Maryland Law Review

Volume 76 | Issue 4 Article 8

Rule 41 Amendments Provide for a Drastic Expansion of Government Authority to Conduct Computer Searches and Should Not Have Been Adopted by the Supreme Court

Markus Rauschecker

RULE 41 AMENDMENTS PROVIDE FOR A DRASTIC EXPANSION OF GOVERNMENT AUTHORITY TO CONDUCT COMPUTER SEARCHES AND SHOULD NOT HAVE BEEN ADOPTED BY THE SUPREME COURT

MARKUS RAUSCHECKER*

INTRODUCTION

Advances in technology have created gaps in the law that hinder the capabilities of law enforcement to conduct its investigations and prosecute criminals. Prior to December 1, 2016, such a gap existed in Rule 41 of the Federal Rules of Criminal Procedure.[1] As it was written, the Rule contained a territorial limitation on a magistrate judge's ability to issue a search warrant and limited law enforcement's ability to successfully apply for search warrants targeting internet-connected computers.[2] With a few exceptions, magistrate judges were authorized to issue warrants only when the warrant was to be executed within the judge's district.[3] This territorial limitation presented a problem for law enforcement as more and more online users began employing technological tools to hide their locations.[4] When law enforcement was unable to clearly identify the location of a computer it wanted to

* Markus Rauschecker, J.D., University of Maryland Francis King Carey School of Law, is the University of Maryland Center for Health and Homeland Security's Cybersecurity Program Manager, where he focuses on legal and policy issues in cybersecurity. Mr. Rauschecker has been published in various outlets and been called upon by professional organizations to present at seminars and conferences. He has provided testimony on cybersecurity issues to numerous government bodies at the federal, state, and local levels. Mr. Rauschecker is also an adjunct faculty member at the University of Maryland Francis King Carey School of Law, where he teaches "Law and Policy of Cybersecurity" and "Law and Policy of Cyber Crime" to J.D., LL.M., and Masters of Science in Law students.

1. *Compare* FED. R. CRIM. P. 41(b), *with* FED. R. CRIM. P. 41(b), 18 U.S.C. app. (2012) (amended 2016).

2. FED. R. CRIM. P. 41(b), H. COMM. ON THE JUDICIARY, 113TH CONG., FEDERAL RULES OF CRIMINAL PROCEDURE 52–53 (Comm. Print 2014) (amended 2016).

3. *Id.*

4. Leslie R. Caldwell, Assistant Attorney Gen., U.S. Dep't of Justice, Remarks Highlighting Cybercrime Enforcement at Center for Strategic and International Studies (Dec. 7, 2016), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-highlighting-cybercrime; *see also* Andy Greenberg, *How to Anonymize Everything You Do Online*, WIRED (June 17, 2014, 6:30 AM), https://www.wired.com/2014/06/be-anonymous-online/ (noting that "cryptography has shifted from an obscure branch of computer science to an almost mainstream notion," which makes it possible to hide internet activity).

search, judges were hesitant to issue search warrants, because they were concerned that the computer could be located outside of their district and the warrant would, therefore, run afoul of the territorial limitation of Rule 41.[5]

On April 28, 2016, Chief Justice John Roberts submitted a letter to Congress, giving notice of changes to Rule 41.[6] The change to Rule 41 marked the end of a three-year rulemaking process that included a long period of public comment.[7] Public hearings were held by the Advisory Committee on Federal Rules of Criminal Procedure. The Advisory Committee approved the rule change. The amendments were then unanimously approved by the Standing Committee on Rules and the Judicial Conference, and adopted by the United States Supreme Court.[8] The amendments went into effect on December 1, 2016.[9] The December 1, 2016, amendments to Rule 41 read as follows:

> [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; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.[10]

Proponents of the Rule 41 amendments see the changes as critical to enabling law enforcement to effectively conduct investigations and prosecute criminals in light of new technologies used by these criminals.[11] Presumably, everyone would agree that criminals should be identified and prosecuted, yet

5. *See, e.g.*, *In re* Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753, 757, 761 (S.D. Tex. 2013) (denying a search warrant application because territorial requirements were not met).

6. Letter from John G. Roberts, Chief Justice, U.S. Supreme Court, to Paul D. Ryan, Speaker, U.S. House of Representatives, and Joseph R. Biden Jr., President, U.S. Senate (Apr. 28, 2016), https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf. The Supreme Court has authority to write rules of procedure pursuant to the Rules Enabling Act, which was enacted by Congress in 1934. Rules Enabling Act, Pub. L. No. 73-416, 48 Stat. 1064 (1934) (codified at 28 U.S.C. § 2071–77 (2012)).

