of the NIT search by the location of the relevant government server or investigating officer (within the United States), rather than of the targeted device or data (abroad).

A NIT search target facing prosecution may move to suppress evidence obtained from an unlawful search under the Fourth Amendment's

---

Arellanes, No. CR-11-00150-004-TUC-DCB (BPV), 2019 WL 417039, at *2 (D. Ariz. Jan. 31, 2019) (denying Osorio-Arellanes's motion to suppress on finding that the defendant "did in fact speak with [his attorney] privately and did in fact answer questions upon the advice and with the assistance of [his attorney]"); *Osorio-Arellanes*, No. CR-11-00150-004-TUC-DCB (BPV), 2019 WL 357933, at *5–6 (holding the government violated Osorio-Arellanes's right to counsel by seeking to interrogate him after he had "invoked his constitutional right to counsel" but "before such counsel was made available to him").

135. See supra notes 119, 131 and accompanying text.

136. See supra notes 114–118 and accompanying text.

137. *In re Terrorist Bombings*, 552 F.3d at 201.

138. Id. at 199; see also supra text accompanying note 119.

139. *In re Terrorist Bombings*, 552 F.3d at 199.

140. Id. (quoting U.S. Const. amend. V).

exclusionary rule.[141] Courts may be particularly sympathetic to claims arising from watering-hole attacks, which execute without law enforcement's knowledge of a target's citizenship or the location of the device or data, such that law enforcement officers cannot tailor the legal process they pursue based on these distinctions. As courts may note, any unlawful watering-hole attack would harm both nonresident aliens, who are unable to raise Fourth Amendment claims for searches said to occur abroad, and U.S. citizens, who may. Courts might conclude that a suppression motion raised by a nonresident alien would serve what the Court has defined as the exclusionary rule's singular goal—deterring officer misconduct.[142]

In turn, nonresident aliens subject to an unlawful NIT search but not facing prosecution might assert a civil *Bivens* action against the federal officers who executed the search. In *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, the Court recognized an implied private right of action for money damages arising under the Constitution for alleged violations by federal officers.[143] In the 1971 opinion, the Court held that petitioner Webster Bivens could pursue a claim for money damages against Federal Bureau of Narcotics agents to enforce the Fourth Amendment.[144] The Court extended *Bivens* in *Davis v. Passman* (1979)[145] and *Carlson v. Green* (1980)[146] to recognize implied rights of action under the Fifth Amendment's Due Process Clause and the Eighth Amendment's prohibition against "cruel and unusual punishments." In the decades since, however, the Court has effectively cabined *Bivens* actions to the factual circumstances of these three cases.[147]

---

141. See Anna C. Henning, Cong. Rsch. Serv., R40189, *Herring v. United States*: Extension of the Good-Faith Exception to the Exclusionary Rule in Fourth Amendment Cases 2–3 (2009), https://fas.org/sgp/crs/misc/R40189.pdf [https://perma.cc/32UL-UEK5] (outlining the Fourth Amendment exclusionary rule).

142. See Davis v. United States, 564 U.S. 229, 236–37 (2011) ("The [exclusionary] rule's sole purpose, we have repeatedly held, is to deter future Fourth Amendment violations."); see also Daskal, The Un-Territoriality of Data, supra note 14, at 383–84 (arguing that "if a warrant based on probable cause is required to collect the content of electronic communications," this requirement should presumptively apply to citizens and noncitizens "irrespective of the location of the data or the target").

143. 403 U.S. 388, 397–98 (1971); see also James E. Pfander & David Baltmanis, Rethinking *Bivens*: Legitimacy and Constitutional Adjudication, 98 Geo. L.J. 117, 118, 125–26 (2009) (summarizing *Bivens* and critiquing the Court's subsequent "willingness to analyze the existence of a *Bivens* action on a case-by-case basis," an approach that "introduces a layer of uncertainty into constitutional litigation").

144. *Bivens*, 403 U.S. at 389–90, 397–98.

145. 442 U.S. 228, 248–49 (1979) (holding that a female congressional assistant has a cause of action for damages against a former congressman for alleged gender discrimination in violation of the Fifth Amendment's Due Process Clause).

146. 446 U.S. 14, 23–25 (1980) (extending a *Bivens* action to the estate of deceased incarcerated person Joseph Jones, Jr., for the alleged failure of federal prison officials to afford adequate medical care in violation of the Eighth Amendment).

