Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure

Richard M. Thompson II
Legislative Attorney

September 8, 2016

Congressional Research Service
7-5700
www.crs.gov
R44547

CRS REPORT
Prepared for Members and
Committees of Congress

Contents

Appendixes

Contacts

Summary

With the Rules Enabling Act, Congress granted to the Supreme Court the authority to write federal rules of procedure, including the rules of criminal procedure. After several years of evaluation by the Judicial Conference, the policy-making arm of the federal judiciary, on April 28, 2016, the Supreme Court transmitted to Congress proposed changes to Rule 41 of the Federal Rules of Criminal Procedure. These proposed changes would amend the federal search and seizure rules in two ways. First, they would permit the government to remotely access electronic devices although the location of the device may be unknown. This issue has become more pressing in recent years with an increasing number of users anonymizing their communications, hindering the government's ability to pinpoint the location of the target, and thus making it difficult to discern the appropriate federal court to apply for a search warrant. Second, they would permit DOJ to search multiple computers in numerous districts as part of a large-scale investigation of computer crimes.

In recent years, a tension has arisen between Rule 41 as currently drafted and the Department of Justice's (DOJ's) desired use of the rule for digital searches. One facet of this problem arose in a 2013 magistrate judge's ruling from the Southern District of Texas, in which the court denied DOJ's application to conduct remote searches of a computer believed to have been part of a fraudulent scheme. The court declined to grant the DOJ's application because the government could not establish the location of the target, thereby placing the proposed search outside the scope of Rule 41 and in violation of the Fourth Amendment particularity requirement.

There have been at least two lines of argument against the proposed rule change, one based on the substance of the proposed amendment and the other grounded in the process by which the rule is being changed. The substantive arguments pertain to the actual substance of the rule and include, for example, an argument that the new rule would breach the particularity requirement of the Fourth Amendment. The procedural arguments pertain to how this potential authorization should be made law: through the rulemaking process by the courts or through enacted legislation by Congress. While federal law enforcement has been supportive of the proposed change, some advocacy groups have argued that the proposed rule change "would have significant legal and technical implications" and thus "merit[s] open consideration by Congress, rather than a rulemaking proceeding of the Judicial Conference."

This report provides a brief overview of the proposed amendment to Rule 41. First, it provides background on the origin of, and rationale underlying, the proposed amendment and a description of the rule as currently written. Second, it reviews the potential changes made by the proposed amendment and surveys various concerns commenters have raised with the proposal.

With the Rules Enabling Act,[1] Congress granted to the Supreme Court the authority to write federal rules of procedure, including the rules of criminal procedure. After several years of evaluation by the Judicial Conference, the policy-making arm of the federal judiciary,[2] on April 28, 2016, the Supreme Court transmitted to Congress proposed changes to Rule 41 of the Federal Rules of Criminal Procedure.[3] These proposed changes would amend the federal search and seizure rules to permit the government to remotely access electronic devices although the location of the device may be unknown. This issue has become more pressing in recent years with an increasing number of users anonymizing their communications, hindering the government's ability to pinpoint the location of the target, and thus making it difficult to discern the appropriate federal court to apply for a search warrant.[4]

In recent years, a tension has arisen between Rule 41 as currently drafted and the Department of Justice's (DOJ's) desired use of the rule for digital searches. One facet of this problem arose in a 2013 magistrate judge's ruling from the Southern District of Texas, in which the court denied DOJ's application to conduct remote searches of a computer believed to have been part of a fraudulent scheme.[5] The court declined to grant the DOJ's application because the government could not establish the location of the target, thereby placing the proposed search outside the scope of Rule 41 and in violation of the Fourth Amendment particularity requirement.

There have been at least two lines of argument against the proposed rule change, one based on the substance of the proposed amendment and the other grounded in the process by which the rule is being changed. The substantive arguments pertain to the actual substance of the rule and include for example, an argument that the new rule would breach the particularity requirement of the Fourth Amendment.[6] The procedural arguments concern how this potential authorization should be made law: through the rulemaking process by the courts or through enacted legislation by Congress.[7] While federal law enforcement has been supportive of the proposed rule change,[8] some advocacy groups have argued that the proposed change "would have significant legal and technical implications" and thus "merit[s] open consideration by Congress, rather than a rulemaking proceeding of the Judicial Conference."[9]

---

[1] *See* 28 U.S.C. §§ 2071-77.