7. Letter from Peter J. Kadzik, Assistant Attorney Gen., U.S. Dep't of Justice, to Ron Wyden, Senator, U.S. Senate (Nov. 18, 2016), https://assets.documentcloud.org/documents/3225184/DOJ-Rule-41-Response.pdf.

8. *Id.*

9. Letter from John G. Roberts to Paul Ryan & Joseph Biden, *supra* note 6.

10. FED. R. CRIM. P. 41(B)(6); *see also* Letter from John G. Roberts to Paul Ryan & Joseph Biden, *supra* note 6.

11. *See, e.g.*, 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.

the Rule 41 amendments are concerning in that they provide for a drastic expansion of government authority. Given that the rule changes are not merely procedural, but provide a substantive expansion of government authority to conduct searches, the Supreme Court acted beyond the rulemaking authority granted to it through the Rules Enabling Act. Rather, Congress should have initiated, debated, and enacted these significant changes to Rule 41.

Part I of this Essay discusses the arguments in support of the Rule 41 changes. The changes provide law enforcement with a way to conduct computer searches in light of new technologies used by criminals. Part II discusses arguments against the Rule 41 changes. Opposition to the changes existed in Congress, where Senator Wyden led an effort to prevent the changes from taking effect. The Senator was joined by others arguing that these rule changes are a significant expansion of government authority to conduct searches and Congress should debate these changes. Civil liberties groups also opposed the changes arguing that they provide for a drastic expansion of governmental surveillance powers and jeopardize privacy.

Part III of the Essay provides a closer analysis of the Rule 41 changes. By examining the precise language of the amendments, it becomes evident that the rule changes are vague and do, in fact, substantively expand the government's ability to conduct searches. Furthermore, the rule changes violate the particularity requirement of the Fourth Amendment. Part IV of the Essay discusses likely additional consequences of the rule changes, such as violations of warrant notice requirements, violations of international law, and forum shopping.

I. ARGUMENTS IN SUPPORT OF THE RULE 41 AMENDMENTS

The change to Rule 41 is intended to help law enforcement investigate and prosecute certain computer crimes.[12] The advancement of technology has made it more difficult for law enforcement to conduct its investigations, because it is now difficult to locate search-targeted computers. Calls for amending Rule 41 go back to April 2013, when a judge rejected a federal government remote electronic search warrant application.[13] Prior to the rule change, courts would deny search warrants in cases where the location of the target computer was unknown (except in limited situations), as the target computer may have been located outside of the court's district.[14]

12. Letter from Peter J. Kadzik to Ron Wyden, *supra* note 7.

13. *See In re* Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753, 761 (S.D. Tex. 2013) (denying a search warrant because of Rule 41 concerns and recognizing potential rationale for updating the rule).

14. *See, e.g., id.*

A. In re Warrant to Search a Target Computer at Premises Unknown

The case of *In re Warrant to Search a Target Computer at Premises Unknown*[15] ("*In re Warrant*") illustrates the reasoning for courts' refusals to grant search warrants when the target computers' locations are unknown.[16] In *In re Warrant*, the Government requested a search and seizure warrant pursuant to Rule 41 to target a computer that was allegedly used to violate federal bank fraud, identity theft, and computer security laws.[17] Based on the warrant, the Government sought to install data extraction software on the target computer to collect both metadata and content stored on the computer, such as internet activity, emails, and photographs.[18] The Government, however, did not know the precise location of the target computer, nor could it ensure that only the targeted computer would be affected by the search. According to the court, the Government thereby failed to satisfy the territorial limits of Rule 41, as well as the particularity requirement of the Fourth Amendment.[19] Thus, the court denied the Government's warrant application.[20]

The court's reasoning began with the premise that Rule 41 allows a "magistrate judge with authority in the district . . . to issue a warrant to search for and seize a person or property located within the district."[21] At the time of the *In re Warrant* decision, Rule 41 authorized the issuance of a warrant if the target property was outside of the judge's district in only a few limited circumstances: (1) when the target property "might . . . be moved outside the [court's] district before the warrant [was] executed"; (2) when the target property was part of a terrorism investigation; (3) if the warrant pertained to a tracking device that was installed inside the judge's district, but had been moved outside the judge's district; (4) when "activities related to the crime . . . occurred" in the judge's district, and the target property was located in a United States territory, or on "the premises—no matter who own[ed] them—of a United States diplomatic or consular mission in a foreign state."[22] The *In re Warrant* court reviewed each of these exceptions to the territorial

15. 958 F. Supp. 2d 753.