147. See Whitney K. Novak, Cong. Rsch. Serv., LSB10500, Regulating Federal Law Enforcement: Considerations for Congress 2–3 (2020), https://crsreports.congress.gov/

Notwithstanding this contraction, a *Bivens* remedy may remain available in jurisdictions that define the situs of a NIT search by the location of the government server or investigating officer. This definition would classify the alleged Fourth Amendment violation as domestic even if the device or data searched is located abroad, such that the claim could proceed as a "classic *Bivens*-style tort."[148]

A nonresident alien's pursuit of a Fourth Amendment suppression motion or *Bivens* action would, however, depend on the reviewing court's jurisdictional definition—not on normatively consistent constitutional rationales.[149] Indeed, though defining the situs by the location of the government server or law enforcement officer may facilitate a Fourth Amendment challenge, defining the situs by the device or data would preclude one.

III. A LEGAL FRAMEWORK FOR LAW ENFORCEMENT HACKING

As Part II offers, jurisdiction-specific definitions of the situs of a NIT search may implicate nonresident aliens' ability to pursue remedies for Fourth Amendment harms. Though individual courts may account for this consideration, because one NIT search may deploy across judicial districts or indeed beyond the United States, this Note argues that one definition should govern.

---

product/pdf/LSB/LSB10500 [https://perma.cc/MN5K-YAMS]; Alexander A. Reinert, Measuring the Success of *Bivens* Litigation and Its Consequences for the Individual Liability Model, 62 Stan. L. Rev. 809, 835–45 (2010) (drawing on data from cases filed in five federal district courts from 2001–2003 and finding that the success rate of *Bivens* suits is "substantially less than the success rate reported for nonprisoner constitutional tort lawsuits").

148. See Reply Brief for Petitioners at 1, Hernandez v. Mesa, 140 S. Ct. 735 (2020) (No. 17-1678), 2019 WL 5542990, at *1 (internal quotation marks omitted) (quoting Sutton v. United States, 819 F.2d 1289, 1293 (5th Cir. 1987)) (arguing that unlike the "nine merits rulings [since *Carlson v. Green* that] have declined to recognize a damages remedy under *Bivens*," *Hernandez* involves a "classic *Bivens*-style tort, in which a federal law enforcement officer uses excessive force, contrary to the Constitution or agency guidelines" (internal quotation marks omitted) (quoting *Sutton*, 819 F.2d at 1293)); see also Kelsey Y. Santamaria, Cong. Rsch. Serv., LSB10361, *Bivens* at the Border: Supreme Court to Consider Whether Cross-Border Shooting Case Can Proceed 2 (2019), https://crsreports.congress.gov/product/pdf/LSB/LSB10361/2 [https://perma.cc/C9LL-4CHH].

149. For a discussion of two leading theories on the extraterritorial application of the Constitution's provisions—the "compact theory" and "organic theory"—see Cabranes, supra note 108, at 1665–67 ("Under the compact theory, the procedural safeguards set forth in the Constitution for the domestic investigation and prosecution of individuals have no force abroad."); id. at 1667–69 (noting that supporters of the organic theory "contend that government action is legitimate only insofar as it conforms to all legal restraints applicable domestically, including the fundamental law of our country set forth in the Constitution").

A. *A Legislative Approach*

This Note proposes that Congress standardize the situs of NIT searches as part of a comprehensive bill regulating law enforcement's use of these remote search techniques. This definition would draw from Federal Rule of Criminal Procedure 41(b)(6)(A) and from circuit courts' interpretation of the situs of a wiretap under the federal Wiretap Act.[150]

1. *Why Legislation.* — Commentators have long called for statutory regulation of NIT searches.[151] Yet the hyperpartisanship and political gridlock that have beset contemporary politics and given rise to "unorthodox lawmaking" cast doubt on the prospect of congressional action or legislation that would follow committee deliberation and stakeholder input.[152] Indeed, Congress passed the CLOUD Act—the most recent significant measure regulating law enforcement access to electronic communications—as an attachment to an omnibus spending bill.[153]

Moreover, legislation may aggravate the very privacy and civil liberties concerns that lawmakers might aim to address. For example, scholars of the Wiretap Act have argued that Congress has failed to amend the Act to

---

150. Nearly a decade ago, scholar Susan Brenner suggested that courts might draw from circuit precedent governing cross-border wiretaps to define the situs of a remote data search. See Susan W. Brenner, Law, Dissonance, and Remote Computer Searches, 14 N.C. J.L. & Tech. 43, 66 n.107 (2012).