[2] *See* 28 U.S.C. § 331 ("The Conference shall also carry on a continuous study of the operation and effect of the general rules of practice and procedure now or hereafter in use as prescribed by the Supreme Court for the other courts of the United States pursuant to law. Such changes in and additions to those rules as the Conference may deem desirable to promote simplicity in procedure, fairness in administration, the just determination of litigation, and the elimination of unjustifiable expense and delay shall be recommended by the Conference from time to time to the Supreme Court for its consideration and adoption, modification or rejection, in accordance with law.").

[3] *See* Rules Package in Support of Amendments to Federal Rules of Procedure 201 (Apr. 28, 2016), *available at* http://www.uscourts.gov/file/document/2016-04-28-final-package-congress [hereinafter Rules Package].

[4] *See* DOJ Memorandum to Members of Criminal Rules Advisory Committee (March 17, 2014), *in* Advisory Committee on Criminal Rules, Agenda Book April 7-8, 2014 (April 2014), *available at* http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-april-2014 [hereinafter Agenda Book, April 7-8, 2014].

[5] *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013).

[6] *See* Particularity of Search, *infra* p. 7.

[7] *See* Process Concerns, *infra* p. 7.

[8] *See* Rationale for Amendment, *infra* p. 7.

[9] Written Statement, Center for Democracy and Technology, Before the Judicial Conference Advisory Committee on Rules (Oct. 24, 2014), *available at* https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0009 [hereinafter CDT, Written Statement].

This report provides a brief overview of the proposed amendment to Rule 41. First, it sets out background on the origin of, and rationale underlying, the proposed amendment and a description of the rule as currently written. Second, it reviews the potential changes made by the proposed amendment and surveys various concerns commenters have raised with the proposal.

Background on Amendment to Rule 41

Rule 41 of the Federal Rules of Criminal Procedure governs the procedures for obtaining a search warrant in federal court.[10] Among other elements, Rule 41 primarily requires a government official to demonstrate probable cause that evidence of a crime will be found in the place to be searched.[11] As to the question of venue—that is, which is the appropriate federal district court to seek a search warrant—Rule 41 provides that a search warrant may be issued by "a magistrate judge with authority in the district."[12] In a 2013 ruling from the Southern District of Texas, discussed below, the court found that although Rule 41 permits extraterritorial warrants (a warrant to be served outside of that judge's jurisdiction) in limited situations, the factual predicates to obtaining one were not present there.[13]

Rule 41 permits the issuance of extraterritorial warrants in four limited instances: (1) the property is within the jurisdiction but may be moved out of the jurisdiction before the warrant is executed; (2) the property is part of an investigation of domestic or international terrorism; (3) tracking devices are used which can be monitored outside the jurisdiction if installed within the jurisdiction; or (4) the property is located in a U.S. territory or U.S. diplomatic or consular mission.[14] However, based on the text of the rule, none of these exceptions appear to permit searches where the location of the target is unknown, such that it is not clear in which jurisdiction to request a warrant.

The amendment to Rule 41 approved by the Supreme Court and now before Congress would expand the instances in which DOJ could seek extraterritorial warrants. More broadly, it would codify DOJ's ability to "to use remote access to search electronic storage media and to seize or copy electronically stored information," an authority that is not explicitly found in the rule now. Before looking at the amendment, it is helpful to understand some of the background and cases behind the current version of Rule 41.

The universe of reported cases in which DOJ has relied on the current version of Rule 41 to remotely access a target's computer is small, but does shed light on how DOJ might use amended Rule 41 if adopted. The federal government's ability to remotely access computers as part of a criminal investigation was first revealed in 2001 when journalists discovered the existence of "Magic Lantern," later renamed the "Computer and Internet Protocol Address Verifier," a covert project used by the FBI to hack into a target's computer.[15] Known more generally as "network investigative techniques" (NIT), this technology can be used to gather both *metadata* from a computer, such as the Internet Protocol (IP) address of a target's computer, and the *content* of data stored on that computer, such as email communications or photographs.

---

[10] FED. R. CRIM. P. 41.

[11] *Id.* at (d)(1).

[12] *Id.* at (b)(1).

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

[14] FED. R. CRIM. P. 41(b)(2-5).

[15] *See FBI Sheds Light on "Magic Lantern" PC Virus*, USA TODAY (Dec. 13, 2001), *available at* http://usatoday30.usatoday.com/tech/news/2001/12/13/magic-lantern.htm.