16. *Id.* at 756–61.

17. *Id.* at 755.

18. *Id.* at 755–56.

19. *Id.* at 757, 759; *see infra* text accompanying note 25 (explaining the Fourth Amendment's particularity requirement).

20. *In re Warrant*, 958 F. Supp. 2d at 755.

21. *Id.* at 757 (quoting FED. R. CRIM. P. 41(b)(1)).

22. FED. R. CRIM. P. 41(b)(2)–(5). The sections of Rule 41 that are cited here were not affected by the 2016 amendments. Letter from John G. Roberts to Paul Ryan & Joseph Biden, *supra* note 6.

limitation of Rule 41 and determined that none applied to the Government's warrant application.[23]

The court then turned to the Fourth Amendment's particularity requirement. The Fourth Amendment prescribes, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[24] In considering the particularity requirement, the court began by stating, "[t]he Government's application contain[ed] little or no explanation of how the Target Computer w[ould] be found."[25] Furthermore, the court argued, "[t]he Government's application offer[ed] nothing but indirect and conclusory assurance that its search technique w[ould] avoid infecting innocent computers or devices . . . ."[26] Because the Government neither showed how it would identify the target computer nor provided assurances that the search would not include other devices, the court rejected the Government's warrant application on the Fourth Amendment's particularity requirement, in addition to the Rule 41 territorial requirement.[27] Interestingly, however, in the concluding paragraph of its opinion, the court acknowledged that "there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology."[28]

B. The Department of Justice's Arguments for Amending Rule 41

After the ruling in *In re Warrant*, the Department of Justice sought to have Rule 41 amended. In a letter submitted to the Advisory Committee on the Federal Rules of Criminal Procedure, the Department argued in favor of the Rule 41 amendments "to address two increasingly common situations."[29] First, the Department of Justice often knew what computer it wanted to search, but did not know the district in which the computer was located.[30] Secondly, the Department increasingly found itself needing to "coordinate searches of multiple computers in multiple districts."[31] Both of these situa-

23. *In re Warrant*, 958 F. Supp. 2d at 757–58.

24. U.S. CONST. amend. IV.

25. *In re Warrant*, 958 F. Supp. 2d at 758.

26. *Id.* at 759.

27. *Id.* at 758–59.

28. *Id.* at 761.

29. Letter from Mythili Raman, Acting Assistant Attorney Gen., U.S. Dep't of Justice, to the Honorable Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 1 (Sept. 18, 2013), https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf.

30. *Id.*

31. *Id.* at 1–2.

tions represent instances of when the Department's investigative and enforcement capabilities were limited due to advances in technology.[32] Specific examples highlighted by the Department involved "a fraudster exchanging email with an intended victim or a child abuser sharing child pornography over the Internet [who] may use proxy services designed to hide his or her true IP address."[33] The Department concluded: "There is a substantial public interest in catching and prosecuting criminals [like these,] who use anonymizing technologies, but locating them can be impossible for law enforcement absent the ability to conduct a remote search of the criminal's computer."[34]

Additionally, the increasing emergence of botnets presents unique challenges to law enforcement.[35] The magnitude of a botnet investigation, which may involve thousands or even millions of computers located in virtually every federal judicial district, imposes practical burdens on investigators. The Department of Justice argued:

> [A] large botnet investigation is likely to require action in all 94 districts, but coordinating 94 simultaneous warrants in the 94 districts would be impossible as a practical matter. At a minimum, requiring so many magistrate judges to review virtually identical probable cause affidavits wastes judicial and investigative resources and creates delays that may have adverse consequences for the investigation.[36]

Considering the challenges posed by new technologies, such as botnets, the Department of Justice argued that it needed new tools to maintain its investigative capabilities in the face of rapidly advancing technology. In response to prevailing critiques of the Rule 41 amendments, the Department posted a statement posted on its website, in which Assistant Attorney General Leslie R. Caldwell argued:

> The amendments do not change any of the traditional protections and procedures under the Fourth Amendment, such as the requirement that the government establish probable cause. Rather, the

32. *Id*.

33. *Id.* at 2.

