A WARRANT TO HACK: AN ANALYSIS OF THE PROPOSED AMENDMENTS TO RULE 41 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

Zach Lerner*

18 YALE J.L. & TECH. 26 (2016)

ABSTRACT

In 2013, a federal magistrate judge denied an FBI request for a remote access search warrant, concluding that, among other deficiencies, Rule 41 of the Federal Rules of Criminal Procedure prevented him from granting a warrant to hack a computer when the location of the device was not known. Just five months later, the DOJ proposed amendments to Rule 41 seeking to eliminate the territorial limits on search warrants in two cybercrime contexts: (1) when suspects conceal their online locations and identities; and (2) when malware affects users in five or more districts. Despite approval from the necessary judicial committees and conferences, the amendments must now survive review by the Supreme Court and Congress. While the government argues that the amendments represent small but necessary changes, critics raise a number of far-reaching legal and policy concerns, labeling the amendments as the legalization of "New Invasive Global Hacking Powers." This paper seeks to impartially present and evaluate both sides of the argument. This Article offers concrete alterations to the amendments, which ensure that law enforcement agencies are able to effectively investigate and prosecute cybercrimes while simultaneously protecting privacy, safeguarding civil liberties, and guaranteeing that remote access search warrants do not become ubiquitous tools of surveillance.

TABLE OF CONTENTS

TABLE OF CONTENTS 26

INTRODUCTION 27

I. THE DEPARTMENT OF JUSTICE'S VISION OF CHANGE 30

II. CONCERNS OVER THE EXPANSION OF RULE 41 42

---

* Many thanks to Susan Crawford, Greg Nojeim, and Nathan Wessler for their guidance in writing this Article as well as Jadzia Butler, Ross Slutsky, Amanda Weingarten, and all of the *Yale Journal of Law & Technology* editors for their support and work in developing and publishing this Article. The Article does not represent the views of the organizations with which the author is affiliated.

III. SUGGESTED ALTERATIONS TO RULE 41 62
CONCLUSION 69

INTRODUCTION

In 2012, the Federal Bureau of Investigation (FBI) faced a serious problem. Agents located troves of child pornography stored on an underground network of untraceable websites frequented by unidentified users.[1] The government could identify neither the individual hosting the website nor the users disseminating and viewing the illicit images. The FBI initiated "Operation Torpedo", seeking a court-issued warrant to collect identifying information on the individuals that visited the websites. If issued, the warrant would allow the FBI to use a remote access search technique to alter the website's code to include secret instructions compelling all computers that visited the site to send identifying information directly to the FBI.[2] Because the court issued the warrant, the FBI was able to identify the previously anonymous users and arrest fourteen suspects. The operation's success prompted the FBI to continue its usage of the remote access search tactic in future investigations.[3]

However, a judicial opinion issued one year later in an unrelated case challenged the legitimacy of remote access searches.[4] The 2013 ruling denied the FBI's application for a remote access search warrant due to concerns regarding Federal Rule of Criminal Procedure 41 (Rule 41), which restricts a judge's ability to issue warrants outside of his or her district.[5] Due to venue requirements, a judge may only issue a warrant to search property known to be within the area over which he or she has jurisdiction.[6] This requirement is not satisfied when a judge does not know where the suspected criminals or their computers are located. Out of fear that the

---

1 *See FBI Admits to Exploiting Tor To Take Down Child Porn Behemoth*, RT (Sept. 13, 2013), http://rt.com/usa/fbi-exploiting-tor-child-porn-842 [https://perma.cc/E8DJ-TTPM].

2 Am. Civil Liberties Union, ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media, (Apr. 4, 2014), https://www.aclu.org/sites/default/files/assets/aclu_comments_on_rule_41.pdf [https://perma.cc/DAE3-X3WV].

3 *See* Kevin Poulsen, *FBI Spyware Has Been Snaring Extortionists, Hackers for Years*, WIRED (Apr. 16, 2009), http://www.wired.com/2009/04/fbi-spyware-pro [https://perma.cc/9N6Q-XFXL].

4 *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 753 (S.D. Tex. 2013).

5 *Id.*

6 FED. R. CRIM. P. 41(b)(2)-(5).

ruling might impede future efforts to curb cybercrime, the government has taken steps to amend Rule 41.

Currently, Rule 41 only authorizes out-of-district – also known as extraterritorial – warrants in four circumstances: (1) property that is in the district when the warrant is issued but might be moved outside of the district before the warrant is executed; (2) tracking devices, which may be monitored outside the district if installed within the district; (3) investigations of domestic or international terrorism; and (4) property located within territory occupied for a United States diplomatic or consular mission.[7] These exceptions do not relax the venue requirements in the digital crime context. Remote access search techniques allow the FBI to search a computer without handling it physically, instead searching its contents through an Internet connection. The amendments to Rule 41 would clarify the legality of extraterritorial remote access search warrants in two scenarios: (1) when suspects conceal their online location and identity, engaging in crime anonymously; and (2) when malware affects innocent users in five or more districts.[8]

The government emphasizes that the amendments would not generate a "new" law enforcement search tool. Remote access searches have been utilized for nearly fifteen years for tasks ranging from monitoring location information[9] to logging

---

7 *Id.*

8 Memorandum from Hon. Reena Raggi, Advisory Comm. on Criminal Rules, on the Report of the Advisory Committee of Criminal Rules to Hon. Jeffrey S. Sutton, Chair, Comm. on Rules of Practice and Procedure 8 (May 5, 2014), *in* COMM. ON RULES OF PRACTICE AND PROCEDURE OF THE JUDICIAL CONFERENCE OF THE U.S., PRELIMINARY DRAFT OF PROPOSED AMENDMENTS TO THE FEDERAL RULES OF APPELLATE, BANKRUPTCY, CIVIL, AND CRIMINAL PROCEDURE: REQUEST FOR COMMENT 326, 338 (Aug. 2014), http://www.uscourts.gov/file/preliminary-draft-proposed-amendments-federal-rules-appellate-bankruptcy-civil-and-criminal [https://perma.cc/9ZJW-GRRC]) [hereinafter REQUEST FOR COMMENT]. The proposed language reads as follows: "(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; 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." *Id.* at 340.

9 Third Amended Application for a Search Warrant, In the Matter of the Search of Network Investigative Technique ("NIT") for Email Address texan.slayer@yahoo.com, No. 1:12-sw-05685-KMT at 4 (D. Col. Dec. 11, 2012).

decryption passwords.[10] The FBI has used information collected with remote access search tools to indict, for example, a suspect who extorted a casino,[11] a sexual predator who threatened a teenage girl,[12] and a sixteen-year-old Swedish hacker charged with breaching networks at Cisco and NASA.[13] Similarly, the government takes the position that the extraterritorial authority proposed by the amendments is not novel. The four exceptions currently embedded in Rule 41 demonstrate the need for exemptions from the venue requirements. The amendments merely seek to expand the ability of law enforcement to apply for extraterritorial authority in instances that are not explicitly covered by the existing exceptions.

Concerns over this expansion in power are legitimate. A variety of professors, media outlets, and non-profit organizations have levied harsh criticisms at the proposed amendments. Opponents believe the amendments will provide law enforcement agencies with mechanisms to bypass the Fourth Amendment and lead to a circumvention of other legal oversight regimes.[14] These critics argue that a lack of transparency and minimization procedures in the warrant applications leaves judges unable to adequately assess the potential uses of remote access search techniques.[15] Further, usage of remote access search techniques will likely increase if the amendments are approved. Finally, opponents point to the amendments' potential unintended consequences, including a harmful effect on the Internet ecosystem,[16] an increased

---

10 *See FBI Has a Magic Lantern to Light the Path to Suspects' Computers*, ABOUT.COM (last accessed Dec. 17, 2014), http://usgovinfo.about.com/library/weekly/aa121401a.htm [https://perma.cc/PV6Z-NANE].

11 Poulsen, *supra* note 3.

12 *Id.*

13 *Id.*; *see also* Press Release, U.S. Dep't of Justice, Swedish National Charged with Hacking and Theft of Trade Secrets Related to Alleged Computer Intrusions at NASA and CISCO (May 5, 2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/petterssonIndicted.pdf [https://perma.cc/LE9U-PCCU].

14 *See, e.g.*, Am. Civil Liberties Union, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media 22 (Oct. 31, 2014), https://www.aclu.org/files/assets/aclu_comment_on_remote_access_proposal.pdf [https://perma.cc/3Y4Z-DSBM].

15 *See, e.g.*, Laura Donohue, Remarks at Panel on the Legal and Policy Implications of Hacking by Law Enforcement, at 21:40 (Feb. 18, 2014), *available at* http://vimeo.com/88165230 [https://perma.cc/F82Y-KSN7].

16 *See, e.g.*, Bijan Madhani, *Government Seeks Expanded Hacking Ability in Criminal Investigations*, CCIA (Nov. 7, 2014), https://www.ccianet.org/2014/11/government-seeks-expanded-hacking-ability-in-criminal-investigations [https://perma.cc/4ZSJ-7VSF].

incentive for the government to stockpile zero-day exploits,[17] and a potential for forum shopping.[18]

This paper seeks to balance impartially the need for amendments to Rule 41 with the legitimate concerns outlined above. Part II will assess the government's justifications for altering Rule 41, detail the proposed amendments, and examine the methods used to conduct remote access searches. Part III will expose various legal and policy concerns with the amendments, as well as the potential consequences of enacting them. Part IV will recommend alterations to the amendments that reflect these concerns and consequences.

I. The Department of Justice's Vision of Change

A. The Rationale for Amending Rule 41

The amendments to Rule 41 would remedy administrative hurdles that frustrate the effective investigation of increasingly common digital crimes. This is accomplished through the addition of two carve-outs for extraterritorial search warrants and the amendment of the notice requirements for remote access searches. The first carve-out would confer authority to judges to grant extraterritorial warrants when suspects use anonymizing software to mask the location of their computers – in essence, codifying the authority used in Operation Torpedo. The second carve-out pertains to the investigation of criminal violations of parts of the Computer Fraud and Abuse Act (CFAA) – most notably, crime that is perpetrated by botnets.[19] Unrelated to the use of anonymizing software, this exception would allow a single court to issue multi-district, multi-computer remote access search warrants for all computers infected by a given piece of malware. Among other merits, the Department of Justice (DOJ) believes that the amendments will finally reconcile Rule 41 with the Electronic Communications Privacy Act (ECPA), which authorizes a judge to issue a warrant for searches of electronic information in another district.[20]

---

17 *See, e.g.*, *supra* note 14.

18 *See, e.g.*, Memorandum from Orin Kerr to Members of the Rule 41 Subcomm. at 1-2 (Feb. 3, 2014), *in* Advisory Comm. on Criminal Rules, *supra* note 28, at 239-40.

19 Memorandum from Hon. Reena Raggi, *supra* note 8.

20 *Id.* at 519; *see also* 18 U.S.C. §§ 2703(a) 2711(3)(A)(II) (2012); *United States v. Bansal*, 663 F.3d 634, 662 (3d Cir. 2011) (rejecting the contention that Rule 41(b)'s limits trump 18 U.S.C. § 2703(a)); *United States v. Berkos*, 543 F.3d 392, 397-98 (7th Cir. 2008) (holding that Rule 41(b) "does not apply to § 2703(a)").