The first publicly reported court case which relied on a NIT was in 2007, where the government obtained a Rule 41 search warrant to identify a Myspace user who had made bomb threats to a high school.[16] The warrant permitted the government to access the computer's IP address, MAC address, and other identifying information, but explicitly did not permit access to the content of any electronic messages.[17] In a similar case from 2013, law enforcement officials were investigating a series of threats to detonate bombs at universities and airports scattered throughout the United States.[18] The FBI sought and received a warrant from a magistrate judge of the U.S. District Court for the District of Colorado that permitted the FBI to access, among other information: the target computer's IP address; MAC address; the computer's open communication ports; a list of programs running on the computer; the type of operating system running on the computer; the web browser running on the computer; the computer's time zone information; and the Uniform Resource Locators (URLs) to which the target computer was previously connected.[19] In these cases, the FBI used a "phishing attack," in which it sent an email embedded with a link to the target of a search.[20] Once the user hit the link, it connected to FBI computers and downloaded malicious software that sent vital identifying information back to the FBI. Ultimately, the software produced two IP addresses which suggested the suspect was located in Tehran, Iran.[21]

In addition to targeting specific computers, DOJ has also targeted nefarious websites more broadly. In 2012, for instance, the government initiated Operation Torpedo, which involved the take down of a large-scale online child pornography network, users of which utilized the Tor network to anonymize their identities when accessing the website.[22] There, the magistrate judge issued a warrant to install a NIT that would collect the IP addresses and other identifying information from visitors to the child pornography site,[23] a technique known as a "watering hole" attack. Ultimately, based on this information, 14 individuals were brought to trial on child pornography charges.[24]

In addition to obtaining addressing information, remote access searches can also be used to activate the microphones in certain cell phones and laptops to record conversations without the

[16] *See In Re* Any Computer Accessing Electronic Message(s) Directed to the Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Message(s) Delivered to that Account By the Government, No. 3:07-mj-05114-JPD (W.D. Wash. June 22, 2007).

[17] *Id.* A "MAC" address or "Media Access Control" address is a "globally unique identifier assigned to network devices, and therefore it is often referred to as hardware or physical address. *See* What is a MAC Address, https://www.iplocation.net/mac-address (last visited September 8, 2016).

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

[19] Third Amended Complaint, *In Re* Search of Network Investigative Technique ("NIT") for Email Address Texan.Slayer@yahoo.com, No. 12-sw-05685 (D. Colo. Dec. 11, 2012).

[20] Timberg & Nakashima, *supra* note 18.

[21] *Id.*

[22] See Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End up In Your Computer*, WIRED (Aug. 5, 2014), *available at* https://www.wired.com/2014/08/operation_torpedo.

[23] Application for a Search Warrant, *In re* Search of Computers that Access the Website "Bulletin Board A," No. 8:12-mj-0356 (April 16, 2014).

[24] Poulsen, *supra* note 22.

user knowing.[25] Additionally, the FBI has stated that it can access the camera on laptops without activating the light which lets users know it is recording.[26]

Perhaps the most prominent case for purposes of the proposed Rule 41 amendment is a 2013 magistrate judge's ruling from the Southern District of Texas in which the government's request to conduct covert searches was denied.[27] There, the government requested a search warrant to remotely search an unknown computer in an unknown location that was believed to have been used to perpetrate a fraudulent scheme.[28] The government wanted access to, among other things, IP addresses used; records of Internet activity, including browsing history and search terms used; and photographs taken using the computer's built-in camera.[29] Magistrate Judge Stephen Smith rejected the government's application on two grounds. First, Judge Smith found that the government's application did not meet one of the territorial limitations found in the Rule.[30] Again, Rule 41 permits extraterritorial warrants in four limited instances, but does not cover instances where the location of the target is simply unknown from the outset. Second, he found that the application failed to meet the particularity requirement contained in the Fourth Amendment, which requires that "no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*,"[31] as the government failed to explain how the target device was to be found.[32] Further, Judge Smith noted the risk of targeting innocent computers when the location of the target is unknown.[33]

Amendment Process

The proposal to amend Rule 41 was first brought to the attention of the Judicial Conference in a September 2013 memorandum from DOJ, which highlighted two "increasingly common situations" faced by investigators that warranted a change in the rules.[34] The first is where the warrant sufficiently describes the device to be searched, but law enforcement officials do not know the location of the target device. The second is where the investigation requires officials to engage in surveillance of numerous computers in multiple jurisdictions. The proposed rule change was published for public comment in August 2014, in which DOJ, privacy advocates, computer experts, and members of the general public offered various arguments for and against the proposed rule change.[35] On April 28, 2016, the Supreme Court transmitted the proposed rule

[25] *See* Jennifer Valentino-DeVries and Danny Yadron, *FBI Taps Hacker Tactics To Spy on Suspects*, WALL STREET JOURNAL (Aug. 3, 2013).