151. See, e.g., Mayer, supra note 7, at 641–43 (advocating for statutorily defined heightened warrant requirements for law enforcement use of malware); Kevin Bankston, Ending the Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors, Lawfare (June 14, 2017), https://lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors [https://perma.cc/EBS7-LZTE] (advocating for statutory regulation that "would help constrain and minimize the privacy and security harms that stem from the government's hacking activities without foreclosing constitutional arguments that litigators might raise against the practice"); Andrew Crocker, What to Do About Lawless Government Hacking and the Weakening of Digital Security, Elec. Frontier Found.: Deeplinks Blog (Aug. 1, 2016), https://www.eff.org/deeplinks/2016/08/what-do-about-lawless-government-hacking-and-weakening-digital-security [https://perma.cc/FNE6-E6KP] (suggesting a "Title III for Hacking" to regulate law enforcement's use of malware, akin to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Act) regulating wiretaps).

152. See Nathaniel Persily, Solutions to Political Polarization in America 4 (2015) (defining hyperpartisanship, gridlock, and incivility and identifying them as "three separate but interacting phenomena [that] fall within the ambit of 'polarization'"); Barbara Sinclair, Unorthodox Lawmaking: New Legislative Processes in the U.S. Congress 256 (2016) ("Some previously unusual practices, such as significant party leadership involvement at the prefloor stage, have become standard but, overall, variety, not uniformity, characterizes the contemporary legislative process."); Walter J. Oleszek, Cong. Rsch. Serv., R46597, The "Regular Order": A Perspective 4–5 (Nov. 6, 2020), https://fas.org/sgp/crs/misc/R46597.pdf [https://perma.cc/WL8Q-L2JS] (describing the transition in lawmaking from committee-oriented processes involving bipartisan compromise to party-centric, nontraditional procedures).

153. See David Ruiz, Responsibility Deflected, the CLOUD Act Passes, Elec. Frontier Found.: Deeplinks Blog (Mar. 22, 2018), https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes [https://perma.cc/WA82-626N].

keep pace with evolving technology and law enforcement operations,[154] and that courts have variably enforced the Act's provisions that are meant to be privacy protective, such as those requiring necessity, minimization, and notice.[155] On a fundamental level, codifying wiretapping may have contributed to the routinization of this investigative tool—originally largely limited to national-security and organized-crime investigations—perhaps because legislation lent legitimacy to the practice.[156]

Notwithstanding these political process obstacles and practical consequences, legislation is uniquely able to regulate and lend transparency[157] to operations that are now firmly within law enforcement's toolkit.[158] Similar to the SCA, which Congress enacted to constrain law enforcement operations that exceeded the Fourth Amendment's ambit,[159] legislation would regulate NIT searches that, in certain jurisdictions, would not implicate the Fourth Amendment.[160] Even when the Fourth Amendment is implicated, legislation may introduce more stringent privacy-protective provisions than those afforded by the Fourth Amendment floor.

---

154. See, e.g., Eldar Haber, The Wiretapping of Things, 53 U.C. Davis L. Rev. 733, 740–44 (2019) (noting that the 2005 expansion of the Communications Assistance for Law Enforcement Act, which itself amended the Wiretap Act, "could indicate a moment when policymakers ceased to further regulate access to communication for regular law enforcement purposes (not accounting for national security)").

155. See Jennifer S. Granick, Patrick Toomey, Naomi Gilens & Daniel Yadron, Jr., Mission Creep and Wiretap Act "Super Warrants": A Cautionary Tale, 52 Loy. L.A. L. Rev. 431, 433, 447–56 (2019) (finding that "[c]ourts of appeals . . . have not applied the necessity requirement to require a showing that all possible alternatives have failed or are not reasonably likely to succeed" and that "courts have generally set a low bar in terms of what minimization requires").

156. See id. at 433–34, 446–47 ("Though intended to provide a set of strong privacy protections that would limit wiretapping . . . Title III legitimized a practice that President Lyndon B. Johnson, many lawmakers, and the ACLU wanted to outlaw in all but the most sensitive national security investigations."); Susan Landau, National Security on the Line, 4 J. Telecomms. & High Tech. L. 409, 416–17 (2006) (noting that "the balance [between law enforcement and civil liberties] has shifted some in the direction of law enforcement," as seen through the expansion of the number of predicate crimes subject to a wiretap order from "the original twenty-six in Title III to just under a hundred today").