1. Exceptions for Extraterritorial Search Warrants.

In a letter to the Advisory Committee on Criminal Rules suggesting the amendments, the Department of Justice asserts that amending Rule 41 is necessary for successful investigations of users implementing anonymizing software. As currently written, Rule 41 deprives judges of the power to issue a warrant if a suspected criminal is using an anonymizing tool, like the "Tor" network, to hide his or her device's true Internet Protocol (IP) address while perpetuating crime. Take, for example, an individual issuing bomb threats over the Internet by means of an anonymizing tool. The proxy service operates as an intermediary that routes the communication through a network of distributed relay computers.[21] The communication hops from relay computer to relay computer until it is eventually sent to the intended recipient.[22] When the recipient – maybe a user on the receiving end of an email or a website on which a threatening post is made – receives the communication, he or she solely collects the IP address of the final proxy computer, not the original actor. As such, law enforcement is unable to determine the true location of the device. Therefore, if a judge only has authority to issue a warrant for devices he or she knows to be in his or her district, as the current venue requirements dictate, no judge in the country would have authority to issue the warrant in this investigation. The DOJ asserts that the frequency of this scenario is increasing because cyber criminals are using "sophisticated anonymizing technologies" with greater regularity.[23]

The second aspect of the amendments, reflecting the DOJ's desire to prevent violations of the CFAA, relates directly to botnets.[24] A botnet is a network of computers infected with malicious software that enables simultaneous command by a single control mechanism or "master."[25] This network of compromised computers or "zombies" can be used to send

---

21 *See* Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, WIRED (Aug. 5, 2014), http://www.wired.com/2014/08/operation_torpedo [https://perma.cc/GH47-QFJ7].

22 *Tor: Overview*, TOR PROJECT, www.torproject.org/about/overview.html.en [https://perma.cc/9QJK-8NMV].

23 Memorandum from Hon. Reena Raggi, *supra* note 8, at 7; *see* REQUEST FOR COMMENT, *supra* note 8, at 325, 338.

24 Proposed Amendments to the Federal Rules of Criminal Procedure 13, *in* REQUEST FOR COMMENT, *supra* note 8. The committee note makes specific reference to the creation and control of botnets in its description of criminal activity under 18 U.S.C. § 1030(a)(5).

25 Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 1 (2014).

unsolicited email or spam, create false web traffic, or install spyware to collect personal information.[26]

There is a legitimate and impending need for law enforcement to develop tools to combat botnets. An individual botnet can command over 12 million zombies concurrently.[27] In support of the efforts to amend Rule 41, Assistant Attorney General Raman stated, "[b]otnets are a significant threat to the public: they are used to conduct large-scale denial of service attacks, steal personal and financial data, and distribute malware designed to invade the privacy of users of the host computers."[28] The Center for Strategic and International Studies predicts that malicious cyber activity costs the economy between $300 billon and $1 trillion per year globally and between $24 billion and $120 billion per year in the United States alone.[29] Microsoft estimates that a single botnet caused over $500 million in losses worldwide.[30]

In its investigation of botnets, the FBI can gain valuable information by gathering data from and disseminating information to the infected zombies.[31] The FBI can also send messages to users alerting them of the botnet, offering instructions on how to determine if their device was infected, and instructing them to "consult a computer professional."[32] In

---

26 *Id.* at 2.

27 *Anatomy of a Botnet: How the Arbor Security Engineering & Response Team (ASERT) Discovers, Analyzes and Mitigates DDoS Attacks*, ARBOR NETWORKS 2 (2012), https://www.arbornetworks.com/images/documents/White%20Papers%20and%20Research/WP_ASERT_EN.pdf [https://perma.cc/T6DY-LZT9].

28 Letter from Mythili Raman, Acting Assistant Attorney General, to The Honorable Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 2 (Sept. 18, 2013), *in* Advisory Comm. on Criminal Rules, Materials for April 7-8, 2014 Meeting 172, http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf [https://perma.cc/4DTL-WB4Q] [hereinafter Advisory Comm. on Criminal Rules].

29 Lerner, *supra* note 25, at 8 (citing CTR. FOR STRATEGIC AND INT'L STUDIES, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE 5 (Jul. 2013), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf [https://perma.cc/YCV3-3Y9P]).

30 *Id.* (citing Press Release, Microsoft, Financial Services and Others Join Forces To Combat Massive Cybercrime Ring, Microsoft (June 5, 2013), http://www.microsoft.com/en-us/news/press/2013/jun13/06-05dcupr.aspx [https://perma.cc/E8C2-DZRQ]).

31 Memorandum from Jonathan J. Wroblewsi, Director, Office of Policy and Legislation to Judge John F. Keenan, Chair, Subcomm. on Rule 41, at 2 (Jan. 17, 2014) (included in the Advisory Comm. on Criminal Rules, *supra* note 28).

32 Lerner, *supra* note 25, at 8 (citing Gregg Keizer, *Feds Lead Biggest Botnet Takedown Ever, End Massive Clickjack Fraud*, COMPUTERWORLD (Nov. 10, 2011), http://www.computerworld.com/s/article/9221699/Feds_lead_biggest_botnet_takedown_ever_end_massive_clickjack_fraud [https://perma.cc/9QTL-9Z4N]).

its investigation of the Coreflood Botnet, the FBI went a step further and delivered a disabling command to the infected zombies, which removed the botnet from their devices entirely.[33] The FBI believes that remote access searches are critical to "assisting victim notification, identifying additional victims, furthering identification of perpetrators, and/or taking steps to disrupt the command and control functions of the botnet."[34]

The government argues that applying for warrants separately in each district in which a zombie device is located presents excessive burdens.[35] Thus, while altering Rule 41 to prevent botnet-related attacks is not necessary, it would relieve a number of administrative obstacles that hinder successful investigation and mitigation. A single botnet can infect millions of users;[36] thus, effective investigation of these crimes can require law enforcement action in dozens of judicial districts.[37] Coordinating simultaneous warrant applications in every district necessarily imposes burdens on both the investigators and magistrate judges.[38] Each application concerns a common piece of malicious software and the affidavits supporting the warrant applications are virtually identical.[39] Requiring a separate magistrate judge in each district to review virtually identical affidavits is a waste of judicial resources and creates "delays that may have adverse consequences for the investigation[s]."[40] Thus, the amendments seek to "remove an unnecessary obstruction currently impairing the ability of law enforcement to investigate botnets and other multi-district Internet crimes."[41]

2. Amending the Notice Requirement for Remote Access Searches

The amendments would also alter Rule 41's notice requirement, reflecting the government's opinion that the subject of a remote access search cannot be provided notice in precisely the same manner as the subject of a physical search.[42]

---

33 *Id.* (citing Kim Zetter, *With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal*, WIRED (Apr. 13, 2011), http://www.wired.com/2011/04/coreflood [https://perma.cc/2QP7-VATN].

34 *See* Memorandum from Jonathan Wroblewsi, *supra* note 31, at 213. It is important to note and underscore that the information is pertinent to identifying the zombies, not the master.

35 Memorandum from Hon. Reena Raggi, *supra* note 8.

36 Lerner, *supra* note 25, at 12.

37 Memorandum from Hon. Reena Raggi, *supra* note 8, at 326.

38 *Id.*

39 *Id.*

40 *See* Letter from Mythili Raman, *supra* note 28, at 173.

41 *Id.*

42 *See* Memorandum from Hon. Reena Raggi, *supra* note 8, at 327.

Notice of remote access searches, the government asserts, should be provided electronically instead of in-person. The government also argues that when law enforcement agents cannot reasonably determine the identity or location of the owner of the device, Rule 41 should provide for an exemption. According to the DOJ, these changes would aid in prosecuting criminals without altering the substantive standards the government must satisfy in warrant applications for extraterritorial searches.[43] Supporters stress that the amendments do not provide authority for new law enforcement tools or broaden the existing ones.[44] In fact, the application of the substantive requirements of the Fourth Amendment – particularity and probable cause – remain unaffected.[45] Thus, the DOJ highlights that the amendments only "address the venue question – the question of which judge can issue a warrant that . . . the Fourth Amendment allows."[46]

B. The Proposed Amendments

The DOJ proposed the amendments to Rule 41 just five months after a court ruling challenged the validity of extraterritorial remote access search warrants.[47] Judge Stephen Smith, a federal magistrate judge in Houston known for speaking out against secret electronic surveillance,[48] denied an FBI request for a remote access search warrant in April 2013.[49] The government had sought authorization to use a remote access search tool to collect identifying information about an individual suspected of bank fraud.[50] The warrant would have sanctioned the collection of network-level

---

43 *See* Memorandum from Jonathan Wroblewsi, *supra* note 31, at 259. The DOJ emphasizes that the amendments do not "impact the standards for when notice may appropriately be delayed with the approval of the issuing court" and is unlikely to "substantially impact existing practice with respect to notice of such warrants." *Id.*

44 *See* Advisory Comm. on Criminal Rules 8 (Apr. 7-8, 2014), *in* Advisory Comm. on Rules of Practice and Procedure Materials for May 29-30 Meeting 516, http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Standing/ST2014-05.pdf [https://perma.cc/4PB3-DSYB].

45 *Id.*

46 *Id.*

47 The DOJ's letter even mentions the case as an example in which a warrant application did not satisfy the territorial jurisdiction requirements. *See* Letter from Mythili Raman, *supra* note 28, at 172.

48 *See, e.g.*, Julia Angwin, *One Judge Who Is Leading the Charge Against Secret Orders*, WALL ST. J. (Oct. 9, 2011), http://www.wsj.com/articles/BL-DGB-23315 [https://perma.cc/SEZ2-W2J6].

49 *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 753 (S.D. Tex. 2013).

50 *Id.*

information and installation of software that could be used in part to take photographs with the device's camera.[51]

Judge Smith described the application as an attempt to "hack a computer suspected of criminal use," and rejected the warrant.[52] The judge focused on three questions: "(1) whether the territorial limits of a Rule 41 search warrant w[ere] satisfied; (2) whether the particularity requirements of the Fourth Amendment ha[d] been met; and (3) whether the Fourth Amendment requirements for video camera surveillance ha[d] been shown."[53] In the end, Judge Smith "concluded that the territorial requirement in Rule 41(b) precluded a warrant for a remote search when the location of the computer was not known."[54] He determined that the warrant application did not fall under any of the extraterritorial exceptions set out in Rule 41(b), including: items that may be moved out of the district, tracking devices, searches related to terrorism, and investigations related to consular missions.[55] Although conceding that there might be sound reasons to update Rule 41's territorial limitations, Judge Smith ultimately concluded that "the extremely intrusive nature of such a search requires careful adherence to the strictures of Rule 41 as currently written."[56]

In response to Judge Smith's ruling, the DOJ wrote a letter to Judge Raggi, a member of the Advisory Committee on Criminal Rules, proposing changes to Rule 41.[57] The Advisory Committee, composed mostly of judges with no legislative oversight or input, is charged with studying the operation and impact of the rules of practice and procedure in the criminal justice system and, when necessary, making changes and additions to the rules to promote simplicity, fairness, justice, and frugality.[58] "The rules amendment process, at its fastest, spans three years from proposal to full enactment" and requires that proposals pass through specific subcommittees

---

51 *Id.* at 756.

52 *Id.* at 755.

53 *Id.* Additionally, Judge Smith expressed concern with regard to the lack of detail explaining how the government would install the software as well as efforts to minimize harm to innocent people.

54 Memorandum from Sara Beale and Nancy King, Reporters to Members, Criminal Rules Advisory Comm. 3 (March 17, 2014), *in* Advisory Comm. on Criminal Rules, *supra* note 28, at 156-57.

55 *See* Memorandum from Hon. Reena Raggi, *supra* note 8, at 324 n.7.

56 *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 765 (S.D. Tex. 2013).

57 *See* Letter from Mythili Raman, *supra* note 28, at 171.