[26] *See* Timberg & Nakashima, *supra* note 18.

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

[28] *Id.* at 755.

[29] *Id.* at 755-56.

[30] *Id.* at 758.

[31] U.S. CONST. amend. IV (emphasis added).

[32] *In re Warrant*. 958 F. Supp. 2d at 759.

[33] *Id.*

[34] Memorandum, Department of Justice to Advisory Committee on Criminal Rules 2 (Sept. 18, 2013), *in* Agenda Book, April 7-8, 2014, *supra* note 4, at 172.

[35] *See* Docket Folder, Proposed Amendments to the Federal Rules of Criminal Procedure (last visited Sept. 5, 2016), *available at* https://www.regulations.gov/docket?D=USC-RULES-CR-2014-0004.

change to Congress. Pursuant to the Rules Enabling Act, unless Congress responds via enacted legislation, the proposed rule will take effect on December 1, 2016.[36]

Upon transmittal of the proposed amendment to Rule 41, Senator Ron Wyden and Representative Ted Poe introduced companion bills (S. 2952, H.R. 5321) to reject this rule change. Each bill provides as follows:

> The proposed amendments to rule 41 of the Federal Rules of Criminal Procedure, which are set forth in the order entered by the Supreme Court of the United States on April 28, 2016, shall not take effect.[37]

Proposed Amendment

The proposed amendment was designed to address two issues: (1) access to a device at an unknown location; and (2) access to multiple computers in multiple districts. Each will be addressed in turn.

Searches of Devices with Unknown Locations

The first rationale for amending Rule 41 applies to situations when the government is able to describe the computer to be searched, but does not know the location of the computer. DOJ asserted, and the Judicial Conference accepted, that the government faces this situation more regularly because persons who commit crimes on the Internet are using anonymizing technologies with greater frequency.[38] Through the use of proxy servers, criminals are able to mask their IP addresses such that the recipient only knows the IP address of the proxy and not the originator's IP address.[39] This issue of knowing the computer to be searched but not its location was the primary issue facing the court in the Southern District of Texas ruling, a case that was cited by DOJ as a motivating factor in seeking the amendment to Rule 41.[40]

To permit extraterritorial searches, Rule 41 would be amended to read as follows:

> a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if ... (A) the district where the media or information is located has been concealed through technological means[.][41]

It appears that the government would have to demonstrate two elements: (1) that activities of the crime occurred in the magistrate judge's jurisdiction, and (2) that the location of the target has been concealed through technological means. Note that the first element—"any district where activities related to the crime may have occurred"—is the same as that found in the provision for extraterritorial searches as part of a terrorist investigation—"any district in which activities

[36] 28 U.S.C. §2074.

[37] S. 2952, 114th Cong. (2016); H.R. 5321, 114th Cong. (2016).

[38] Advisory Committee on Criminal Rules, Agenda Book, Meeting of March 16-17, 2015, at 88 (2016), *available at* http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015 [hereinafter Agenda Book, March 16-17, 2015].

[39] *Id.*

[40] *See* Memo from Mythili Raman, Acting Assistant Attorney General, to Reena Raggi, Chair, Advisory Committee on the Criminal Rules 172 (Sept. 18, 2013), *in* Agenda Book, April 7-8, 2014, *supra* note 4.

[41] *See* Rules Package, *supra* note 3, at 222.

related to the terrorism may have occurred."[42] Additionally, beyond permitting extraterritorial searches, this amendment would codify the authority to engage in "remote access" searches altogether, something that is not explicitly found in the current text of the rule.

Multi-device, Multi-district Searches

The second rationale for amending Rule 41 applies to situations where the government needs to search multiple computers in numerous districts as part of a large-scale investigation of computer crimes.[43] Under the current rule, there are limited mechanisms for seeking a warrant outside of the judicial district in which a computer is located, but none cover the type of authorization DOJ seeks here.[44] In its submission to the Judicial Conference, DOJ argued that effective investigation of large-scale online attacks, such as botnets—an "interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals"[45]—requires a change to Rule 41 such that government officials can seek authorization in one district court, although the criminal activity may span multiple districts.[46]

As submitted to Congress, the second prong of the proposed rule change reads as follows:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if ... (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.[47]

Issues Raised by Proposed Amendment to Rule 41 in Public Comments

As part of the review process, the Advisory Committee received comments both supporting and opposing the proposed amendment to Rule 41. The Advisory Committee noted that "the most common theme in the comments opposing the amendment was concern that it relaxed or undercut the protections for personal privacy guaranteed in the Fourth Amendment."[48] Objectors made other arguments against the proposal including that it might engender forum shopping. This section will briefly explore these and other concerns raised by public comments.