34. *Id.*

35. A botnet refers to a group of computers that have been infiltrated by cybercriminals. *What Is a Botnet Attack?—Definition*, KASPERSKY LAB, https://usa.kaspersky.com/internet-security-center/threats/botnet-attacks#.WH00x7GZMUE (last visited May 17, 2017). The cybercriminals install malware on the computers and create a network, which they then use to engage in cybercrime. *Id.*

36. Letter from Mythili Raman to Reena Raggi, *supra* note 29.

> amendments would merely ensure that at least one court is available to consider whether a particular warrant application comports with the Fourth Amendment.[37]

Caldwell emphasized that the amendments would not provide any new authority to law enforcement to conduct searches.[38] Fundamentally, the Department argued that the changes simply provide law enforcement with a framework within which to investigate and prosecute cybercrime in light of new technologies used by criminals.[39]

II. ARGUMENTS AGAINST THE CHANGES TO RULE 41

Opposition to the rule changes has been significant. Not only have interest groups, such as the Electronic Frontier Foundation and the Center for Democracy and Technology, criticized the changes, but also several members of Congress have expressed their concerns and tried to block the amendments from taking effect. Opposition to the rule changes centered on the belief that the changes provided for a significant expansion of government authority to conduct computer searches. Moreover, this increased governmental authority would mean that individual privacy rights would be infringed.

A. Congressional Opposition to the Rule 41 Amendments

Congressional opposition against the Rule 41 amendments was led by Oregon Senator Ron Wyden. Senator Wyden saw the amendments as a massive expansion of government authority to search computers.[40] This search authority would not be limited to perpetrators of cybercrime, but include victims of crime as well.[41] Due to these concerns, Senator Wyden called on Congress to reject the new rules through legislation.

Senator Wyden was especially troubled by new government capabilities related to botnet investigations. The Rule 41 changes would enable the government to obtain a single warrant that would permit it to access and search the thousands or millions of computers involved in a botnet.[42] The majority of the searched computers would belong to victims of botnets, rather than the criminals behind the botnets.[43] While the government may have a need to

37. Caldwell, *supra* note 11.

38. *Id.*

39. *Id.*

40. Press Release, Senator Ron Wyden, Wyden: Congress Must Reject Sprawling Expansion of Government Surveillance (Apr. 28, 2016), https://www.wyden.senate.gov/news/press-releases/wyden-congress-must-reject-sprawling-expansion-of-government-surveillance.

41. *Id.*

42. *Id.*

43. *Id.*

search affected botnet computers for evidence, such government authority nevertheless raises significant privacy concerns for computer owners whose computers may be searched.

Finally, Senator Wyden was concerned about the way in which these rule changes were developed. In his view, the rule changes implicate privacy rights, digital security and the Fourth Amendment.[44] Therefore, the changes should not be left to the Supreme Court's rulemaking process, but rather to Congress, the representative body of the American people, to decide: "Substantive policy changes like these are clearly a job for Congress, the American people and their elected representatives, not an obscure bureaucratic process."[45]

Further evidence of congressional concern was presented on October 27, 2016, when a group of over twenty concerned members of Congress sent a letter to then-U.S. Attorney General, Loretta Lynch, requesting responses to a series of significant questions about the rule change.[46] In particular, the members asked Attorney General Lynch to specify how the department would notify users that their devices had been searched, the grounds on which probable cause authorizes "the remote search of tens of thousands of devices," and what procedures the department would put in place to protect users' private information.[47] These questions regarding the rule changes and the concerns about expanding government authority to search computers led Senator Wyden and others to introduce legislation to stop the rule changes.[48] Ultimately, however, the legislative efforts brought forth by Senator Wyden and others failed to prevent the rule changes from taking effect.[49]

B. Civil Liberties Groups' Opposition to the Rule 41 Amendments

Ever since the amendments to the rule were proposed, civil liberties groups argued that the changes provided for a dangerous expansion of government surveillance powers. Indeed, the Electronic Frontier Foundation, which has been very vocal in its opposition to the rule changes, argued that the amendments are not "merely a procedural update. [They] significantly expand[] the hacking capabilities of the United States government without

44. *Id.*

45. *Id.*

46. Letter from Ron Wyden et al., Senator, U.S. Senate, to Loretta Lynch, Attorney Gen., U.S. Dep't of Justice (Oct. 27, 2016), https://www.wyden.senate.gov/download/?id=586322BE-A957-4C97-94C3-23CD8219DE1F&download=1.