58 *See* FED. R. CRIM. P. 2. *See also* Mark R. Kravitz et al., *They Were Meant for Each Other: Professor Edward Cooper and the Rules Enabling Act*, 46 U. MICH. J. L. REFORM 495, 504 (2013).

and face public comment, as well as gain approval by the Supreme Court.[59]

The DOJ's letter suggests two sets of changes, which, if enacted, would establish "a court-supervised framework through which law enforcement can successfully investigate and prosecute sophisticated Internet crimes."[60] First, the proposed framework would modify Rule 41(b) to add a fifth exception to the in-district venue requirement. This exception would authorize out-of-district warrants in those investigations where location information is "concealed through technological means," or where CFAA violations have damaged computers located in five or more districts.[61] As a result of this exemption, Rule 41 would authorize a court in any district "where activities related to a crime have occurred" to issue a warrant "for electronic storage media and electronically stored information located within or outside that district."[62] Second, the amendments would update Rule 41's notice requirements. Currently, an officer executing a warrant must provide the subject of the search with both a copy of the warrant and a receipt for property taken.[63] The amendments would modify these requirements in remote access searches, such that the government would only need to "make reasonable efforts to serve a copy of the warrant on the person whose property was searched or whose information was seized or copied."[64] The service used to deliver this notice would have to be "reasonably calculated to reach that person."[65]

The DOJ's proposal advanced through the Advisory Committee's standard review process. The Rule 41 subcommittee approved the proposal on March 12, 2014 and forwarded it to the Advisory Committee on Criminal Rules.[66] Through the early part of 2014, a representative of the DOJ engaged in intense debate with Professor Orin Kerr, a member of the subcommittee, as documented in a series of memoranda.[67] Following this debate, edits were made to the initial draft,[68] and in August 2014, the Advisory Committee

---

59 Memorandum from Jonathan Wroblewsi, *supra* note 31, at 245

60 *See* Letter from Mythili Raman, *supra* note 28, at 171.

61 *See* Memorandum from Hon. Reena Raggi, *supra* note 8, at 327.

62 *See* Letter from Mythili Raman, *supra* note 28, at 171.

63 *See* FED. R. CRIM. P. 41(f)(1)(C).

64 *See* Proposed Amendments to the Federal Rules of Criminal Procedure at 12, *in* REQUEST FOR COMMENT, *supra* note 8, at 338, 340.

65 *Id.*

66 *See supra* note 2.

67 Advisory Comm. on Criminal Rules, *supra* note 28, at 239-56.

68 Minutes of Advisory Comm. on Criminal Rules at 6 (Apr. 7-8, 2014), *in* (Advisory Comm. on Rules of Practice and Procedure Materials for May 29-30 Meeting, *supra* note 44, at 514. In addition to exceptions for location concealment and violations of the CFAA, the proposal originally

officially recommended, "that the proposed amendment[s] to Rule 41 be published for public comment."[69] The public comment phase followed for three months concluding in a hearing held on November 5, 2014.[70] On March 16, 2015, the Advisory Committee on Criminal Rules approved the rule change by a vote of eleven to one.[71] The Standing Committee on Rules of Practice and Procedure approved the amendments in May 2015, and the Judicial Conference followed suit in September.[72] At that point, on October 9, 2015, the amendments were transmitted to the Supreme Court, which can adopt the amendments by order before May 1, 2016. If the Court adopts them, they will take effect no earlier than December 1, 2016, unless Congress enacts legislation to reject, modify, or defer them.[73]

C. Capabilities, Methods, and Processes Used to Conduct Remote Access Searches

The public first learned of the government's use of remote access search techniques in 2001.[74] That year, journalists uncovered FBI software—codenamed Magic Lantern—that covertly accessed information stored on targets' computers.[75]

---

sought to permit authorization of remote searches of "electronic information accessible from a computer at a known location when the information is stored remotely in another district." Memorandum from Sara Beale & Nancy King, *supra* note 54, at 157. In other words, it would have authorized the FBI to execute a warrant on a person in New York to remotely and simultaneously seize the data on the computer itself as well as all data accessible from that computer stored with cloud-based servers anywhere in the country.

69 *See* Memorandum from Hon. Reena Raggi, *supra* note 8, at 327.

70 Dibya Sarkar, *Federal Panel Holds Hearing on Rule Change that Expands FBI Electronic Surveillance Powers*, FIERCEGOVERNMENTIT (Nov. 5, 2014), http://www.fiercegovernmentit.com/story/federal-panel-holds-hearing-rule-change-expands-fbi-electronic-surveillance/2014-11-05 [https://perma.cc/LME8-9THL].

71 *See* Dustin Volz, *FBI's Plan to Expand Hacking Power Advances Despite Privacy Fears*, NAT'L J. (Mar. 16, 2015), https://www.benton.org/headlines/fbis-plan-expand-hacking-power-advances-despite-privacy-fears [https://perma.cc/J32U-AFF7].

72 *See Pending Rules Amendments*, U.S. COURTS, http://www.uscourts.gov/rules-policies/pending-rules-amendments [https://perma.cc/YR6J-JSEV].

73 *See id.*

74 In reality, these techniques may go back as far as 1999, when the FBI placed a covert keystroke logger on the computer of a criminal with significant mob ties. *See* Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED (July 18, 2007), http://archive.wired.com/politics/law/news/2007/07/fbi_spyware [https://perma.cc/6TEE-MS5T].

75 *See FBI Sheds Light on 'Magic Lantern' PC Virus*, USA TODAY (Dec. 13, 2001), http://usatoday30.usatoday.com/life/cyber/tech/2001/12/13/magic-lantern.htm [https://perma.cc/4W6C-4LRG].

This tool, initially labeled "a workbench project," was renamed the Computer and Internet Protocol Address Verifier (CIPAV) and reportedly entered into regular use by law enforcement agencies in 2002.[76] However, the government did not disclose the use of CIPAVs as a prosecutorial tool until 2007. That year, the FBI applied for and received a warrant to implement a CIPAV in its investigation of a MySpace user who had made bomb threats to a high school.[77] The CIPAV infiltrated the individual's computer, surreptitiously gathered a wide range of information, and sent it to the FBI.[78] Warrant applications pursuant to Rule 41, like the one used in the MySpace bomber investigation, are considered ex parte without adversarial representation.[79]

In the following years, the FBI used CIPAVs more frequently and rebranded them as network investigative techniques (NITs).[80] In 2012, an FBI task force officer in Colorado applied for a warrant to employ an NIT in the collection of information from a user suspected of threatening to detonate bombs at a jail, hotel, group of international airports, and number of major universities.[81] The suspect, who referred to himself as "Mo," made these threats via voice over Internet Protocol, email, and video chat over a month-long period.[82] However, he used a "virtual proxy" and avoided revealing his identity or location – both physical and digital.[83] A federal magistrate judge in Colorado authorized an

---

76 *See* Memorandum from [redacted] to CTCs 1 (Mar. 7, 2002), https://www.eff.org/document/fbicipav-05pdf [https://perma.cc/Z9HS-8GPD]. When introduced, the CIPAV was initially referred to as an Internet Protocol Address Verifier.

77 *See* Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government, No. MJ07-5114, at 2-3, 6-9 (W.D. Wash. June 12, 2007), http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf [https://perma.cc/6A9D-EBKK] [hereinafter Application and Affidavit for Search Warrant].

78 Poulsen, *supra* note 3.

79 *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 753 (S.D. Tex. 2013).

80 *See* Poulsen, *supra* note 3.

81 Third Amended Application for a Search Warrant, In the Matter of the Search of Network Investigative Technique ("NIT") for Email Address texan.slayer@yahoo.com, No. 1:12-sw-05685-KMT, at 4 (D. Col. Dec. 11, 2012). The calls demanded the release of James Holmes, the suspect in the Aurora Theater or Dark Knight shooting spree.

82 *Id.*

83 Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, WASH. POST (Dec. 6, 2013), http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html [https://perma.cc/X6FM-456E].

extraterritorial remote access search, enabling the FBI to collect information on "Mo" through an NIT.[84] The NIT covertly planted software on the suspect's computer, which delivered various location and identifying information to the FBI.[85]

Remote access search tools have a number of capabilities, ranging in complexity and invasiveness. The most basic function of a remote access search tool is collecting the IP address of a targeted computer.[86] Law enforcement agents can use this IP address to subpoena subscriber information from the Internet Service Provider (ISP) responsible for that IP address. In the FBI's investigation of a target using anonymizing software, this could lead to the discovery of a physical address for the suspect. In the investigation of a large-scale botnet, this could provide points of contact for infected users. Remote access search tools can also gather more sophisticated identifying information, such as the target's MAC address; open communication ports; a list of programs running on the computer; the type, version, and serial number of the operating system; the type and version of the web browser; the default language; time zone; registered computer name; logged-in user name; and list of user accounts.[87] A remote access search tool can reveal inherently personal information about a user's Internet activity including "firewall logs, caches, browser history and cookies, 'bookmarked' or 'favorite' Web pages, search terms that the user entered into any Internet search engine, and records of user-typed Web addresses."[88] Additionally, these tools can collect actual content, such as "documents, . . . user profiles, e-mail contents, e-mail contacts, chat messaging logs, photographs, and correspondence."[89] Remote access techniques can also actively enable functions on the target's computer or mobile device. For example, the

---

84 Third Amended Application for a Search Warrant, In the Matter of the Search of Network Investigative Technique ("NIT") for email address texan.slayer@yahoo.com, No. 1:12-sw-05685-KMT at 1 (D. Col. Dec. 11, 2012).

85 *Id.* at 4.

86 *Id.* at 16.

87 *Id.*

88 *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755-56 (S.D. Tex. 2013).

89 *See id.*

government can remotely turn on GPS chips,[90] microphones,[91] and webcams.[92]

Remote access search tools enable the FBI to collect prospective, real-time data on suspects. In its investigation of a MySpace user threatening to bomb a high school, the FBI applied for a warrant to install a remote access search tool with a "pen register" element.[93] The tool continuously recorded and transmitted "the routing and destination addressing information for electronic communications originating from the activating computer."[94] Similarly, in a 2012 remote access search warrant application, the FBI sought to collect "prospective data obtained during a 30-day monitoring period."[95] The desired contemporaneous data included location data based on latitude and longitude calculations as well as photographs taken using the target computer's built-in camera.[96]

The FBI relies on two primary methods of implementing remote access search tools to enable the capabilities discussed above: social-engineering attacks and watering-hole attacks.[97] These methods require different techniques and implicate varying concerns. Understanding how law enforcement employs these tools is necessary to adequately address their utility, the consequences of their use, and the need for limiting their capabilities.

The first method, social engineering, is commonly used in investigations of suspects who have employed anonymizing

---

90 *See id.*

91 Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, WALL ST. J., (Aug. 3, 2013), http://online.wsj.com/articles/SB10001424127887323997004578641993388259674 [https://perma.cc/4FG5-WXHX].

92 *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 755-56; *see also* Timberg & Nakashima, *supra* note 83 (highlighting the ability to do so covertly without triggering the indicator light that alerts the user that the camera is operating).

93 A pen register (or dialed number recorder) is a device that permits the recording of telephone numbers dialed out from a particular phone. Deborah F. Buckman, Annotation, *Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use*, 15 A.L.R. Fed. 2d 537 (2006). Ordinarily, law enforcement must satisfy the requirements under 18 U.S.C. § 3121 in order to obtain a pen register. *Id.*

94 *See* Application and Affidavit for Search Warrant, *supra* note 77, at 13-14.

95 *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755-56 (S.D. Tex. 2013).

96 *Id.* at 756.

97 Am. Civil Liberties Union, ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media, *supra* note 2 at 5-9.

software. Agents send a communication – often an email – to the target, which requires a specific action – often clicking a link or opening an attachment.[98] The FBI used this method in its investigation of "Mo", the man who made numerous bomb threats in Colorado. Although a sergeant with the Denver Police communicated with the suspect regularly over email, "Mo" used anonymizing software that made it impossible to determine his or her IP address.[99] The FBI filed a warrant application seeking authorization to embed an NIT in the sergeant's next e-mail to the target. Once opened, the NIT would surreptitiously install software and collect identifying information. "All investigators needed, it seemed, was for Mo to sign on to his account and, almost instantaneously, the software would start reporting information back to Quantico."[100]

In situations where agents do not have an ongoing dialogue with the suspect, social engineering attacks often require deception on the part of law enforcement. For example, agents may impersonate a third-party, tricking the suspect into clicking on the activating mechanism. In order to deliver a CIPAV in the investigation of the MySpace user making bomb threats in 2007, the FBI emailed the target a fake Associated Press article that, once clicked, exploited a vulnerability in his web browser.[101]

The second method of delivery, a watering-hole attack, also known as a "drive by download," is likewise prevalent in the investigation of users implementing anonymizing techniques. Watering hole attacks are effective when law enforcement agents do not know the identity of a suspect, but know a website that he or she would likely frequent. Agents can then install custom code on the website. This code includes computer instructions that cause all visiting users' computers to deliver specific information to a computer controlled or known by the government.[102] The FBI utilized a watering-hole attack in

---

98 *Id.* at 5.