Rationale for Amendment

Commenters have proffered various arguments in support of the proposed rule change. First, and perhaps most obviously, is the fact that DOJ has been prevented in at least one reported ruling

[42] Fed. R. Crim P. 41(b)(3).

[43] *Id.* at 89.

[44] FED. R. CRIM. P. 41(b)(2)-(5).

[45] *See* What is a Botnet Attack?—Definition, Kaspersky Lab (last visited June 29, 2016), https://usa.kaspersky.com/internet-security-center/threats/botnet-attacks#.V3QTpfkrJbU.

[46] *See* Agenda Book, April 7-8, 2014, *supra* note 4, at 156.

[47] *See* Rules Package, *supra* note 3, at 223. Federal law outlaws the transmission of a program or command with the intent to damage a computer system. *See* 18 U.S.C. §1030(a)(5).

[48] Memorandum from Reporters to Advisory Committee on Rules, Rule 41 (Feb. 25, 2015), *in* Advisory Committee on Criminal Rules, Agenda Book, March 2015, *supra* note 38, at 90.

from remotely searching a target's computer when it could not state the location of the target. More generally, DOJ has argued that criminals are using anonymizing techniques more frequently, so that DOJ is able to identify the computer but not the location of the target. In this vein, DOJ has argued that "there is a substantial interest in catching and prosecuting criminals who use anonymizing technologies, but locating them can be impossible for law enforcement absent the ability to conduct a remote search of the criminal's computer."[49] As noted by the Judicial Conference, DOJ "could not now obtain a warrant even by going to every one of the 94 judicial districts, since it would not be able to establish that the property to be searched was located in any of these districts."[50] As to the second proposed change, which would most directly implicate the investigation of botnet-like schemes that involve many computers in many districts, the National Association of Assistant United States Attorneys argued that coordinating many requests and review by many magistrate judges "not only wastes judicial and investigative resources, but also may cause delay that impedes investigation."[51] Similarly, DOJ noted that in certain large-scale botnet investigations, the government would have to go to 94 federal courts in 94 judicial districts, a task "impossible as a practical matter."[52]

Particularity of Search

Opponents of the proposed amendment to Rule 41 have argued that it would violate the particularity requirement of the Fourth Amendment. The Fourth Amendment requires that no warrant shall issue unless it "*particularly describe[s] the place to be searched, and the persons or things to be seized*."[53] There are several different iterations of the argument that Rule 41 could authorize practices inconsistent with the particularity requirement, depending on the type of hack the government is attempting to employ.

One civil liberties group argues that with "watering hole" attacks, in which the government configures a website to deliver malware to every computer that visits it, the government "will end up searching the computers of people who it cannot particularly identify or describe and to whom it lacks probable cause."[54] Although there may websites that have no legitimate lawful purpose (e.g., terrorist websites), there may be valid reasons for visiting these sites (e.g., research, journalism).

Even with more targeted surveillance that might be performed by law enforcement, such as including a link in an email directed at a specific target, the civil liberties advocate notes that the target could easily forward the message to an innocent third party in which the government would not have probable cause to search.[55] A similar concern was raised by Magistrate Judge Smith in the Southern District of Texas Rule 41 ruling. There, Judge Smith described the government as having offered little to no information on how the targeted computer was to be found, and Judge

[49] *See* Agenda Book, April 7-8, *supra* note 4, at 172.

[50] Agenda Book, March 16-17, 2016, *supra* note 38, at 91.

[51] *See* Written Comment on Rule 41, National Association of Assistant United States Attorneys (Feb. 4, 2015), *available at* https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0027.

[52] *See* Letter, Mythili Raman, Acting Assistant Attorney General, to The Honorable Reena Raggi, Chair, Advisory Committee on the Criminal Rules 3 (Sept. 18, 2013) *in* Agenda Book, April 7-8, *supra* note 4, at 173.

[53] U.S. CONST. amend. IV (emphasis added); Groh v. Ramirez, 540 U.S. 551, 557 (1978).