47. *Id.*

48. S. 2952, 114th Cong. (2016); H.R. 5321, 114th Cong. (2016).

49. Joe Uchill, *Last-Ditch Effort to Prevent Changes to Law Enforcement Hacking Rule Fails*, THE HILL (Nov. 30, 2016, 12:13 PM), http://thehill.com/policy/cybersecurity/308088-last-ditch-effort-to-prevent-change-to-rule-41-fails.

any discussion or public debate by elected officials."[50] If law enforcement is to be given a substantive expansion of its authority to conduct searches, then, according to the Electronic Frontier Foundation, that expansion should be provided by Congress as the representative body of the American people.[51] Similarly, the Center for Democracy and Technology called the Rule 41 amendments "astoundingly dangerous" and posited that they could have "profound consequences for the privacy and security of computers worldwide."[52]

While the Supreme Court has the authority to make changes to procedural rules governing the federal courts, it may not make substantive changes to the law.[53] Members of Congress as well as civil liberties groups saw the Rule 41 amendments as substantive changes to the law in that the amendments expanded government's ability to conduct computer searches and affect computer users' privacy. From their perspective, Congress, as the legislative branch, should have been the entity that passed the Rule 41 amendments.

III. A CLOSER ANALYSIS OF THE RULE 41 AMENDMENTS

The Rule 41 amendments provide a magistrate judge with the authority to issue a search warrant for a target computer outside of the judge's district in two new circumstances: (1) when the location of the target "has been concealed through technological means," and (2) when, in a Computer Fraud and Abuse Act investigation, the target computers "have been damaged without authorization and are located in five or more districts."[54] The implications of these amendments are concerning in that they drastically expand the scope of the government's ability to conduct computer searches. First, the amendments allow government to search computers that are "concealed through technological means," which is unduly vague language. Second, the amendments likely violate the particularity requirement of the Fourth Amendment. Third, the amendments will allow government to search not only the computers of criminals, but the computers of the criminals' victims as well.

50. Rainey Reitman, *With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Apr. 30, 2016), https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government.

51. *Id.*

52. Jadzia Butler, *U.S. Supreme Court Endorses Government Hacking*, CTR. FOR DEMOCRACY & TECH.: BLOG (May 6, 2016), https://cdt.org/blog/u-s-supreme-court-endorses-government-hacking/.

53. 28 U.S.C. § 2072(b) (2012) ("Such rules shall not abridge, enlarge or modify any substantive right).

54. FED. R. CRIM. P. 41(b)(6).

A. Rule 41(b)(6)(A): "Concealed Through Technological Means" Is Vague and Drastically Expands the Scope of the Government's Ability to Conduct Searches

Law enforcement has been struggling with the increasingly common situation of needing to describe a computer to be searched, but not knowing its precise location. Frequently, targets of law enforcement investigations are using technologies that hide their locations online.[55] Undoubtedly, new anonymizing technologies provide challenges to law enforcement. Yet, it has to be noted that such technologies are not just used by criminals. Often, computer users have very legitimate reasons for using technologies that hide their identities online.

For example, as the Electronic Frontier Foundation points out, "people who use Tor, folks running a Tor node, or people using a VPN would certainly be implicated" by the Rule amendments.[56] Furthermore, the new language could extend to individuals who chose not to share their location with apps or ad networks, or people who change their country setting in order to gain access to services that they otherwise would not be able to.[57] There are many additional reasons why someone may want to use anonymizing technologies:

> From journalists communicating with sources to victims of domestic violence seeking information on legal services, people worldwide depend on privacy tools for both safety and security. Millions of people who have nothing in particular to hide may also choose to use privacy tools just because they're concerned about government surveillance of the Internet, or because they don't like leaving a data trail around haphazardly.[58]

These examples illustrate that, in many cases, individuals may hide their identities online for reasons that are not at all motivated by any criminal intent. The changes to Rule 41 could, however, subject these individuals to government searches.

In response to these concerns, the Department of Justice argues that the use of anonymizing technology in and of itself does not provide grounds for a search warrant. The government must still demonstrate probable cause that

---

55. ADVISORY COMM. ON CRIMINAL RULES, CRIMINAL RULES COMMITTEE MEETING 88 (2015), http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015.

56. Reitman, *supra* note 50; Ian Paul, *How—and Why—You Should Use a VPN Any Time You Hop on the Internet*, TECHHIVE (Jan. 18, 2017, 3:00 AM), http://www.techhive.com/article/3158192/privacy/howand-whyyou-should-use-a-vpn-any-time-you-hop-on-the-internet.html; *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited May 17, 2017).