99 Third Amended Application for a Search Warrant, In the Matter of the Search of Network Investigative Technique ("NIT") for email address texan.slayer@yahoo.com, No. 1:12-sw-05685-KMT at 4 (D. Col. Dec. 11, 2012).

100 Timberg & Nakashima, *supra* note 83.

101 *See* Ellen Nakashima & Paul Farhi, *FBI Lured Suspect with Fake Web Page, but May Have Leveraged Media Credibility*, WASH. POST (Oct. 28, 2014), http://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 [https://perma.cc/H86J-D6S2].

102 Am. Civil Liberties Union, ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronick Storage Media, *supra* note 2, at 6.

Operation Torpedo to identify and indict 14 users of child pornography sites hosted on Tor.[103] It is unclear whether social engineering or watering-hole attacks would be better suited to investigate violations of the CFAA.

Regardless of the method of delivery, the surveillance software infection process follows the same basic steps. The first step is reconnaissance, in which agents ascertain a selector – an email address, user name, website, and so on – to identify the target.[104] Next, the agents must prepare the code that will be delivered to the target's device to carry out the planned attack.[105] Third, agents introduce the attacking code to the target's device through one of the methods detailed above.[106] In step four, the attacking code bypasses the user's security software or abuses a vulnerability in the target's software.[107] Next, the attacking code installs the surveillance software on the target's computer.[108] Ultimately, the software collects and transmits the desired information to the government.[109] In some cases, the attacking code erases itself, while in others, it remains on the device for an extended period of time.[110]

II. Concerns Over the Expansion of Rule 41

Both civil society and the media have criticized the proposed amendments to Rule 41. Reporters have classified the proposed rule change as a means "to seize significant new powers to hack into and carry out surveillance of computers throughout the US."[111] Numerous organizations, including the ACLU, New America Foundation's Open Technology Institute, Center for Democracy & Technology (CDT), Electronic Privacy Information Center (EPIC), and Access Now, as well as a professor at the Hastings College of Law, testified in opposition to the proposal at the Advisory Committee's November 2014 open hearing.[112] Chris Soghoian, a technologist and policy

---

103 *See* Poulsen, *supra* note 21.
104 *See supra* note 14.
105 *Id.*
106 *Id.* at 7-8.
107 *Id.* at 8.
108 *Id.*
109 *Id.*
110 *Id.* at 9.
111 Ed Pilkington, *FBI Demands New Powers to Hack into Computers and Carry Out Surveillance*, GUARDIAN (Oct. 29, 2014), http://www.theguardian.com/us-news/2014/oct/29/fbi-powers-hacking-computers-surveillance [https://perma.cc/A8LQ-4TLM].
112 *See* Tal Kopan, *Morning Cybersecurity*, POLITICO (Nov. 4, 2014), http://www.politico.com/morningcybersecurity/1114/morningcybersecurity15967.html [https://perma.cc/W2L3-KBVY].

analyst at the ACLU, believes that the amendments "giv[e] the FBI the green light to hack into any computer in the country or around the world."[113] Thus, while the government defends the amendments as mere extensions of an extraterritorial caveat for two pressing situations, others attack them with Orwellian concerns.

This section will first address concerns regarding the lack of transparency and minimization procedures in the government's remote access search warrant applications. Next, this section will consider whether changing Rule 41 would result in an increase in the use of remote access search techniques. Third, this section will discuss whether remote access search warrants conform to the requirements of the Fourth Amendment. Next, this section will discuss the fear that the amendments to Rule 41 would allow law enforcement to circumvent existing legal oversight regimes. Finally, this section will detail a number of unintended consequences of the Rule 41 amendments, such as disrupting Internet infrastructure, incentivizing stockpiling of zero-day exploits, and permitting forum shopping.

A. A Lack of Transparency

Critics argue that the government may not be disclosing exactly how it plans to use and implement the new Rule 41 authority. The general nature of remote access searches can be gleaned from sample warrant applications provided by the government, warrant applications filed in federal court, and the Advisory Committee's memoranda. However, these sources may not paint a full picture of the remote search techniques' invasiveness. The sample warrants include references to NITs,[114] RNTs,[115] and CIPAVs,[116] but do not provide an adequate description of the methods by which the tools will be delivered. Laura Donohue, a professor at the Georgetown University Law Center, states that government "applications do not include detailed technology, or technological explanations as to how [the remote access search] is actually going to be executed, enter the computer, exactly what information is going to be obtained, which other devices might be infected, how many devices may be infected, and so on."[117]

---

[113] Brett Wilkins, *FBI Seeking New Invasive Global Hacking Powers*, ETHICSINTECH (Nov. 1, 2014), https://www.ethicsintech.com/fbi-seeking-invasive-global-hacking-powers [https://perma.cc/4W8M-RCTE].

[114] Memorandum from Jonathan Wroblewsi, *supra* note 31, at 200-203.

[115] *Id.* at 215-16.

[116] *Id.* at 217.

[117] *See supra* note 15; *see also* Memorandum from Jonathan Wroblewsi, *supra* note 31, at 19, 25 (stating knowledge of dozens of cases involving

Thus, in seeking remote access warrants, the FBI does not provide the judiciary with proper notice or understanding of how the tools will be used.

As such, the judges charged with ruling on remote access search warrant applications may not fully understand what they are being asked to authorize. What, in reality, amounts to the use of hacking software to take advantage of computer vulnerabilities in order to breach a device's defense is described as the simple installation of software that will extract information. Chris Soghoian points out that these search warrant applications do not include the words "hack," "malware," or "exploit."[118] As Kevin Poulsen writes, "Instead the NIT comes across as something you'd be happy to spend 99 cents for in the App Store."[119] The Operation Torpedo warrant application, for example, merely revealed that "the web site would augment content with some additional computer instructions."[120] Another FBI affidavit states, "the exact nature of these commands, processes, capabilities, and their configuration is classified as a law enforcement sensitive investigative technique, the disclosure of which would likely jeopardize other on-going investigations and/or future use of the technique."[121] Recently, a federal judge in Washington indicated the practical effect of this concealment. The judge misinterpreted the use of the word "instructions" – thinking the word referred to a human following instructions as opposed to computer code – and failed to understand where the data obtained from the defendant came from.[122] As a result of this misunderstanding, the judge clashed with the public defender, confused as to how the FBI could have accessed information from the defendant's computer when "they [didn't] have his computer."[123] Without suitable transparency, the judiciary is unable to adequately oversee the warrant application process.

The government subscribes to a policy of revealing "as little information as possible" about how remote access search tools are utilized. In a redacted email from an FBI unit chief

---

government use of hacking tools, but explaining that most of the relevant magistrate judge orders are sealed).

118 Poulsen, *supra* note 21.

119 *Id.*

120 *See* In the Matter of the Search of Computers that Access the Website "Bulletin Board A," No. 8:12MJ3565 (D. Neb. Nov. 16, 2012), https://www.documentcloud.org/documents/1261620-torpedo-affidavit.html [https://perma.cc/MJ9E-ARUQ].

121 *See* Application and Affidavit for Search Warrant, *supra* note 77.

122 Joseph Cox, *Judge in FBI Hacking Case is Unclear on How FBI Hacking Works*, MOTHERBOARD (Jan. 27, 2016), http://motherboard.vice.com/read/judge-in-fbi-hacking-case-is-unclear-on-how-fbi-hacking-works [https://perma.cc/W9AM-88B8].

123 *Id.*

released to the public, the government stated that they "try to make every effort possible to protect the FBI's sensitive tools and techniques" in order "to ensure that the capabilities of the CIPAV are minimized [in future media reports], if discussed at all."[124] The email adds, "this and many tools deployed by the FBI are law enforcement sensitive and, as such, we request that as little information as possible be provided to as few individuals as possible."[125] Another redacted email instructs agents to avoid discussing how data collection works in warrant applications; affidavits; and conversations with case agents, U.S. Attorneys, squad supervisors, and outside agencies.[126] Although the Supreme Court has stated that the execution of warrants should generally be left to law enforcement,[127] judges may not be able to properly assess the invasiveness, effectiveness, and necessity of an electronic search tool without a sophisticated understanding of how it functions. As Kevin Poulsen writes, "Depending on the deployment, an NIT can be a bulky full-featured backdoor program that gives the government access to your files, location, web history and webcam for a month at a time, or a slim, fleeting wisp of code that sends the FBI your computer's name and address, and then evaporates."[128] The difference between these two instruments is significant and the limited information provided to judges leaves the judiciary ill equipped to distinguish between them.

Furthermore, there is no assurance that, once authorized, remote access searches will be used exclusively for the purposes the FBI claims in a given warrant application. In 2011, the largest European hacker club, Chaos Computer Club (CCC) reverse engineered a "lawful interception" malware program used by German law enforcement.[129] The CCC determined "that the Trojan's developers never even tried to put in technical safeguards to make sure the malware can

---

124 *See* Email from [redacted], Unit Chief, FBI Cryptologic and Electronic Analysis Unit to [redacted] (SE) (FBI) 10 (July 18, 2007, 5:35 PM), https://www.eff.org/document/fbicipav-08pdf [https://perma.cc/L83K-VZGA].

125 *Id.*

126 *See* Email from [redacted] (OTD) to [redacted] (OTD) (CON) et al. 11 (Aug. 15, 2004, 8:31 AM), *available at* https://www.eff.org/files/filenode/cipav/fbi_cipav-07.pdf [https://perma.cc/52MF-YF7J].

127 Jennifer Valentino-DeVries, *Judge Denies FBI Request to Hack Computer in Probe*, WALL ST. J. (April 24, 2013), http://online.wsj.com/news/articles/SB10001424127887324743704578443011661957422 [https://perma.cc/CL46-KA7U].

128 *See* Poulsen, *supra* note 21.

129 *Chaos Computer Club Analyzes Government Malware*, CHAOS COMPUTER CLUB (Oct. 8, 2011), http://ccc.de/en/updates/2011/staatstrojaner [https://perma.cc/RE2T-M3ZV].

exclusively be used for wiretapping internet telephony, as set forth by the constitution court."[130] The software included functionality to surreptitiously insert additional requests for information from the target's computer beyond the types approved by the court.[131]

The lack of minimization procedures and transparency raises important concerns regarding the use of remote search techniques. A formerly classified memo written by the DOJ's Computer Crime and Intellectual Property Section, exposes a similar concern: "While the [remote access search] technique is of indisputable value in certain kinds of cases, we are seeing indications that it is being used needlessly by some agencies, unnecessarily raising difficult legal questions (and a risk of suppression) without any countervailing benefit."[132]

B. Increased Frequency of Use

The DOJ does not anticipate that the Rule 41 amendments will greatly affect the frequency with which agents apply for remote access search and seizure warrants because out-of-district warrants are already permitted in certain circumstances. As the government has emphasized, the amendments to Rule 41 would not create new search techniques or weaken the standards for extraterritorial authorization for that technique. The DOJ states, "if conducting a remote search of a computer offers the government practical advantages over conducting a physical search of the same computer," one would expect to have already observed an increase in remote searches, which is not the case.[133] However, the DOJ does not account for the likely effect of enacting an explicit mandate for these two increasingly common circumstances. Currently, the out-of-district warrant exceptions to Rule 41 are confined to a set of narrow circumstances that occur with limited frequency. Conversely, the two circumstances that the amendments address could apply broadly and impact millions of individuals.

