THE NEW RULE 41: RESOLVING VENUE FOR ONLINE CRIMES WITH UNKNOWN LOCATIONS

Julianna Coppage[*]

CITE AS: 1 GEO. L. TECH. REV. 228 (2017)
https://perma.cc/VK73-Z9EN

INTRODUCTION

On December 1, 2016, Rule 41 of the Federal Rules of Criminal Procedure, which governs the procedures regarding issuances of search warrants, was amended in two critical ways.[1] The amendments remove venue restrictions in two narrow situations, authorizing magistrate judges to issue warrants for remote searches of electronic storage media when (A) the location of the electronic media "has been concealed through technological means" or (B) the investigation pertains to botnets that have damaged computers "without authorization" in violation of the Computer Fraud and Abuse Act[2] and the damaged computers "are located in five or more districts."[3] The amendments mark the end of a three-year review process of the proposals, which culminated with the adoption of the new rules by the U.S. Supreme Court in April 2016.[4]

[*] GLTR Staff Member; Georgetown Law, J.D. expected 2018; Barnard College, B.A. 2012. © 2017, Julianna Coppage.

[1] Susan Hennessey, *Rule 41: Resolving Procedural Debates to Face the Tough Questions on Government Hacking*, LAWFARE (Dec. 1, 2016, 2:38 PM), https://www.lawfareblog.com/rule-41-resolving-procedural-debates-face-tough-questions-government-hacking [https://perma.cc/62JR-ZXCW].

[2] 18 U.S.C. § 1030.

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

[4] Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, U.S. DEP'T OF JUSTICE (June 20, 2016), https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches [https://perma.cc/X855-EP63]. The review process occurred pursuant to the Rules Enabling Act, which grants the Supreme Court authority to promulgate rules of procedure for federal courts and designates subcommittees that consider the proposed

Critics of the amendments argue they amount to sweeping substantive changes that dramatically increase the investigative power of the government and weaken individual privacy and security protections.[5] Proponents of the change insist that the amendments merely close a procedural loophole that enabled nationwide crimes to elude the jurisdiction of any court.[6] Each provision will be subsequently examined in light of its stated purpose, critical response, and likely overall effect. Because the amendments close a procedural loophole without altering underlying substantive law, the scope of the amendments is appropriately narrow to meet its corrective function.

BACKGROUND

The amendments authorize magistrate judges to issue warrants for the government to use "*remote access* to search electronic storage media."[7] This kind of search is accomplished using a "Network Investigative Technique" ("NIT").[8] The government defines a NIT as a set of computer instructions that augments the content a user requests from a website.[9] When delivered successfully back to the computer with the requested content, the NIT gathers limited, specified identifying information from that computer and relays it back to a government-controlled server.[10] This typically occurs without the knowledge of the host computer's operator.[11] Opponents decry the use of the

rules and accept public comment before issuing a recommendation on the adoption of the rule to the Supreme Court. Susan Hennessey, *The Lorax of the Rules Enabling Act: How Not to Stop Mass Hacking*, LAWFARE (Sept. 16, 2016, 11:25 AM), https://www.lawfareblog.com/lorax-rules-enabling-act-how-not-stop-mass-hacking [https://perma.cc/N4SV-4TZC].

[5] *See* Rainey Reitman, *With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government*, ELEC. FRONTIER FOUND. (Apr. 30, 2016), https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government [https://perma.cc/VZW6-WJN4]; *see also* Leslie R. Caldwell, *Additional Considerations Regarding the Proposed Amendments to the Federal Rules of Criminal Procedure*, U.S. DEP'T JUSTICE (Nov. 28, 2016), https://www.justice.gov/archives/opa/blog/additional-considerations-regarding-proposed-amendments-federal-rules-criminal-procedure [https://perma.cc/CW6T-R6WZ].

[6] *See* Leslie R. Caldwell, *Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation*, U.S. DEP'T JUSTICE (Nov. 21, 2016), https://www.justice.gov/archives/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation [https://perma.cc/74CJ-GARS].

[7] FED. R. CRIM. P. 41(b)(6) (emphasis added).

[8] *See* Playpen Search Warrant, 2:15-cr-00274-MJP, ECF No. 48-1, 23-30.

[9] *Id.* at 24.