157. See Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 859 (2004) (arguing that "[t]he context of legislative rule-creation offers significantly better prospects for the generation of balanced, nuanced, and effective investigative rules involving new technologies"); Crocker, supra note 151 (arguing "the government shouldn't engage in 'policy by blog post,'" for "[g]overnment action that actively sabotages or even collaterally undermines digital security is too important to be left open to executive whim"). But see Daniel J. Solove, Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference, 74 Fordham L. Rev. 747, 773 (2005) (arguing that "[t]he answer to the problem of creating rules to regulate law enforcement and new technologies is not to call for judicial caution and leave it to legislatures to draft the primary law," but "simply to craft better rules").

158. See supra notes 30–32 and accompanying text.

159. See supra note 44.

160. See supra notes 45–46 and accompanying text.

2. *Proposed Definition: Drawing from Rule 41(b)(6) and the Wiretap Act.* — This Note proposes embracing approaches tied to (1) the target device or data, and (2) the law enforcement officer executing the search. When law enforcement knows the location of the device or data prior to executing the remote search, this location would govern—consistent with the Fourth Amendment's traditionally territorial framework. Alternatively, when the device or data's location has been concealed, the proposed definition would draw from the jurisdictional limitation set forth in Rule 41(b)(6). The situs would be the location of the law enforcement officer executing the search, provided the officer is located in a district in which activities related to the crime under investigation may have occurred.

By statutorily empowering magistrate judges to issue warrants for extra-district NIT searches, this Note's proposed definition would qualify as a "law" under the Federal Magistrates Act—codifying Rule 41(b)(6)(A) and thereby setting it on firm legal terrain.[161] The proposed definition may also shape (though it would not preempt) a court's independent analysis of a nonresident alien's Fourth Amendment claim.[162]

This proposal for alternate definitions draws from the judicially defined dual locations of a wiretap under the Wiretap Act.[163] Like NIT searches, wiretaps of in-transit electronic communication also feature the phenomenon of location independence. Law enforcement officers executing a wiretap may be separated from the phone tapped, the "listening post" where officers first hear the contents of the intercepted communication, and the suspect.[164]

Congress passed the Wiretap Act in 1968, one year after the Court held that a wiretap constituted a Fourth Amendment search in *Katz v. United States*.[165] Through the Act, Congress built on the Court-developed Fourth Amendment baseline, introducing a "statutory right of privacy in 'aural' communications" and expanding the regulated parties to include

---

161. See supra section II.A.

162. See supra section II.B.2.

163. See United States v. Cano-Flores, 796 F.3d 83, 86–87 (D.C. Cir. 2015); United States v. Henley, 766 F.3d 893, 911–12 (8th Cir. 2014); United States v. Luong, 471 F.3d 1107, 1109–10 (9th Cir. 2006); United States v. Ramirez, 112 F.3d 849, 852 (7th Cir. 1997); United States v. Denman, 100 F.3d 399, 402–04 (5th Cir. 1996); United States v. Rodriguez, 968 F.2d 130, 135–36 (2d Cir. 1992). The Supreme Court has recognized but not issued a holding on this definition. See Dahda v. United States, 138 S. Ct. 1491, 1495 (2018) ("The Government here adds (without [petitioners'] disagreement) that an intercept takes place *either* where the tapped telephone is located *or* where the Government's 'listening post' is located." (citing 18 U.S.C. § 2510(4) (2018))).

164. See Brenner, supra note 150 (distinguishing traditional searches in which "the searchers and the target(s) of the search are necessarily physically proximate" from remote data searches, for which "physical proximity is no longer inevitable").

165. Katz v. United States, 389 U.S. 347, 353 (1967); see also Granick et al., supra note 155, at 439.

not only federal law enforcement but also state officials and nongovernment entities.[166]

Section 2518(3) of the Wiretap Act authorizes a district court judge to issue an order "authorizing or approving *interception* of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting" upon receipt of an application establishing probable cause and satisfying other privacy-protective provisions.[167] Though Section 2510(4) of the Act defines "intercept,"[168] the Act does not specify where "interception" occurs within the meaning of Section 2518(3).[169] This definition is significant, for the district court may only authorize a Section 2518(3) wiretap in the judicial district(s) of "interception."