If Rule 41 is amended, the number of extraterritorial requests for remote access searches will likely grow as the number of users implementing anonymizing software increases. Following the summer of 2013, and the revelations made public by Edward Snowden, the average number of daily users on Tor more than doubled from 550,000 to over

---

130 *Id.*
131 *Id.*
132 Poulsen, *supra* note 3.
133 Memorandum from Jonathan Wroblewsi, *supra*, note 31, at 260.

1,200,000.[134] In November 2014, that number was well above 2,000,000.[135] As more users turn to Tor or other means of concealing their identity and location on the Internet, the government will likely increase its reliance on the exceptions promulgated in the amendments to Rule 41.

Similarly, the recent growth in botnets presents reason to believe that, if permitted, multi-district, multi-computer remote access searches would become commonplace. In 2014, botnet-operated attacks increased by 240%.[136] In fact, it is estimated that "as many as one quarter of all personal computers may now be participating in a botnet, unknown to their owners."[137] The number of attacks is expected to grow immensely as the marketplace for botnets continues to flourish.[138] As proposed, Rule 41 would become one of the FBI's primary weapons in the fight against botnets, and the frequency of out-of-district remote access searches would increase concurrently with the upsurge in botnet related crime. Additionally, the invasive nature of these searches would necessarily deepen as individual botnets become more sophisticated and infect unprecedented numbers of devices. The amendments, for better or for worse, would give the government the ability to seek, through a single ex parte hearing, authorization to remotely search and manipulate the millions of zombie computers in a given botnet network.

C. Fourth Amendment Concerns

The Advisory Committee suggested "the use of anonymizing software to mask the location of a computer should not prevent the issuance of a warrant if the investigators can satisfy the Fourth Amendment's threshold requirements for obtaining a warrant."[139] The Fourth Amendment requires that the

---

134 Lee Munson, *Tor Usage Doubles in August. New privacy-seeking users or botnet?*, NAKED SECURITY (Aug. 29, 2013), https://nakedsecurity.sophos.com/2013/08/29/tor-usage-doubles-in-august-new-privacy-seeking-users-or-botnet [https://perma.cc/L9HK-22XR].

135 *See Direct Users by Country*, TOR METRICS, https://metrics.torproject.org/userstats-relay-country.html [https://perma.cc/D7R5-A52S].

136 Lerner, *supra* note 25, at 239-240.

137 *Discover the Anatomy of a Botnet*, IT SECURITY WATCH, http://www.itsecuritywatch.com/internet-security/discover-the-anatomy-of-a-botnet [https://perma.cc/2BWT-7SRN].

138 *See* Lerner, *supra* note 25, at 3-7. HP Enterprise Services predicts that by the year 2020, "there will be another million people working in cybercrime globally." Stilgherrian, *Cyber Criminals Are Out-Spending the Defenders Two to One: HP*, ZDNET (Apr. 4, 2014), http://www.zdnet.com/cyber-criminals-are-out-spending-the-defenders-two-to-one-hp-7000028056 [https://perma.cc/HHH9-HLJG].

139 Memorandum from Hon. Reena Raggi, *supra* note 8, at 326.

government describe the target computer with particularity and demonstrate probable cause that the evidence sought will "aid in apprehension or conviction of a criminal."[140] However, the Advisory Committee made clear "the amendment[s] do[ ] not address [these] constitutional questions or attempt to influence their resolution."[141] Instead, the amendments leave the constitutional analysis to the courts.[142] This leaves the Rule 41 amendments vulnerable to attack under Fourth Amendment standards.

1. Lack of Probable Cause

For one, the government may have difficulty establishing that the information sought is necessarily related to criminal activity. In order to obtain a search warrant, the government's affidavit must establish probable cause, which requires "enough information for the issuing magistrate to determine that the items sought are related to the criminal activity under investigation, and that they may reasonably be expected to be located in the place to be searched."[143] In a watering-hole attack, it is unlikely that the government can demonstrate that the information seized from each person that visits a website over the course of the surveillance period will be related to the investigation. While there may be some websites for which access alone may violate the law – such as a website that upon visitation disseminates child pornography to the user – the vast majority of websites will be frequented by legitimate users for whom probable cause does not exist. "For example, members of the press, researchers, policymakers, and attorneys regularly visit websites associated with terrorist groups, cyber-criminals, and drug dealers."[144] In social engineering attacks – such as the FBI email to the MySpace bomber with a link to a fake AP story that actually delivered a CIPAV – it may seem unlikely that the FBI will collect information unrelated to the criminal activity under investigation. However, the target could forward the email to others or post the link to social media. Any innocent person that visited the website containing the fake news story would become subject to the search despite a lack of probable cause.

---

140 *Id.*

141 Memorandum from Sara Beale & Nancy King, *supra* note 54, at 158.

142 Memorandum from Hon. Reena Raggi, *supra* note 8, at 326.

143 Commonwealth v. Cefalo, 409 N.E.2d 719, 726 (Mass. 1980).

144 Am. Civil Liberties Union, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media, *supra* note 104, at 22.

2. The Particularity Requirement: Concerns and Counterarguments

Similarly, remote access search warrants may not satisfy the Fourth Amendment's particularity requirement. Warrants "must particularly describe the things to be seized, as well as the place to be searched."[145] The particularity requirement prevents the issuance of general warrants and warrants based on vague information.[146] The Supreme Court has stated that the Fourth Amendment's particularity requirement is especially important in the eavesdropping context.[147] Given that the government is unable to articulate either the location of the device to be searched or its IP address, there is reason to doubt the government's ability to meet the particularity requirement. In fact, in rejecting the FBI's warrant application, Judge Smith raised a number of questions regarding the affidavit's satisfaction of the particularity requirement and expressed concern that "[t]he Government's application contains little or no explanation of how the Target Computer will be found."[148]

Additional concerns with the particularity requirement arise in the government's investigations of botnets and attempts to simultaneously search multiple computers. The devices in these searches, all targeted by the same warrant, do not share one owner.[149] In the physical search context, the particularity requirement demands that a warrant specify each individual unit subject to search. When searching a building with multiple apartments, for example, the warrant must identify every apartment of interest to investigators. "Particularity concerns frequently arise in circumstances where the description in the warrant of the place to be searched is so vague that it fails reasonably to alert executing officers to the limits of their search authority."[150] It follows that "the same concerns and rules should apply when police search digital 'occupancies.'"[151] In granting a remote-access search warrant for multiple computers infected by the same botnet, courts are unable to properly limit the breadth of the applying agency's search authority.

---

145 Dalia v. United States, 441 U.S. 238, 239 (1979).

146 *See* Go-Bart Importing Co. v. United States, 282 U.S. 344, 357 (1931).

147 Berger v. New York, 388 U.S. 41, 56 (1967).

148 *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 760 (S.D. Tex. 2013).

149 *See* Greenstreet v. County San Bernardino, 41 F.3d 1306, 1309 (9th Cir. 1994).

150 U.S. v. Clark, 638 F.3d 89, 94 (2d Cir. 2011).

151 Am. Civil Liberties Union, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media, *supra* note 104, at 21.

There are, however, numerous counterarguments indicating that the government's remote access search techniques fit squarely within the parameters of the particularity requirement. A single warrant can be used to search more than one physical location or piece of property only if there is probable cause to search each location.[152] "A separate warrant for each suspected place to be searched is not called for either by the letter or the spirit of the constitution . . . To require it would occasion useless delay and expense, and tend to defeat the salutary objects of the law."[153] Additionally, in the context of tracking warrants – promulgated in Rule 41(b)(4) – the government seeks information from locations unknown at the time of the application. In *United States v. Karo*, the Supreme Court ruled that the particularity requirement is excused if the purpose of the search is, in fact, to determine the search area.[154] Furthermore, when collecting evidence from the Internet, the particularity requirement permits warrants "for individual suspects rather than individual Internet accounts."[155] That is, the government does not need to identify a specific account that is plausibly connected to the desired evidence. Rather, it need only specify that a given suspect has or will use the Internet to receive, store, or transmit evidence relevant to criminal activity.

3. Additional Fourth Amendment Concerns

However, even if remote access searches generally comport with particularity requirements, the warrants may authorize the seizure of broad swaths of information in violation of the Fourth Amendment. The capabilities of remote access search techniques – as identified above[156] – are vast, and their use would likely lead to the collection of information beyond just the user's location. Judge Smith determined that the sheer "volume of information" sought by the government did not amount to "only limited amounts of data" as the affidavit

---

152 Memorandum from Jonathan Wroblewsi, *supra* note 43 at 263.

153 Gray v. Davis, 27 Conn. 447, 455 (1858).

154 Memorandum from Jonathan Wroblewsi, *supra* note 43, at 260; *see also* United States v. Karo, 468 U.S. 705, 718 (1984) ("It will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance.").

155 Memorandum from Jonathan Wroblewsi, *supra* note 43, at 262 (citing Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1045-46 (2010)).

156 *See infra* Part II. C.

claimed.[157] Similarly, the Seventh Circuit concluded that when the information sought "is identical in its indiscriminate character to wiretapping and bugging" it cannot be authorized solely by a remote access warrant pursuant to Rule 41.[158] In the physical context, investigators cannot simply seize everything in a house if it poses no rational connection to the crime. As Laura Donohue stated, "you can't just go on a fishing expedition. There needs to be a nexus between the crime being alleged and the material to be seized. What they are doing here, though, is collecting everything."[159] This criticism is particularly applicable to searches of electronic devices. In its *Riley v. California* opinion, the Supreme Court emphasized that electronic devices, "as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[160]

But according to one member of the Advisory Committee, the government may not even need a warrant to acquire location information from botnet-infected devices.[161] Similarly, if the remote searches are solely sought for remediation purposes – such as removing the botnet from the zombie's computer – not the prosecution of the master, the Fourth Amendment concerns are less relevant. In these instances, the information collected would not be used at trial and thus the user would have no standing to exclude the fruits of the search.[162] However, these Fourth Amendment interests would remain relevant in a civil suit against the offending law enforcement agents.[163]

The Fourth Amendment requires extra scrutiny for certain capabilities of remote access search tools, principally contemporaneous and video surveillance. Although the FBI labels the real-time surveillance capabilities of remote access

---

157 *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 760 (S.D. Tex. 2013).

158 United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984).

159 Timberg & Nakashima, *supra* note 83.

160 Riley v. California, 134 S. Ct. 2473, 2489 (2014). The opinion goes on to explain that electronic devices hold a "cache of sensitive personal information," which expose "far more than the most exhaustive search of a house." *Id.* at 290-91.

161 Minutes of Advisory Comm. on Criminal Rules, *supra* note 64, at 520.

162 *Id.* at 525; *see also* United States v. Maceo, 873 F.2d 1, 6 (1st Cir. 1989) (concluding "[t]he only remedy available within the context of the criminal trial for fourth amendment violations is the exclusion of any evidence illegally obtained. In this case, the prosecutor did not attempt to admit any evidence concerning the examination. Thus, whether or not a violation has occurred, no remedy is available to Maceo during this criminal phase of his trial. [This holding does not foreclose other possible remedies (such as a civil suit against the offending Marshal) outside of this context if indeed there has been a violation.]").