[10] *Id.*

[11] *See, e.g., id.*, at 27-28 (requesting delayed notice to affected users).

term NIT as pure semantics and insist the tool used by the government is malware.[12] Privacy advocates maintain the use of such tools amounts to the U.S. government hacking computers of individuals around the world.[13] For the purposes of this article, the term NIT will be used.[14]

AMENDMENTS

The revised Rule 41b(6) has two provisions; the first pertains to searches of electronic media when the location of that media was concealed through technological means, and the second regards venue provisions for botnet investigations.

Concealing Location Through Technological Means

This provision is designed to facilitate the government's investigation of serious crimes that, due to increasingly advanced anonymization techniques, otherwise elude prosecution.[15] Particularly, the government has used NITs to pierce the veil of websites hosted on hidden services using Tor.[16] Sites that use this functionality can hide the locations of the website's host and users.[17] This technology is abused by tens of thousands of criminals; investigators readily locate websites devoted to criminal activity, many of which involve sexual abuse of children, but because of the technology, the investigators have no ability to identify the people involved.[18]

[12] *See The Playpen Cases: Frequently Asked Questions*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions (last visited Feb. 21, 2017) [https://perma.cc/PVT9-AHCS] (discussing this debate in subsections entitled "Why does the U.S. government want to use the term NIT instead of malware or hacking?" and "Is a NIT a type of malware?").

[13] *See* Mark Rumold, *The Playpen Story: Rule 41 and Global Hacking Warrants*, ELEC. FRONTIER FOUND. (Sept. 26, 2016), https://www.eff.org/deeplinks/2016/08/illegal-playpen-story-rule-41-and-global-hacking-warrants [https://perma.cc/D94T-3RQX].

[14] The debate over the mechanisms of NITs is beyond the scope of this article. For a useful overview, see Susan Hennessy & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE (July 28, 2016 10:17 AM), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques [https://perma.cc/46QQ-YV68].

[15] *See* Caldwell, *supra* note 6.

[16] *See* Hennessey & Weaver, *supra* note 14.

[17] *See id.*

[18] *See* Caldwell, *supra* note 6.

The government has increasingly used NITs to target Tor users trafficking in child pornography, such as the recent Playpen cases.[19] In these cases, the government took over the server that hosted the child pornography site named "Playpen," physically moved the server to the Eastern District of Virginia, obtained a search warrant from a magistrate judge in the Eastern District of Virginia authorizing the use of a NIT, and deployed the NIT on all users that accessed certain sub-forums on the Playpen website over the course of a two-week period.[20] The sting has resulted in hundreds of prosecutions and the rescue of at least forty-nine children from sexual abuse.[21]

The Playpen prosecutions have encountered a large number of motions to suppress the search warrant used, however, because the warrant was issued under the previous version of Rule 41, which did not lift the venue restrictions for such prosecutions.[22] Many courts have found at least a technical violation of Rule 41 because the magistrate judge in the Eastern District of Virginia did not possess the authority to authorize a search in a district outside of her own, and at least one court even held the search warrant wholly invalid.[23] Such rulings necessarily present a catch-22, however, because the government cannot ascertain the location of the users without the NIT, but they cannot use the NIT without seeking authority based on probable cause from a federal judge.[24] Rule 41 helps prevent forum shopping and ensures that judges only issue warrants for crimes located in their districts.[25] However, because in this case the location of the targets were unknown and the crimes occurred online outside of any territorial bounds, the older venue provision of Rule 41 created confusion as to whether *any* judge could issue a warrant.[26]

Critics of the amendment claim this is a substantive, not procedural, change, and as such, it is better left to Congress.[27] Critics further maintain that the rule authorizes government hacking, and as such should be approved by a full body of democratically elected representatives rather than by an "obscure"

[19] *Id.*

[20] *See* Hennessey & Weaver, *supra* note 14.

[21] Caldwell, *supra* note 6.

[22] *See* Hennessey, *supra* note 4.

[23] *See, e.g.*, *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016).

[24] *See* Hennessey, *supra* note 1.

[25] Rumold, *supra* note 13.

[26] Caldwell, *supra* note 6.