Every circuit court to have considered the question has interpreted "intercept" by two locations: the jurisdiction where the "to-be-tapped telephone is located," and where the "contents of the redirected communication are first to be heard."[170] The Second Circuit, which first advanced this interpretation in the 1992 case *United States v. Rodriguez*, reasoned that the dual points would promote the Act's privacy-protective goals, particularly when law enforcement seeks to wiretap phones in several jurisdictions and monitor the tapped phones from one.[171] In such investigations, the court reasoned, uniform rather than diffuse oversight would better constrain law enforcement operations.[172]

As the *Rodriguez* court reasoned with respect to the Wiretap Act, this Note's proposed definition would ensure that the technical variety of NIT searches remain subject to regulation. Unlike the Wiretap Act, the proposed definition would require a showing of connection between the relevant judicial district and the crime under investigation—minimizing the forum shopping concerns that the *Rodriguez* concurrence cautioned would flow from the majority's dual interpretations.[173] Further, this definition

166. See Haber, supra note 154, at 740 (citing the Wiretap Act).

167. 18 U.S.C. § 2518(3) (emphasis added); Granick et al., supra note 155, at 440–41 (summarizing the Act's principal provisions).

168. See 18 U.S.C. § 2510(4) (defining "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device").

169. See, e.g., United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) (noting the absence of this jurisdictional definition).

170. Id.; see also supra note 163 (collecting cases).

171. *Rodriguez*, 968 F.2d at 136.

172. Id.

173. Id. at 143–44 (Meskill, J., concurring) ("If a judge in one district denies authorization, law enforcement officials may simply move their listening posts to another jurisdiction until they find a judge willing to authorize the wiretap."); see also Beryl A. Howell, Seven Weeks: The Making of the USA PATRIOT Act, 72 Geo. Wash. L. Rev. 1145, 1196 (2004) (noting that the USA PATRIOT Act's similar jurisdictional provision "was intended to minimize the risk of forum shopping or centralization of all electronic

would form but one piece of a comprehensive statute meant to regulate remote data searches.

3. *Privacy-Protective Standards.* — Indeed, beyond this jurisdictional provision, legislation should impose constraints on the execution of NIT searches.[174] This Note sets forth focal points for consideration.

First, legislation might impose procedures to limit the breadth of information collected, such as by requiring officers to obtain separate warrants for the collection of non-content and content data.[175] These conditions would add teeth to the Fourth Amendment's particularity requirement in the context of NIT searches.[176] Second, when law enforcement knows that a NIT will deploy onto a device or computer system located abroad, legislation might require officers to secure the consent of qualifying foreign sovereigns before carrying out an extraterritorial search.[177] This would add to longstanding Justice Department guidance that officers may need to provide notice to the relevant foreign sovereign before conducting a search that officers know will reach data stored beyond the United States.[178] An exigency exception could address situations in which this provision would unreasonably constrain investigations.[179]

---

surveillance . . . no matter where the actual criminal activity under investigation was occurring").

174. Ahmed Ghappour, Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, 69 Stan. L. Rev. 1075, 1128–35 (2017) (outlining proposals to govern when, how, and who may execute NIT searches).

175. Emily Berman, Digital Searches, the Fourth Amendment, and the Magistrates' Revolt, 68 Emory L.J. 51, 82–85 (2018) (suggesting that magistrate judges should impose minimization procedures on remote data searches); Crocker, supra note 151 (advocating for legislation governing law enforcement hacking that would impose "strict minimization requirements, so that the targets of hacking are identified with as much specificity as the government can possibly provide").

176. See Benton, supra note 25, at 210 & n.171 (outlining the particularity requirement as applied to digital searches); Mayer, supra note 7, at 620–25 (discussing the doctrine of anticipatory warrants and the challenge of "establishing probable cause of a crime and describing evidence with particularity based solely on a visit to a webpage," as in Operation Pacifier).

177. Jennifer Daskal, Transnational Government Hacking, 10 J. Nat'l Sec. L. & Pol'y 677, 700 (2020) (advocating that countries, including the United States, adopt this requirement "as a default rule and matter of domestic law").

178. See H. Marshall Jarrett, Michael W. Bailie, Ed Hagen & Nathan Judish, Exec. Off. for U.S. Att'ys, Off. of Legal Educ., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 85 (3d ed. 2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [https://perma.cc/688J-R29D].

179. See Daskal, Borders and Bits, supra note 16, at 230; Memorandum from David Bitkower, Deputy Assistant Att'y Gen., Crim. Div., DOJ, to Reena Raggi, Chair, Advisory Comm. on Crim. Rules (Oct. 20, 2014), *in* Advisory Committee on Criminal Rules: Orlando, FL, March 16–17, 2015, at 133, 135, https://www.uscourts.gov/sites/default/files/fr_import/CR2015-05.pdf [https://perma.cc/R3WW-FTAL] (arguing against the imposition of "unnecessary and unworkable restrictions on remote search authority in [Federal Rule of Criminal Procedure] 41, such as a requirement to search only for 'country information'").