57. Reitman, *supra* note 50.

58. *Id.*

evidence of a crime will be discovered before a magistrate judge will issue a search warrant. Assistant Attorney General Caldwell was blunt in her remarks at the Center for Strategic and International Studies:

> [The update to the rule] doesn't change the level of evidence and proof that we have to present to a judge in order to get the judge to agree that there's probable cause to issue a warrant. What [the rule] does change is, now, when criminals hide the location of their computers through anonymizing technology, we don't have to figure out which federal district the computers are physically located in before we can act to stop criminal activity.[59]

Assistant Attorney General Caldwell's comments imply that the use of anonymizing technology is not grounds for a search warrant. Law enforcement must still demonstrate probable cause that evidence of a crime will be found if a search warrant is to be issued. Nevertheless, the amended Rule provides a new ability for government to conduct expansive searches of computers. Even if government is able to demonstrate probable cause, it must no longer clearly identify the location of a computer to be searched, and it may use a single warrant to search thousands or even millions of computers.

B. The Rule 41 Amendments Violate the Particularity Requirement of the Fourth Amendment

The amendments to Rule 41 violate the Fourth Amendment's particularity requirement. The Fourth Amendment requires that no warrants be issued without "particularity describing the place to be searched, and the persons or things to be seized."[60]

Without being able to describe the location of the target to be searched, it is difficult to see how law enforcement may satisfy the Fourth Amendment's particularity requirement. Moreover, the methods that law enforcement would presumably use to enable a search of a target computer could have the unintended consequence of accessing innocent computers.[61] For example, the rule changes would allow a single warrant to be the basis for searching hundreds, thousands, or even millions, of computers if they are all part of a botnet. It is doubtful that each of the many involved computers would be described with particularity.

---

59. *The State of Cybercrime: A Look Back and a Look Forward*, CTR. FOR STRATEGIC & INT'L STUDIES 17:18 (Dec. 8, 2016), https://www.csis.org/events/state-cybercrime-look-back-and-look-forward.

60. U.S. CONST. amend. IV.

61. For example, law enforcement could access innocent computers through the use of watering hole attacks or users forwarding a government phishing email. *See* Memorandum from American Civil Liberties Union to Members of the Advisory Committee on Criminal Rules (Oct. 31, 2014), https://www.aclu.org/files/assets/aclu_comment_on_remote_access_proposal.pdf.

Unfortunately, these constitutional concerns were not explored by the Advisory Committee when it contemplated the rule changes. Indeed, the Committee chose to pass questions of constitutionality on for the courts to decide:

> The 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.[62]

It is concerning that questions of constitutionality were not considered during the development of the rule amendments. It is even more concerning that law enforcement would have new authorities that are potentially unconstitutional until courts decide otherwise.

C. Rule 41(b)(6)(B): Allowing Government to Search Victim Computers That Are Part of a Botnet Is a Sweeping Expansion of Government Authority

The amendments to Rule 41 will allow the government to search all computers that are part of a botnet. This new authority is a sweeping expansion of government authority. In particular, Rule 41(b)(6)(B) allows a magistrate judge of a district where activities related to a crime may have occurred to issue a warrant that permits law enforcement to use remote access to search electronic storage media and to seize or copy electronically stored information. A magistrate judge may exercise this authority if, "in an investigation of a violation of [the Computer Fraud and Abuse Act], the media are protected computers that have been damaged without authorization and are located in five or more districts."[63]

The effect of the rule changes, however, has worrisome implications for individual computer users, most of whom are not criminals. The authority granted in this new section of Rule 41,

> means victims of malware could find themselves doubly infiltrated: their computers infected with malware and used to contribute to a botnet, and then government agents given free rein to remotely access their computers as part of the investigation. Even with the best of intentions, a government agent could well cause as much or even more harm to a computer through remote access than

62. ADVISORY COMM. ON CRIMINAL RULES, CRIMINAL RULES COMMITTEE MEETING 141 (2015), http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015.

63. FED. R. CRIM. P. 41(b)(6)(B).

> the malware that originally infected the computer. . . . Government access to the computers of botnet victims also raises serious privacy concerns, as a wide range of sensitive, unrelated personal data could well be accessed during the investigation.[64]

During a panel discussion presented by the Stanford Center for Internet and Society in October 2016, Allison Bragg, Assistant United States Attorney, offered a justification for the government's need to search computers that have been compromised as part of a botnet.[65] She stated that data on computers that have been compromised as part of a botnet is evidence of a crime and the government must have access to that evidence.[66] The government's need to obtain this evidence is the reason why the government should be able to search a "victim's" computer.[67] Bragg analogized this kind of search with the government executing a warrant to search the home of an innocent bystander to collect a gun that was used for a murder, unbeknownst to the gun-owner and owner of the home being searched.[68] Since the government's search of the home is legal, Bragg argues, the government's search of botnets is legal as well.