[54] *See* Amer. Civil Liberties Union, Second Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media 22 (Oct. 31, 2014), *available at* https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0013ACLU [hereinafter ACLU, Second Comment].

[55] *Id.*

Smith also suggested that a sophisticated target might "spoof" a fake IP address, such that the search technique could infect innocent devices.[56]

In the context of botnets, one advocacy group claimed that that the proposed amendment would allow the police to search multiple computers using one warrant, "often without particularly describing those computers or demonstrating probable cause as to their owners or users."[57] Courts have noted that with multiple-location search warrants, the magistrate must be careful to evaluate each location separately: "A search warrant designating more than one person or place to be searched must contain sufficient probable cause to justify its issuance as to each person or place named therein."[58] One commenter argues that this same rule should apply when multiple computers, instead of multiple residences, are involved, as "[t]he need for particularity . . . is especially great in the case of eavesdropping."[59]

In response to these concerns, the Advisory Committee included a Committee Note to Rule 41, providing the following explanation about how the Fourth Amendment should apply to the proposed amendment:

> The amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media or seizing or copying electronically stored information, leaving the application of this and other constitutional standards to ongoing case law development.[60]

However, some privacy advocates believe that this proviso will be largely ineffective. For example, the one privacy advocate noted that while "the Committee does not seek to address such questions in this rulemaking, the proposed modification to Rule 41 nonetheless does have direct bearing on these very questions since it specifically contemplates the issuance of warrants for computers in concealed locations."[61]

Circumvent Existing Laws

Some have argued that, in certain situations, remote access searches can only be conducted using an order under Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[62] commonly referred to as the Wiretap Act, and not a warrant under Rule 41. Title III applies when the government seeks to intercept electronic, wire, or oral communications in real time, rather than stored on a computer or with a service provider.[63] Because of the invasiveness of these searches, Title III has more robust procedural safeguards than a traditional warrant, including that the government has exhausted other investigatory procedures prior to seeking a Title III application; and that the court shall limit surveillance to what is necessary for the investigation and that the government shall minimize any communications not relevant to the purpose of the search.[64] In

[56] *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 758-59 (S. D. Tex. 2013).

[57] *See* ACLU, Second Comment, *supra* note 54.

[58] *See* Greenstreet v. Cty. of San Bernardino, 41 F.3d 1306, 1309 (9th Cir. 1994).

[59] ACLU, Second Comment, *supra* note 54 (quoting Berger v. New York, 388 U.S. 41, 56 (1967)).

[60] Rules Package, *supra* note 3.

[61] CDT, Written Statement, *supra* note 9.

[62] P.L. 90-351, 82 Stat. 197.

[63] *See* 18 U.S.C. §§2510-2522.

[64] *See* 18 U.S.C. § 2518(1)-(5).

addition to oral and written communications, courts have also applied Title III's requirements to video surveillance.[65]

One commenter posited that some of the searches envisioned under the changes to Rule 41 would trigger Title III's heightened requirements.[66] For instance, if the government seeks to activate a camera or microphone on a device remotely, which the FBI claims it is capable of doing,[67] or it seeks to access electronic communications in real time, this commenter argues that it should adhere to Title III, rather than simply Rule 41. Moreover, this entity suggests that the installation of malware, spyware, or other government software that remains on a target computer and collects information could trigger similar concerns.[68] However, there is nothing in the text of the proposed amendment that would seem to require a Title III order when real time content was being accessed. That said, the Judicial Conferences Committee Note seems to envision that courts would resolve such questions on a case-by-case basis.[69]

Surreptitious Entry, Destructive Searches

At least one observer has argued that the proposed amendment cannot meet the more demanding Fourth Amendment standard required for covert-entry remote access searches, [70] which generally requires that the government has some "reasonable necessity" for conducting the surreptitious search and that notice be given a reasonable time after the search is conducted.[71]

Others have argued that the use of "malware and zero-day exploits is more invasive than other forms of permissible searches because the consequences and collateral damage associated with their use are inherently unpredictable and often irreversible."[72] Poorly designed malware could cause the destruction of data or the corruption of the whole operating system.[73] Moreover, when the government releases malware, there may be a risk that the code gets into the hands of bad actors or spreads virally across the Internet, causing damage to innocent third parties.[74] Like with the particularity arguments, discussed earlier, the Judicial Conference responded to these comments by highlighting the Committee Note, which asserts that the rule "does not foreclose or prejudge these constitutional issues," but rather "leaves them to be resolved on a case-by-case basis."[75]

[65] See 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).