163 *See* United States v. Maceo, 873 F.2d 1, 6 (1st Cir. 1989).

search tools – like the prospective collection of routing and destination information in the investigation of the MySpace bomb threats – as pen registers, they may, more accurately, be called trespassory searches. A pen register order is intended to compel "dialing, routing, addressing, or signaling information transmitted by" a device.[164] In contrast, the contemporaneous surveillance authorized pursuant to Rule 41 may be installed on a target device to monitor and collect information pertaining to all electronic communications originating from a device. This may fall within the definition of a Fourth Amendment search provided in *United States v. Jones*, which includes occasions when "the Government physically occupie[s] private property for the purpose of obtaining information."[165] Relatedly, in his denial of a remote access warrant, Judge Smith determined that the remote access search tool's ability to take photos with the device's camera amounted to a live video feed.[166] Accordingly, he ruled that the government did not satisfy the heightened Fourth Amendment warrant standards for video surveillance.[167]

Additionally, the amendments to Rule 41 will authorize remote access searches of all persons regardless of whether they are inside or outside of the United States. The government readily admits that it does not know where suspects using anonymizing technology are located. Before a warrant is executed, then, the FBI cannot know whether such suspects are located within or outside of the United States. Although the Fourth Amendment's warrant requirement does not apply to searches of non-U.S. persons outside of the country, these extraterritorial searches are subject to a "requirement of reasonableness."[168] Citing the presumption against international extraterritorial application, the DOJ insists that the amendments do not create authority for searches of electronic storage media located in foreign countries.[169] Yet the government also asserts, "should the media searched [pursuant to Rule 41] prove to be outside the United States, . . . the existence of the warrant would support the reasonableness of

---

164 18 U.S.C. § 3127(3) (2012).

165 United States v. Jones, 132 S. Ct. 945, 949 (2012).

166 *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 760 (S.D. Tex. 2013). The opinion sets out the four requirements of a warrant authorizing video surveillance in addition to probable cause – (1) use and failure of alternative investigative methods, (2) description of the particular communication sought, (3) statement of the duration of the order, (4) steps to assure minimization – ruling that the application failed to meet the first and fourth criteria. *Id.* at 760.

167 *Id.*

168 *In re* Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 157, 171 (2d Cir. 2008).

169 Letter from Mythili Raman, *supra* note 28, at 174-75.

the search."[170] Thus, according to this circular argument, approval of a remote access search pursuant to Rule 41 would, by default, authorize a search anywhere in the world. This interpretation has been the focus of significant media and public scrutiny.[171]

The significance of each Fourth Amendment concern is magnified by the fact that warrant applications are currently reviewed ex parte, without adversarial representation. While the judiciary is well suited to tackle complex questions of particularity, reasonableness, and probable cause, the cybercrime context introduces new gray areas that may merit adversarial briefing.[172] Without a technical understanding of Internet architecture – and no opportunity for oppositional consultation – a judge may be deprived of the tools needed to comprehensively evaluate the Fourth Amendment's reach in this context.[173] While wiretap orders are also granted ex parte,[174] a service provider must confirm the order's sufficiency. Conversely, once approved by a judge, remote access search warrants are implemented directly by the law enforcement agency with no third party check. Additionally, because judicial opinions related to warrants often go unpublished and are commonly sealed, the capacity for case law development to tackle these questions, as the Advisory Committee recommends, may be unrealistic.

D. Circumvention of Existing Legal Oversight Regimes

The searches authorized under the amendments to Rule 41 may circumvent existing legal regimes. Certain uses of remote access search techniques would ordinarily require additional showings and increased burdens under the Wiretap Act, 18 U.S.C. §2518 ("Title III").[175] These same criteria may not apply to the analysis of applications under the amended Rule 41 framework. When applying for a Title III warrant, the government must: describe, with particularity, the place and person to be surveilled; demonstrate that it has exhausted all other investigative alternatives; and ensure proper constraint on the duration of the surveillance and minimization of the collection of communications outside the scope of the warrant.[176] Additionally, the DOJ's Office of Enforcement

---

170 *Id.* at 174-75.
171 *See* Wilkins, *supra* note 113.
172 *See supra* note 2, at 18.
173 *Id.*
174 18 U.S.C. § 2518 (3) (2012).
175 The government must obtain a Title III warrant if it seeks to intercept wire, oral, or electronic communications in real time.
176 18 U.S.C. §§ 2518 (1), (4), (5) (2012).

Operations must review each wiretap application before it can be submitted to the court.[177] Warrants targeting a device's camera activate the heightened requirements for video surveillance imposed by Title III.[178] The same is true for mechanisms used to activate a device's microphone or to record contents of incoming or outgoing communications. Any attempt to conduct real-time surveillance necessarily requires compliance with the amplified strictures of 18 U.S.C. § 3123.[179]

Yet warrant applications for these same search methods pursuant to Rule 41 may be authorized without being subjected to the rigorous Title III requirements. Creating new exceptions to Rule 41's venue requirements may enable the FBI to avoid the heightened Title III burdens by applying for Rule 41 warrants instead. As such, a "warrant application submitted under Rule 41 may be constitutionally insufficient and infirm."[180]

Additionally, the altered Rule 41 notice requirements do not guarantee that all relevant parties will be notified of a remote access search. As drafted, the amendments would permit the government to provide notice to *either* "the person whose property was searched *or* whose information was seized or copied."[181] This means the individual who owns the remotely accessed device may never receive notification that his or her property was searched. Similarly, the actual owner of the seized information might not be provided notice of the search and thus would remain ignorant of his or her ability to challenge its constitutionality.[182] This is especially troubling for locations with publicly shared computers such as libraries and schools.

---

177 *See* Am. Civil Liberties Union, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media, *supra* note 104, at 18.

178 *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 753 (S.D. Tex. 2013). Even though Title III does not technically cover authorization of surreptitious video, courts have consistently imposed its requirements. *See also* United States v. Cuevas-Sanchez, 821 F.2d 248, 250 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504, 510-11 (2d Cir. 1986); United States v. Torres, 751 F.2d 875, 884 (7th Cir. 1984).

179 18 U.S.C. § 3123 (2012).

180 *See* Am. Civil Liberties Union, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media, *supra* note 104, at 18.

181 Proposed Amendments to the Federal Rules of Criminal Procedure, *supra* note 24, at 338 (emphasis added).

182 *See* Am. Civil Liberties Union, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media, *supra* note 104, at 24.

The amendment to Rule 41 could also have a significant impact on law enforcement and judicial practices, eventually leading the government to forum shop. The ACLU argues that the amendments would expand the judiciary's power to grant search warrants in two ways.[183] First, the amendments would broaden magistrate judges' jurisdictional authority, permitting a magistrate judge "in any district where activities related to a crime may have occurred" to issue the remote access search warrant.[184] In the cybercrime context, activities related to a crime often implicate conduct in multiple areas of the country, leaving the government with a plethora of districts to choose from when shopping a warrant. Second, the amendments would enable warrants that authorize searches both within and outside of a district. In the botnet context, for example, judges would be empowered to authorize multi-district, multi-computer search warrants with repercussions across many jurisdictions, despite differing circuit law and precedent. Combined, these two enlargements of authority could generate powerful forum shopping effects, allowing the FBI to systematically select the district considering its applications and potentially circumvent the legal protections put into place by the district where the warrant should actually have been evaluated.

E. Unintended Consequences

The amendments' enactment may bring about unanticipated consequences for the public and for law enforcement. First, the amendments may adversely affect Internet infrastructure, causing disruption to innocent third parties, weakening security for both the target of the search and law enforcement, and exposing the investigation to tampering. Second, the amendments may incentivize government stockpiling of zero-day exploits and use of surreptitious malware. Finally, as described above, the alterations to Rule 41 could lead to forum shopping by investigators.

1. Effect on Internet Population and Infrastructure

Remote access search techniques could inadvertently deny access to a target website or disrupt the functionality of a target computer. While altering a website's code during a watering-hole attack, the government may impede functionality of the website. As part of a 2013 watering hole

---

183 *See* Am. Civil Liberties Union, ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media, *supra* note 2.

184 Memorandum from Hon. Reena Raggi, *supra* note 8.

attack, the FBI deliberately caused all websites on a given server to cease transmission of their intended content, and instead display an error message.[185] This type of disruption could have an immense impact on websites and their owners. An online store taken offline for one day could lose $10,000 in sales.[186] Regardless of the site's functionality, the site itself could end up suffering even greater loss in reputational damage as a result of the malfunction.[187] Similarly, the installation of software on a user's computer could impede the device's utility. Although the affidavit filed in support of the Operation Torpedo warrant application makes assurances that "the NIT will not deny the user of the 'activating' computer access to any data or functionality of that computer," it does not provide any explanation or rationale to support its claims.[188]

The potential to disable a targeted computer becomes especially troubling in the botnet context. In these investigations, the targeted devices are owned and operated by innocent users who are victims of criminal activity. The Computer & Communications Industry Association notes, "attempting to hack botnets . . . can damage many of the computers connected to them."[189] Recently discovered malware, believed by some to be used by U.S. authorities in their surveillance efforts, "clearly impairs the operation of the target computers in multiple ways, including by draining battery life and using bandwidth and other computer resources."[190] Considering that victims of a botnet would neither be required to consent to the search nor receive notice in most cases, the harms would be particularly in conflict with their civil liberties.

Known flaws in surveillance software may weaken the security of both the target's and law enforcement's devices, as

---

185 *See* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013), http://www.wired.com/2013/09/freedom-hosting-fbi [https://perma.cc/26QJ-XAHW].

186 *The Economic Impact of Cybercrime and Cyber Espionage*, *supra* note 29, at 6.

187 *See id.*

188 *See* In the Matter of the Search of Computers that Access the Website "Bulletin Board A", No. 8:12MJ3565, at 31 (D. Neb. Nov. 16, 2012), https://www.documentcloud.org/documents/1261620-torpedo-affidavit.html [https://perma.cc/MJ9E-ARUQ].

189 *See supra* note 16.

190 Dennis Fisher, *Experts Question Legality of Use of Regin Malware by Intel Agencies*, THREAT POST (Nov. 25, 2014), http://threatpost.com/experts-question-legality-of-use-of-regin-malware-by-intel-agencies/109566 [https://perma.cc/6BLZ-LT6C].

well as expose the investigation to tampering.[191] When security researchers examined the surveillance software used by German law enforcement to remotely monitor targets, they were "shocked by the lack of even elementary security in the code."[192] Firstly, the targeted user faced potential privacy breaches because the files transmitted to law enforcement in the exfiltration stage were poorly encrypted.[193] This meant that individuals other than authorities could potentially view screenshots and listen to audio being captured.[194] Similarly, other surveillance software had backdoors permitting hackers to "gain access to the system . . . and listen to recorded calls without authentication."[195] Additionally, due to the poor craftsmanship of the software, third parties could actually use the law enforcement tool to penetrate the target's system.[196] Second, the software weakened the law enforcement agencies' own security, making it "conceivable that the law enforcement agencies' IT infrastructure could be attacked through this channel."[197] Finally, German law enforcement did not verify that the evidence collected actually originated from the target's computer.[198] Thus, law enforcement may instead have been analyzing imitated data.

Further, this is especially concerning in light of the well-documented flaws in the U.S. government's information technology procurement process.[199] Federal agencies reported more than 25,000 security breaches in 2013, which was more than double the amount reported in 2010.[200] This presents various concerns regarding the security and authenticity of the information gathered as well as the potential openings generated for hackers in both the target's and law enforcement's systems.

---

191 *See* Am. Civil Liberties Union, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media, *supra* note 104, at 9.

192 *See* CHAOS COMPUTER CLUB, *supra* note 129.

193 *Id.*

194 *Id.*

195 *Id.*

196 *Id.*

197 *Id.*

198 *Id.*

199 *See supra* note 2 (citing Craig Timberg and Lena H. Sun, *Some Say Health-Care Site's Problems Highlight Flawed Federal IT Policies*, WASH. POST (Oct. 9, 2013), http://www.washingtonpost.com/business/technology/some-say-health-care-sites-problems-highlight-flawed-federal-it-policies/2013/10/09/d558da42-30fe-11e3-8627-c5d7de0a046b_story.html).

200 Jeryl Bier, *Security Breaches of Personal Information at Federal Agencies More than Doubles Since 2009*, WKLY. STANDARD (Apr. 3, 2014), http://www.weeklystandard.com/blogs/security-breaches-personal-information-federal-agencies-more-doubles-2009_786450.html.