The Department of Justice further responded to opponents of Rule 41 amendments by stating:

> In general, we anticipate that the items to be searched or seized from victim computers pursuant to a botnet warrant will be quite limited. For example, we believe that it may be reasonable in a botnet investigation to take steps to measure the size of the botnet by having each victim computer report a unique identifier; but it would not be lawful in such circumstances to search the victims' unrelated private files.[69]

In other words, law enforcement claims that it may not search the entire victim computer and that the particularity requirement limits the extent of what is to be searched and seized. While the Department's response may be commendable, it does not guarantee the scope of computer searches will not expand beyond the directly affected computer, or that private files truly remain private and protected. Despite the Department's assurances, countless computers may end up being searched pursuant to a single warrant issued on the basis of the new Rule 41 amendments. The vast majority of the owners

64. Reitman, *supra* note 50.

65. *Government Hacking: Rule 41*, STANFORD LAW SCH. CTR. FOR INTERNET & SOC'Y 1:08:13–109:35 (Oct. 27, 2016), http://cyberlaw.stanford.edu/events/government-hacking-rule-41.

66. *Id.*

67. *Id.*

68. *Id.*

69. Letter from Peter J. Kadzik to Ron Wyden, *supra* note 8.

of these computers will have no connection to the criminal activity being investigated other than being victims of the criminal botnet. Moreover, the computer owners' private information will be put at risk every time it is accessed remotely. So, even if the Department intends to limit itself when conducting computer searches under Rule 41, it is reasonable to expect that the number of computers and the information involved in a government search will be beyond the scope of the warrant.

IV. ADDITIONAL LIKELY CONSEQUENCES OF THE RULE 41 AMENDMENTS

In addition to specific concerns related to the venue amendments contained in section (b)(6), there are other troubling consequences to the Rule 41 amendments, including violations of warrant notice requirements, violations of international law, and forum shopping.

A. Rule 41 Amendments May Violate the Warrant Notice Requirement

Rule 41(f)(1)(C) requires that an "officer executing [a] warrant *must* give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken."[70] Recognizing the impracticality of notifying owners of computers of unknown location, or notifying every owner of the thousands or millions of computers involved in a botnet, Rule 41 establishes a different notice requirement for remote electronic searches. In cases where government conducts remote electronic searches, government must only make "reasonable efforts" to notify the owner of the property that was searched:

> For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.[71]

Providing notice to computer owners may be difficult and impractical. For its part, the Department of Justice says that in an investigation involving botnet victims, for example, the Department would make reasonable efforts to notify victims of searches: "if investigators obtained victims' IP addresses at a particular date and time in order to measure the size of the botnet, inves-

70. FED. R. CRIM. P. 41(f)(1)(C) (emphasis added).

71. Letter from John G. Roberts to Paul D. Ryan & Joseph Biden, *supra* note 6.

tigators could ask the victims' Internet service providers to notify the individuals whose computers were identified as being under the control of criminal bot herders."[72]

It is unrealistic, however, to expect every computer owner of an affected botnet to be notified of a government search. Botnets may include hundreds, thousands, or millions of computers. Due to this fact, there is a significant chance that owners of computers that have been searched will never receive notice that a search has occurred. However, as long as government made a "reasonable effort" to notify owners of searched computers, government would be in compliance with Rule 41. It is unclear, however, what notice attempts would constitute a reasonable effort. Especially concerning is the fact that the owners of searched computers who do not get notice of a search may never find out that a search has occurred and will therefore never be able to contest the search warrant. In this situation, a court will not review the search warrant's legitimacy, thus failing to exercise a necessary check on law enforcement power.

B. Rule 41 Amendments May Lead to Violations of International Law

If the location of a target computer is unknown, it may be the case that the computer is located outside of the United States. If law enforcement conducts an electronic remote search based on Rule 41, and the target computer is outside of the United States' jurisdiction, such a search may be considered a violation of state sovereignty and international law.