[66] ACLU, Second Comment, *supra* note 54, at 18.

[67] *See* "Rule 41 and Remote Searches," *supra* p.3.

[68] ACLU, Second Comment, *supra* note 54, at 20.

[69] *See supra* note 57.

[70] Electronic Privacy Information Center, Statement on Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure (Nov. 5, 2014), *available at* https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0010.

[71] *See* United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990).

[72] *See* ACLU, Second Comment, *supra* note 54, at 18.

[73] *Id.*

[74] *Id.* at 17.

[75] *See* Agenda Book, March 16-17, 2015, *supra* note 38, at 92.

Notice

Several commenters challenged the sufficiency of the notice requirements provided under the proposed rule. One privacy advocate argued, for instance, that the notice requirements were lessened under the proposed amendment as they did not require that the officer "must" provide a copy of the warrant—as is required currently under Rule 41(f)(1)(C)—but instead would require only that the officer "make reasonable efforts to serve a copy of the warrant and receipt" and ensure service is "reasonably calculated to reach that person."[76] This advocate argued that providing notice will be difficult in many common situations, such as a target who signs onto a wireless network at a coffee shop or library.[77] In response, the Advisory Committee described the proposed notice requirements as "intended to be parallel, to the degree possible, with the requirement for physical searches."[78] Providing notice in the case of physical searches is not always possible, the Committee noted, and the rule as currently written does not require actual notice, but rather that notice be given "to the person from whom, or from whose premises, the property was taken, or leave a copy of the warrant and receipt at the place where the officer took the property."[79]

Additionally, one commenter argued that the government should have to provide notice to both the owner of a computer *and* others who may have used and stored information on that device, not one *or* the other as is currently proposed in the rule.[80] The Judicial Conference rejected this suggestion, claiming that if the government executes a warrant for a business and seizes records of individual customers, providing notice to each customer would be too burdensome on the government, and is not required under current law.[81]

Finally, several commenters argued that government officials could delay giving notice, as the proposed notice requirement only requires that the government make "reasonable efforts" to provide notice, but does not require that it be given promptly.[82] Answering these comments, the Committee noted that Rule 41(f)(3) permits delayed notice if allowed by statute. The Committee added a Committee Note stating that "Rule 41(f)(3) allows delayed notice *only* 'if the delay is authorized by statute.'"[83]

Impediments to Judicial Review

Some commenters also raised concerns that the proposed rule, combined with existing judicial doctrines, could hinder judicial review in various ways, including the following:

- *Ex parte proceedings and lack of technical sophistication in the judiciary.* Warrant proceedings are largely resolved *ex parte*—that is, only the government's attorney is present to offer arguments to the magistrate judge. Some have argued that the nature of these one-sided proceedings would hinder

[76] ACLU Second Comment, *supra* note 54, at 23-24; Final Rules Package, *supra* note 3, at 224.

[77] ACLU Second Comment, *supra* note 54.

[78] Agenda Book, March 2015, *supra* note 47, at 93.

[79] FED. R. CRIM. P. 41(f)(1)(C).

[80] ACLU, Second Comment, *supra* note 54, at 24.

[81] Agenda Book, March 16-17, 2015, *supra* note 38, at 93-94.

[82] *See* ACLU, Second Comment, *supra* note 54, at 24-25; EPIC, Written Statement, *supra* note 37.

[83] Rules Package, *supra* note 3 (emphasis added).

effective judicial review, especially when difficult technological questions are involved.[84]

- *Good Faith.* Under the good faith exception to the exclusionary rule of the Fourth Amendment, unlawfully obtained evidence can still be admissible in a criminal trial if the evidence was "obtained in objectively reasonable reliance on a subsequently invalidated search warrant."[85] Some have argued that, because courts have the authority to resolve the good faith question before the substantive Fourth Amendment question,[86] the constitutional merits could largely go unresolved.[87]
- *Qualified Immunity*. Qualified immunity operates in a similar manner in the civil context as good faith does in the criminal context: it "protects government officials from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known."[88] Again, courts are permitted to resolve this procedural question before moving to the merits of the plaintiff's claim.[89] Commenters have posited that qualified immunity, like good faith, could preclude judicial review of the constitutionality of these largely untested search and seizure techniques.[90]

Forum Shopping

Some have argued that permitting remote searches under Rule 41 in any district in which an element of the crime occurred raises significant concerns of forum shopping. That is, they argue that when the government has multiple options of jurisdictions in which to file a warrant application, it will more often than not choose the more government friendly judge.[91]