The FBI cannot predict every harmful consequence of surreptitiously disseminating code to a device. Expanding the circumstances under which remote access searches are permitted only increases the chances that such harms are realized. The warrant applications available to the public do little to address these fears of disruption and the amendments provide no additional safeguards. Judges are given insufficient information about the methods by which the search will be implemented and the precautions, if any, that have been taken to ensure ancillary harms are minimized.

One such harm is the infection of innocent users. In his rejection of the FBI's warrant application, Judge Smith acknowledged, "the Government's application offers nothing but indirect and conclusory assurance that its search technique will avoid infecting innocent computers or devices."[201] He considered the potential injuries generated by an investigation of a target computer in a public library, public Internet café, or workplace.[202] A remote access search could bring about devastating consequences if targeting a shared computer, whether used for public means or shared among friends or family. The government could inadvertently collect personal, identifying information about individuals unrelated to the crime, simultaneously violating those individuals' rights and sidetracking the investigation. When similar mistakes happen in the physical context, it is easy to recognize the harm. When the Washington, D.C. police used a battering ram to break into a home that the suspect had moved out of 18 months before, it was evident to the injured party that his privacy had been invaded.[203] But in the digital context, the wrongly targeted individuals may not even know they have been affected.

The potential to entangle innocent users in a remote access search is even greater in watering hole attacks. In fact, an FBI surveillance tool implemented in August 2013 evoked this very concern. The FBI used a watering-hole attack on all websites hosted by the Freedom Hosting server on the Tor network.[204] The mechanism caused altered websites to display an error message which secretly delivered hidden code to all visiting users, causing their devices to transmit identifying information to the FBI.[205] Although the FBI intended to collect information

---

201 *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 753 (S.D. Tex. 2013).

202 *Id.*

203 *See* Sommer Mathis, *D.C. Police Raided the Wrong House*, DCIST (Jan 26, 2010), http://dcist.com/2010/01/dc_police_raided_the_wrong_house.php [https://perma.cc/VDJ6-445Q].

204 *See* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, *supra* note 185.

205 *See id.*

on Tor users that frequented sites distributing child pornography, the mechanism inadvertently impacted all sites hosted by Freedom Hosting, including a number of legitimate sites that did not host illicit images, such as TorMail, "long considered the most secure anonymous email operation online."[206] The fact that a website is hosted on the same server as a website suspected of accommodating wrongdoing is not sufficient justification for sanctioning government-run hacks of every person that uses that website. "Law-abiding Internet users have no way of knowing if the sites that they are visiting are hosted on the same physical server as a site that facilitates illegal conduct."[207] This invasive conduct "weaken[s] the technology used by human rights workers and activists" and creates "the potential for innocent parties to wind up infected with government malware because they visited the wrong website."[208] Beyond the hypothetical harms posed by the search methods, the public ought to take issue with the government's lack of transparency and failure to support its assurances that innocent users will not be impacted.

2. Incentives for Government Stockpiling of Zero-Day Exploits

Under the proposed amendments, the government would have greater incentive to invest in exploitations that could be used to deliver remote access search tools. In order to utilize a social-engineering or watering-hole attack, law enforcement must exploit either out-of-date or vulnerable software on the target's computer. As such, the government can only infiltrate the suspect's device if two conditions are satisfied: first, the government must have knowledge of the vulnerability; and second, the targeted user must not have patched this

---

206 Darlene Storm, *FBI Behind Firefox Zero-Day Compromising Half of All Tor Sites*, COMPUTERWORLD (Aug. 5, 2013), http://www.computerworld.com/article/2473739/cybercrime-hacking/fbi-behind-firefox-zero-day-compromising-half-of-all-tor-sites-.html [https://perma.cc/92N6-54VK]. Although the FBI confirmed its involvement in the attack, neither the warrant application nor the court order in the case is available to the public. Thus, two explanations are reasonably possible: the judge authorized a broad warrant permitting the attack on a wide spectrum of websites, or the FBI exceeded the scope of the warrant in the course of the attack. Considering the sparse descriptions that these warrants usually include, it is also possible that the application was worded so broadly that the judge did not fully understand what he or she was sanctioning.

207 Am. Civil Liberties Union, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media, *supra* note 104, at 15.

208 *See* Poulsen, *supra* note 21.

vulnerability.[209] The first condition is accomplishable by dedicating resources to purchase or discover these exploits. In fact, a growing industry specializes in identifying security vulnerabilities to sell to governments as well as hackers.[210] To satisfy the second condition, the government can rely on the failure of users to update their software or its ability to convince manufacturers to delay patching vulnerabilities. Alternatively, the government can accomplish both conditions by investing resources into procuring zero-day exploits.

Zero-day exploits are those that even the manufacturer of the software does not know about and thus has not patched.[211] A recent leak of data from spyware developer Hacking Team shows that the company offered multiple zero-day exploits to its customers and provided services for a number of law enforcement agencies.[212] The FBI spent nearly $775,000 on the company's tools.[213] One leaked email makes clear that the FBI retained the Hacking Team's services for its Remote Control System tools, which came loaded with zero-day exploits.[214]

As software manufacturers and users update their software more regularly, zero-day exploits become the only feasible option to deliver remote access search tools. Due to recent modifications, Tor users are now more likely to patch vulnerabilities. "Until September of 2014, the Tor Browser Bundle did not include a built-in security update mechanism."[215] This left Tor users open to vulnerabilities that

---

209 *See* Am. Civil Liberties Union, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media, *supra* note 104.

210 Andy Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012), http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#5bb081066033 [https://perma.cc/KX3R-GEX5].

211 *See What is a Zero-Day Vulnerability?*, PC TOOLS, http://www.pctools.com/security-news/zero-day-vulnerability .

212 *See* Kim Zetter, *Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work*, WIRED (Jul. 24, 2015), http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work [https://perma.cc/3HH4-73PF]; *see also* Swati Khandelwal, *How Hacking Team and FBI Planned to Unmask a Tor User*, THE HACKER NEWS (July 15, 2015), http://thehackernews.com/2015/07/fbi-hacking-team-tor-network.html [https://perma.cc/DQT9-7YKK]; Sara Peters, *4 Lasting Impacts of the Hacking Team Leaks*, DARKREADING (July 15, 2015), http://www.darkreading.com/attacks-breaches/4-lasting-impacts-of-the-hacking-team-leaks/d/d-id/1321317 [https://perma.cc/9DN7-W2HW].

213 *See* Zetter, *supra* note 212; *see also* Khandelwal, *supra* note 212; Peters, *supra* note 212.

214 *See* Khandelwal, *supra* note 212.

215 *See supra* note 104 (citing mikeperry, *Tor Browser 3.6.5 and 4.0-alpha-2 Are Released*, TOR BLOG (Oct. 30, 2014),

had been discovered and patched by the developer but remained unpatched until the user manually downloaded the updates on his or her own. However, recent alterations to the Tor software introduced a mechanism that makes it more convenient and simple for Tor users to update the bundle.[216] Furthermore, efforts by independent users are making it more likely that the Tor software will soon update automatically,[217] which would greatly reduce the number of Tor users falling prey to known but unpatched vulnerabilities. This would, in turn, increase the government's reliance on zero-day exploits. Ultimately, expanding the FBI's license to use remote access searches would correspondingly increase government demand for zero-day exploits.

Dependence on zero-day exploits incentivizes the exploitation of vulnerabilities rather than the notification of manufacturers. The government's decision to prioritize offense over defense puts its own citizens at risk and is explicitly criticized by many both within and outside of the government. Former White House cybersecurity advisor Richard Clarke said in an interview, "if the U.S. government knows of a vulnerability that can be exploited, under normal circumstances, its first obligation is to tell U.S. users."[218] Similarly, the Review Group on Intelligence and Communications Technologies recently stated, "it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection."[219] However, the value in a zero-day exploit is only maintained if the government *does the exact opposite* and keeps the information secret until it can be used.

---

https://blog.torproject.org/blog/tor-browser-365-and-40-alpha-2-are-released [https://perma.cc/ZL58-TWRK]).

216 *Id.*

217 *See* phobos, *Google Funds an Auto-Update for Vidalia*, TOR BLOG (June 6, 2008), https://blog.torproject.org/blog/google-funds-auto-update-vidalia [https://perma.cc/5MAQ-TFGF]; *see also* Micah Lee, *Tor Browser Launcher*, MICAH LEE'S BLOG, https://micahflee.com/torbrowser-launcher [https://perma.cc/3R6F-AR6G] (describing an independent effort to create an automatic Tor security update delivery mechanism).

218 Joseph Menn, *Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback*, REUTERS (May 10, 2013), http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510 [https://perma.cc/GT5Z-K3XD].

219 PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMM'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 37, 220 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [https://perma.cc/6MNY-JGYY].

3. The Effects of Forum Shopping

The potential for forum shopping created by the amendments could propagate a system of "extraterritorial hacking," under which investigators could rely on magistrates in their local district or judges they know to be sympathetic to the law enforcement perspective.[220] While more convenient for the government, this practice implicates concerns regarding the proper forum in which suspects should file motions.[221] A suspect should not be forced to travel great distances in order to defend him or herself in a court of law and "courts should uniformly discourage forum shopping or judge selection."[222] Although out-of-district warrants are permitted in the ECPA context, Professor Orin Kerr argues that ECPA's multi-district warrant authority is justified by the deregulation of the telecommunications industry, which is not applicable to Rule 41.[223] Similarly, "if the arguments in favor of nationwide remote searches are persuasive, why are they not also persuasive for physical searches?"[224]

III. Suggested Alterations to Rule 41

In light of the concerns detailed above, the Rule 41 amendments currently under review by the Supreme Court must be modified. This section will outline these suggestions in three categories. First, this section will detail two major alterations to the Rule 41 amendments intended to limit the collection capabilities of remote access searches: (1) the exception for criminals using anonymizing software should only permit the collection of a user's IP address or MAC Address and (2) Rule 41 should not have an exception for violations of the CFAA. Second, Rule 41 should require the government to supply additional details and meet more rigorous standards in its warrant applications. This includes: satisfying a preliminary showing that the location of the concealed device cannot reasonably be ascertained without an extraterritorial remote access search; requiring a thorough and technical description of both the search tool's installation process and location collection method; and mandating the implementation

---

220 Memorandum from Orin Kerr to Members of the Rule 41 Subcomm. at 1-2 (Feb. 3, 2014), *in* Advisory Comm. on Criminal Rules, *supra* note 18, at 239-40.

221 *See id.*

222 United States v. Bailey, 193 F. Supp. 2d 1044, 1051 (S.D. Ohio 2002).

223 Memorandum from Orin Kerr to the Members of the Rule 41 Subcomm. 3-4 (Feb. 8, 2014), *in* Advisory Comm. on Criminal Rules, *supra* note 28, at 253-54.

224 *Id.*

and description of minimization and accountability measures to limit harm. Finally, this section will recommend that Rule 41 require the government to provide notice to both the owner of the property searched as well as the owner of the information seized.

A. Limitations on Remote Access Searches

1. Minimizing the Information Collected from Anonymous Users

Extraterritorial warrants targeting anonymous users should only authorize the collection of IP and MAC addresses. The government presents a compelling argument for carving out suspects who conceal their location from Rule 41's in-district venue requirement. However, the government has not presented an adequate justification for collecting more than basic identifying information. Limiting the scope of remote access search warrants would dispel many of the concerns detailed above while appropriately accounting for the hurdles impeding effective investigation and prosecution. After collecting a target's IP and MAC addresses, the FBI can then initiate further investigation procedures – whether through additional Rule 41 warrant applications, ECPA, Title III, or other avenues – if investigators think a greater amount of information is necessary.