The Rule 41 amendments may run counter to United States treaty obligations. For example, the Convention on Cybercrime, also known as the Budapest Convention, is explicit about allowing trans-border access to stored computer data only if the data is publicly available or if "lawful and voluntary" consent is obtained from the country in which the search would take place.[73]

Indeed, Department of Justice policies instruct law enforcement officers to:

> exercise their functions in the territory of another country only with the consent of that country . . . . Moreover U.S. law enforcement should only make direct contact with an ISP located in [a foreign country] with (1) prior permission of the foreign government; (2) approval of [the Department of Justice's] Office of International

72. Letter from Peter J. Kadzik to Ron Wyden, *supra* note 8.

73. Convention on Cybercrime, Council of Europe, art. 32, Nov. 23, 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

> Affairs . . . ; or (3) other clear indicia that such practice would not be objectionable in [the foreign country].[74]

This Department policy aligns with the United States treaty obligation under the Convention on Cybercrime. Furthermore, the Department of Justice assured the Advisory Committee: "[S]hould the media searched prove to be outside the United States, the warrant would have no extraterritorial effect, but the existence of the warrant would support the reasonableness of the search."[75] The Department thereby affirmed that it would not conduct searches outside of the United States pursuant to a warrant issued under the Rule 41 amendments.

Nevertheless, if law enforcement does not actually know where a computer is located, it may very well end up searching a computer that is located in another country. If that happens, a violation of international law will have occurred and the legal, as well as the geo-political, fallout could be unsettling.

C. Rule 41 Amendments May Lead to Forum Shopping by Law Enforcement Officers Seeking a Search Warrant

The Rule 41 amendments provide magistrate judges, in any district where activities related to a crime may have occurred, with the authority to issue warrants to conduct remote electronic searches.[76] Given this Rule change, law enforcement officers who seek a remote electronic search warrant may be tempted to apply for the warrant in a district that is historically friendly to such government requests. Such forum shopping is undesirable because it may further diminish protections against unreasonable searches and seizures. Different judges may have different opinions on the sufficiency of a warrant application, especially when complicated technological issues are involved. Instead of having to seek a warrant in their own jurisdiction, where a judge may be less inclined to grant the warrant, law enforcement now has the ability to simply go to a different district where the magistrate judge has demonstrated a willingness to grant such warrants.

According to the Department of Justice, the language of the amended rule actually limits the possibility of forum shopping. The venue in which a magistrate judge may issue a warrant for a remote search is restricted to "any district where activities related to a crime may have occurred."[77] The Department contends that this language will:

---

74. OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 56–57 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

75. Letter from Mythili Raman to Reena Raggi, *supra* note 29, at 5.

76. FED. R. CRIM. P. 41(b)(6).

77. *Id.*

> Often . . . leave only a single district in which investigators can seek a warrant. For example, where a victim has received death threats, extortion demands, or ransomware demands from a criminal hiding behind Internet anonymizing technologies, the victim's district would likely be the only district in which a warrant could be issued for a remote search to identify the perpetrator.[78]

Despite the attempted assurances of the Department, however, it is not hard to imagine that law enforcement officers will tend to choose to apply for warrants in jurisdictions with sympathetic judges.

V. CONCLUSION

Proponents of the Rule 41 changes argue that the changes are procedural and not substantive. They argue that the changes apply only to venue selection and will not negate fundamental legal requirements, such as demonstrating probable cause. It is difficult, however, to deny the substantive effects of the rule change. Given that the rule change, in its practical effect, provides for a significant expansion of the government's ability to search computers, the amendments to Rule 41 should not have been adopted by the Supreme Court. The Rules Enabling Act, which gives the Supreme Court the authority to prescribe rules of judicial procedure is explicit in that "such rules shall not abridge, enlarge or modify any substantive right."[79] Because the Rule 41 amendments do provide new substantive authorities to law enforcement to conduct computer searches, the Supreme Court acted beyond its authority. Only Congress has the authority to allocate new legal authority to law enforcement through the legislative process. With respect to Rule 41, elected officials should have debated these critical changes to the Rule publicly and considered the potential consequences carefully. Even though the Rule changes went into effect on December 1, 2016, Congress could still choose to examine the amendments more closely and repeal or amend them in the future. For now, magistrate judges who are asked to issue a search warrant based on the new Rule 41 amendments should consider the application carefully to ensure Fourth Amendment protections are still protected.

78. Letter from Peter J. Kadzik to Ron Wyden, *supra* note 8.

79. 28 U.S.C. § 2072(b) (2012).