Process Concerns

In addition to comments concerning the changes to Rule 41 itself, many observers have challenged the method in which the rule is being changed. Some have argued that as sensitive a topic as remote hacking should undergo a more thorough vetting via the formal congressional lawmaking process rather than through the rulemaking process of a federal agency.[92] As argued by the one privacy advocacy group:

> The proposed changes to FRCrmP Rule 41 are not a Congressional amendment, nor do they implement a direct expansion of extraterritorial jurisdiction codified in statute. Congress has not authorized extraterritorial or multi-district searches for computers with concealed locations or during investigations under 18 U.S.C. § 1030(a)(5), as the proposed modification to Rule 41 contemplates. The proposed modification attempts to

[84] *See, e.g.*, ACLU, Second Comment, *supra* note 54, at 25-26.

[85] *See* United States v. Leon, 468 U.S. 897, 922 (1984).

[86] *See*., *e.g.*, United States v. Clay, 646 F.3d 1124, 1128 (8th Cir. 2011).

[87] *See* ACLU, Second Comment, *supra* note 54, at 26 ("[E]ven in cases where a remote access warrant fails the particularity, probable cause, or reasonableness requirements of the Fourth Amendment, courts will generally avoid ruling on the issue.").

[88] Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982).

[89] *See* Pearson v. Callahan, 555 U.S. 223, 236 (2009).

[90] *See* ACLU, Second Comment, *supra* note 54, at 26-27.

[91] CDT, Written Statement, *supra* note 9, at 5.

[92] *Id.*

> expand magistrates' Rule 41 authority in a manner that has historically been accomplished by Congressional action. The proposed modification should be handled through Congress rather than judicial rulemaking.[93]

Similar arguments have been made by technologists at one privacy advocacy group : "We have transitioned into a world where law enforcement is hacking into people's computers, and we have never had public debate. . . . Judges are having to make up these powers as they go along."[94]

Conclusion

Rule 41 of the Federal Rules of Criminal Procedure regulates the issuance of warrants to search and seize papers, effects, and other things related to federal crimes. As currently drafted, the rule neither explicitly permits nor prohibits "remote access" searches—that is, searches performed remotely to access a target's device. However, DOJ has sought and obtained Rule 41 warrants to conduct various remote access searches over the past 15 years, including accessing both metadata and content from criminals' devices. The current rule only permits judges to issue warrants within their jurisdiction, subject to several limited exceptions. This requirement cannot be satisfied when the government does not know in which jurisdiction the computer is located. With the increasing use of anonymizing technology by criminals and other targets, DOJ has claimed it has been frustrated in its attempt to seek certain warrants when it cannot locate the device.

To this end, DOJ requested that the Judicial Conference of the United States, the policy-making arm of the federal judiciary, evaluate two changes to Rule 41. The first would authorize remote access searches of computers in which the location has been hidden through technological means. The second would allow the government to use one warrant to search multiple computers when five or more computers have been the subject of certain hacking attacks. After several years of evaluation, the amendments have been approved by the Judicial Conference and are now pending before Congress. Unless Congress acts, the amendments will take effect on December 1, 2016.

Opponents of the rule change have argued, among other things, that it would undermine Fourth Amendment privacy protections, including the particularity requirement. Moreover, they argue that the rule change could have many unintended consequences that should be worked out by Congress in the first instance, and not the rulemaking body of the federal courts. Both DOJ and the Judicial Conference have asserted, on the other hand, that this rule change would only change the venue requirements of the rule, and that any constitutional questions would be addressed as they arise on a case-by-case basis.

[93] *Id.*

[94] Timberg & Nakashima, *supra* note 18.

Appendix. Text of Proposed Amendment to Rule 41

The following language is the final proposed amendment transmitted from the Supreme Court to Congress:

> Rule 41. Search and Seizure.
>
> …
>
> (b) ~~Authority to Issue a Warrant~~. Venue for a Warrant Application.
>
> At the request of a federal law enforcement officer or an attorney for the government:
>
> …
>
> (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 19 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.
>
> (f) Executing and Returning the Warrant.
>
> (1) Warrant to Search for and Seize a Person or Property.
>
> …
>
> (C) Receipt. The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property. For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.[95]

Author Contact Information

Richard M. Thompson II
Legislative Attorney
rthompson@crs.loc.gov, 7-8449

[95] Rules Package, *supra* note 3.