VOL. 121 NO. 4

• NOTE •

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.

The full text of this Note can be found by clicking the PDF link to the left.

* 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 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 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]

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.

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 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.

435 West 116th Street New York, NY 10027
tel: (212) 854-4398