An individual who employs an anonymizing service or frequents a hidden server on the Tor network ("User A") should not be subject to greater scrutiny than an individual who does not conceal his or her location ("User B"). To investigate User B, law enforcement agents would use his or her already available IP or MAC address to engage in a "first step" of surveillance and collection. This would include subpoenaing the user's ISP for information associated with the account and possibly applying for a search warrant, wiretap, or pen register trap and trace. When applying for a remote access search warrant, the government would not satisfy an exception to Rule 41's venue requirements and would have to go to a judge in the district where the device is located.

Investigating User A should be no different. The capabilities authorized pursuant to Rule 41's new exception should be limited to providing only that information the government would have had access to if User A had not utilized anonymizing technology. The extraterritorial warrant authorized in the investigation of User A should be viewed as a "step zero," necessary to permit the government to get to the first step of surveillance. While obtaining a list of programs running on User A's computer, installing a pen register to record the user's Internet activity, and enabling the user's

webcam could be *useful* in the investigation, none of these capabilities would have been available to law enforcement in its investigation of User B without consulting a judge in the proper district. These tools should not be available for use in the investigation of User A until step zero is accomplished. At that point, the government will be aware of the user's location and should direct any subsequent warrant applications to the appropriate district.

In Operation Torpedo, the government conducted an effective investigation despite the limited collection capabilities permitted by its remote access search warrant. The authorized watering-hole attack collected nothing more than the visitors' IP addresses, MAC addresses, and types of operating systems. The operation returned identifying information for over 25 site visitors, allowing the FBI to organize coordinated raids across the country and bring 14 suspects to trial.[225] This exemplary use of a watering-hole attack indicates that restricting the capabilities of remote searches to the simplest identifying information is practical and can achieve the results desired.

This limitation would lessen the harms generated through extraterritorial remote access searches. The collection of a user's IP address is less harmful to that user than the collection of his or her browsing history, email content, or other, more personal information. This applies to both legitimate criminal suspects and innocent users affected by an overly broad collection effort. Users of TorMail, whose data was inadvertently collected in the FBI's investigation of the Freedom Hosting server, fall into the latter category. These individuals would have faced far less harm if the government simply collected their IP addresses rather than their email communications and photographs.

Altering the amendment in this fashion would also reduce the likelihood of forum shopping because the government's choice of district would only affect the collection of IP and MAC addresses. If the government pursued a second warrant with more invasive capabilities, it would *have* to be in the district where the device is located. This would be more convenient for users who may challenge the collection of information and potentially make notification more feasible. Additionally, limiting the amendment would prevent the circumvention of existing legal oversight regimes. After collecting a target's IP address, law enforcement agents would be required to follow standard procedure to engage in more invasive surveillance tactics. Limiting the capabilities of the search such that law enforcement can only collect preliminary identifying

---

225 *See* Poulsen, *supra* note 21.

information would ensure Fourth Amendment compliance, as required by *United States v. Karo*.[226] It would also prevent the FBI from obtaining extraterritorial remote access search warrants for video and photography capabilities that require greater Fourth Amendment scrutiny.

2. Eliminating the Extraterritorial Exception for Botnet Investigations

Similarly, Rule 41 should not include an extraterritorial carve-out for botnets because the government's justification for such a need, rooted in efficiency, is not compelling. Either the Supreme Court or Congress should modify the amendments by removing the language permitting out-of-district authorization of simultaneous multi-district, multi-computer searches. Removing this exception would not affect the government's ability to collect information from and disseminate commands to zombies in a botnet network. It would merely require that the government apply for separate warrants in the corresponding district of each infected user. This change would eliminate Fourth Amendment concerns about whether multi-district, multi-computer search warrants satisfy the particularity requirement.

The long-term consequences of authorizing a government search of millions of innocent users are unknown. Those infected with a botnet are innocent strangers. The government should not be allowed to manipulate these users' computers based upon the power of a single warrant, especially given that these users are likely dispersed throughout the world. These concerns outweigh the government's desire to save investigatory and judicial time and energy. In fact, the "inefficiencies" worrying the government could serve as proper and necessary checks on authority.

The government can adequately eradicate botnets through more modest means. In recent years, the FBI has successfully hijacked and eliminated a number of botnets without being exempted from Rule 41's venue requirements. In 2011, the government initiated and won a civil suit in federal court to obtain a temporary restraining order. The order allowed the government to replace servers, collect IP addresses, and deliver a disabling command.[227] Also, DOJ and Microsoft formed a

---

[226] *See* Memorandum from Jonathan Wroblewsi *supra* note 31 and *supra* notes 144 and accompanying text. *United States v. Karo* held that the particularity requirement is excused if the purpose of the search is, in fact, to determine the search area. If only collecting preliminary identifying information, a remote access search would be doing just that.

[227] *See* Lerner, *supra* note 25 (citing Kim Zetter, *With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal*, *supra* note 33).

public-private partnership, by which Microsoft initiates civil suits based on trademark claims in order to mitigate and disable botnets around the world.[228] The government has multiple tools at its disposal to effectively immobilize botnet networks and alert innocent users of infections. Overhauling Rule 41's venue requirements for CFAA violations, and as a result placing innocent users' Fourth Amendment rights in jeopardy, is an unwarranted and egregious step under these circumstances.

B. Requiring Greater Detail in Warrant Applications

The amendments should be modified to require a preliminary showing that the location of the concealed device cannot reasonably be ascertained absent an extraterritorial remote access search. This alteration would impose a valuable check on the government, and even limit the frequency with which the new Rule 41 exclusions are used. Applying for an extraterritorial remote access search warrant should not be the FBI's first investigative undertaking. Instead, the government should expend reasonable efforts to determine a suspect's location and, if possible, appear in the appropriate court to obtain an in-district warrant. A recent study revealed, "81% of Tor users could be de-anonymized by analyzing router information."[229] If such a technique is feasible, the FBI can simultaneously avoid extraterritorial warrants while saving both investigatory and judicial time and resources.

Judge Smith recognized the need for more details in his rejection of the government's warrant application. He pointed to the hypocrisy in the FBI's simultaneous application for a remote access search warrant and an order under 18 U.S.C. § 2703 compelling an ISP to turn over all records related to the account. In its application for subscriber records pursuant to 18 U.S.C. § 2703, the government swore that the records would likely reveal information about the identities and locations of the users.[230] Yet the same agent swore in a separate affidavit to Judge Smith that no technique, other than a remote access search, was likely to succeed. Accordingly, Judge Smith ruled, "the Government cannot have it both ways."[231]

---

228 *See generally* Lerner, *supra* note 25.

229 Martin Anderson, *81% of Tor Users Can Be De-Anonymised by Analysing Router Information, Research Indicates*, THE STACK (Nov. 14, 2014), http://thestack.com/chakravarty-tor-traffic-analysis-141114 [https://perma.cc/M5LG-PXE6].

230 *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 764 (S.D. Tex. 2013).

231 *Id.*

The Supreme Court or Congress should look to Title III for language outlining the necessary level of detail for a warrant application. Title III contains a provision requiring "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[232] The DOJ opposes such a requirement because it could "lead to litigation over how much the government knew or could learn."[233] In the government's opinion, such a requirement could mandate the involvement of the National Security Agency and Central Intelligence Agency in order to demonstrate that the location of the targeted computer is unknown. However, the DOJ made concessions that "it might be possible to draft language that referred to the type of technology."[234] To accommodate the government's concerns, the new preliminary showing requirement could focus on the importance of using the technology requested, rather than the government's knowledge. As applied, the rule would mandate a preliminary showing that the government expended all reasonable resources to determine the suspect's location, without reference to the government's actual knowledge at the time of application.

The Supreme Court or Congress should also modify the amendments to mandate an individualized and detailed description of the technical process the government will use to install the remote access search tool and collect location information. This change would increase oversight of the technical search techniques authorized by Rule 41.[235] It would also bolster transparency in the Rule 41 extraterritorial warrant application regime.[236] Transparency would mitigate the collateral harm to targets, innocent third parties, the government, and Internet infrastructure generally. Currently, the FBI only discloses that the search tool will alter the suspect's device and collect information. This is not adequate. Instead, the warrant should include, in thorough detail, a step-by-step list of how the remote access search tool will be installed on the device as well as an explicit and technical rundown of how the search tool will alter the targeted device. The government's argument that revealing sensitive and classified techniques could jeopardize other investigations is not compelling. Even if transparency did threaten future investigations, the government could be given the opportunity

---

232 18 U.S.C. § 2518(1)(c) (2012).

233 *See* Minutes of Advisory Comm. on Criminal Rules, *supra* note 68, at 15.

234 *Id.*

235 *See id.* at 8.

236 *See supra* Section IV.A.

to request that the sensitive and classified details be redacted when the affidavit and opinion are published. This would enable a judge to rule on a warrant application with sufficient insight into the process while eschewing government concerns over investigative effectiveness. Requiring detailed, technical descriptions is especially important considering the lack of adversarial representation, and does not necessarily bar the government from keeping certain information inaccessible to criminals.

Finally, Rule 41 should mandate that the warrant application include a section discussing minimization and accountability measures. In particular, the government should aim to protect third parties, prevent the malicious code from disrupting the user's device, and defend both the target and government's systems from security breaches. Mandating a discussion of minimization and accountability would be a major improvement on the current warrant-application requirements. As Judge Smith suggested, "the Government has offered little more than vague assurances."[237]

While the transparency argued for above would be most effective in ensuring that the government avoids inflicting external harm, two additional stipulations would help. First, when implementing watering-hole attacks, the government should be required to list each site it intends to alter. This would prevent the type of mistake that occurred during the Freedom Hosting investigation, when a remote access search was conducted on thousands of innocent users. Second, Rule 41 should require that the government post a bond commensurate to the risk posed to individuals and businesses that could potentially face disruption through the search process. This would hold the government accountable in the case of a failed piece of surreptitious code that accidently crashes a website or disrupts a device.

C. Notice to All Relevant Parties

The Supreme Court or Congress should revise Rule 41's notice requirements for remote access searches. Rule 41 should compel the government to make reasonable efforts to serve a copy of the warrant on both the person whose property was searched *and* the person whose information was seized or copied. The additional requirement does not burden law enforcement agents significantly but provides the necessary assurance that all relevant parties will be made aware of the search. It is important to note that, if either the Supreme Court

---

[237] *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 764 (S.D. Tex. 2013).

or Congress limits extraterritorial remote access searches to the collection of IP and MAC addresses as suggested above, this expanded notice requirement would no longer apply to extraterritorial searches. Because IP and MAC addresses provide information about the owner of the computer, the person whose property was searched would be the same person whose information was seized. However, the alteration to the notice requirement would remain important outside of the extraterritorial warrant context, for which the full gamut of remote access search capabilities would remain available. As such, the notice requirement should be altered to protect users whenever the owner of property searched is different from the owner of the information seized.

CONCLUSION

Although the amendments to Rule 41 merely seek to extend extraterritorial warrant authority to two emerging cybercrimes, these changes, if unchecked, could effectively transform remote access search warrants into ubiquitous surveillance tools. The government's desire to create an exception for violations of the CFAA in multiple districts – including botnet attacks – is based in practicality and efficiency. While this element of the Rule 41 amendments could promote frugality in the criminal justice system, the preservation of government resources does not justify the authorization of multi-district, multi-computer searches of millions of individuals by a single court order.

However, the necessity for extraterritorial remote access search warrants to determine the location of users concealing their online identities is compelling. Creating an explicit exception for users implementing anonymizing techniques is critical to ensuring that the FBI can prevent grave, Internet-based crimes. But the need for extraterritorial authority only extends to the acquisition of a user's most basic identifying information. After collecting the user's IP or MAC address, the FBI can, and should, continue its investigation as if the suspect had never concealed his or her identity in the first place. Furthermore, the amendments, as currently drafted, do not provide the judiciary with sufficient resources or information to competently assess the legality and consequences of remote access searches. Supplementing Rule 41 with the necessary oversight and transparency regimes, as well as requiring more detailed information from law enforcement, will alleviate this concern and help reduce the unnecessary harms caused by remote access searches.