[27] *See* Reitman, *supra* note 5.

committee.[28] Two senators opposed the rule, but their measures to stop the adoption of the change gained no traction.[29]

Proponents of the new rule dispute this characterization, insisting that the change only allows the search warrant applications to be heard by a judge and does not change substantive Fourth Amendment jurisprudence.[30] Indeed, the Advisory Committee comments to this rule change reiterated that position, stating that "[t]he amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media or seizing or copying electronically stored information, leaving the application of this and other constitutional standards to ongoing case law development."[31]

Botnet Investigations

The second part of the amendment is specifically targeted to provisions of the Computer Fraud and Abuse Act that prohibit programmed viruses that infiltrate victims' computers without permission.[32] This rule change was designed to counteract the particular problem of botnets, which the Department of Justice defines as "essentially a mass hack—a network of victim computers that have been surreptitiously infected with malware and are controlled remotely by criminals."[33] Botnets cause a variety of problems, ranging from installing keystroke logging software on a victim's computer to utilizing victim computers to carry out a distributed denial of service ("DDoS") attack.[34] Botnets are widespread and malicious, often hiding in plain sight, which makes dismantling them incredibly tricky.[35]

Investigating botnets and prosecuting developers can be even more difficult. The first step in investigating botnets is often identifying infected

[28] *Id.*

[29] *See* Hennessey, *supra* note 1; *see also* Jeff John Roberts, *FBI's New Hacking Powers Take Effect This Week*, FORTUNE (Nov. 30, 2016), http://fortune.com/2016/11/30/rule-41/ [https://perma.cc/U4ZK-A2XX].

[30] *See* Caldwell, *supra* note 6.

[31] FED. R. CRIM. P. 41 advisory committee's note to 2016 amendment.

[32] *See* 18 U.S.C. § 1030(a)(5).

[33] Leslie R. Caldwell, *Ensuring Botnets Are Not "Too Big to Investigate"*, U.S. DEP'T JUSTICE (Nov. 22, 2016) https://www.justice.gov/archives/opa/blog/ensuring-botnets-are-not-too-big-investigate [https://perma.cc/3C3Y-Y6SS].

[34] *Id.*

[35] *See id.*; *see also* Nathan Judish, Senior Counsel, U.S. Dep't of Justice, Deb. at Georgetown Univ. Law Ctr. Edge Techs. Legal Stud. Colloquium: Network Investigative Techs. (Jan. 25, 2017).

computers.[36] To do so, the government frequently needs to obtain a search warrant to gain identifying information about those computers.[37] However, these are typically nationwide investigations that span multiple judicial districts.[38] Under the previous version of Rule 41, the government would have to simultaneously apply for and be granted a search warrant in all ninety-four judicial districts in the United States to successfully run a botnet investigation.[39] This is logistically absurd and practically infeasible. The amended Rule 41 allows an investigator to apply for a search warrant from a single magistrate judge when investigating a botnet that targets computers in more than five judicial districts.[40]

This change angers privacy advocates, who argue that hacking victims' computers falls well outside the powers delegated to the executive branch. [41] They contend the change at minimum conveys an implicit approval of government hacking, which is inappropriate for the limited jurisdiction of the rules committee that approved the change.[42] They also contend that the techniques used for such investigations could cripple or permanently damage a victim's computer, causing even greater harm than the botnet itself.[43] A tool with a capability for such damage to innocent victims should not be legalized without the public debate afforded by Congressional hearings, according to these privacy advocates. [44]

Such arguments, though they may reflect legitimate concerns, seem conceptually misplaced in the Rule 41 debate. The rules committee noted a similar problem, finding that "much of the opposition [to the changes] reflected a misunderstanding of the scope of the proposal. The proposal addresses venue; it does not itself create authority for electronic searches or alter applicable statutory or constitutional requirements."[45] While the wisdom and legality of such tactics may be hotly contested, the fact that there should exist *a* court in the country that can authorize the investigation of these crimes

[36] Judish, *supra* note 35.
[37] Caldwell, *supra* note 33.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *See* Reitman, *supra* note 5 (arguing that the Rule 41 changes amount to expanding executive authority, a role belonging solely to Congress).
[42] *See id.*; *see also* Mark Rumold, Senior Staff Attorney, Elec. Frontier Found., Deb. at Georgetown Univ. Law Ctr. Edge Techs. Legal Studs. Colloquium: *Network Investigative Techniques* (Jan. 25, 2017).
[43] Rumold, *supra* note 42. *Accord* Reitman, *supra* note 5.
[44] Reitman, *supra* note 5.
[45] Caldwell, *supra* note 5.

seems to be ignored. That is all the text of the new Rule 41 allows, and all that it can allow. The legality of the investigative techniques is still a matter for Congress and the courts and will continue to be litigated. In the meantime, though, a procedural loophole that enabled criminals to escape the jurisdiction of any American court has been closed.