Finally, legislation might authorize the Justice Department to enter into bilateral or multilateral agreements with qualifying foreign nations—agreements that would set ground rules for government-executed malware searches.[180] Legislators provided for executive agreements in the CLOUD Act, the amendment to the SCA that regulates cross-border compelled disclosure orders.[181] As of February 2021, the executive branch has concluded one CLOUD Act agreement with the United Kingdom[182] and announced formal negotiations with the European Union and Australia.[183] Although the process of concluding bilateral or multilateral agreements regarding government-led malware searches is likely to be protracted and complex, a provision calling for this sort of cooperation would signal the United States' regard for foreign sovereign interests.

B. *Reconsidering the Fourth Amendment's Reach*

Though this proposed definition may lay the groundwork for nonresident aliens to assert Fourth Amendment claims, litigants would remain bound by the Court's precedent conditioning the Fourth Amendment's reach on territorial- and citizenship-driven distinctions.[184] It is beyond the scope of this Note to examine how NIT searches complicate the compact theory of constitutional extraterritoriality as embodied in the Court's case law.[185] This Note offers, however, that NIT searches constrain the normative rationales underpinning the theory, for extra-district NIT searches could be said to occur within or beyond the United States. This Note further urges a shift toward noncategorical application of the compact theory with respect to NIT searches. Courts may do so by analyzing NIT searches

---

180. Cf. Secil Bilgic, Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act, 32 Harv. J.L. & Tech. 321, 347–51 (2018) (arguing the CLOUD Act will accelerate foreign states' adoption of data localization laws that jeopardize foreign citizens' privacy interests).

181. See 18 U.S.C. § 2523 (2018); supra note 26 and accompanying text.

182. Press Release, DOJ, U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online (Oct. 3, 2019), https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists [https://perma.cc/HA3J-HHPH].

183. Press Release, DOJ, Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton (Oct. 7, 2019), https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us [https://perma.cc/BCC9-75NR]; Press Release, DOJ, Joint U.S.–E.U. Statement on Electronic Evidence Sharing Negotiations (Sept. 26, 2019), https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations [https://perma.cc/2U3V-NJPP].

184. See supra section II.B.1.

185. See Cabranes, supra note 108, at 1665–67 (elaborating on the compact theory).

under *Boumediene*'s functionalist test, rather than *Verdugo-Urquidez*'s "substantial connections" analysis.[186]

NIT searches do not present the functional concerns that had animated Justice Kennedy's concurrence in *Verdugo-Urquidez*.[187] Unlike the search considered in *Verdugo-Urquidez*, law enforcement would not need to obtain a NIT search warrant from a foreign judge.[188] Further, Justice Department protocol advising law enforcement to consider foreign sovereign interests[189] would minimize the concern of "the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials."[190] Indeed, just as Kennedy would later conclude as to the Suspension Clause in *Boumediene*, there would be "few practical barriers" to extending the Fourth Amendment's reasonableness requirement to NIT searches.[191]

CONCLUSION

Litigation stemming from law enforcement's execution of NIT searches has highlighted federal courts' divergent definitions of the situs of a NIT search. As this Note argues, the jurisdictional definition has implications for the legality of NIT searches and the constitutional remedies available to nonresident alien search targets. This Note urges Congress to define the situs of a NIT search as part of legislation setting the contours of and imposing constraints on NIT searches.

Though the proposed legislation would lend consistency to judicial process governing NIT searches, it would not modify the Supreme Court's doctrines restricting the Fourth Amendment's extraterritorial reach. This Note concludes by suggesting that courts assess Fourth Amendment claims by nonresident alien search targets under *Boumediene*'s functionalist framework, rather than *Verdugo-Urquidez*'s substantial connections test.

186. Boumediene v. Bush, 553 U.S. 723, 770–71 (2008); United States v. Verdugo-Urquidez, 494 U.S. 259, 271–75 (1990); see also supra section II.B.1.

187. See Cabranes, supra note 108, at 1707–08.

188. See supra text accompanying note 124.

189. See supra note 178 and accompanying text.

190. *Verdugo-Urquidez*, 494 U.S. at 278 (Kennedy, J., concurring).

191. *Boumediene*, 553 U.S. at 770–71.