Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 34, ISSUE 3 / JULY 15, 2016

EXPERT ANALYSIS

Government Hacking Ok? New Rules Will Expand Government Authority To Do So

By John McCaffrey, Esq., and Adrienne Kirshner, Esq.
Tucker Ellis LLP

Currently, law enforcement hacks into cellphones and conducts remote electronic searches of computers when the government can satisfy the probable cause requirements and can identify the judicial district where the device is located — the district in which it should apply for the search warrant.

The U.S. Supreme Court recently approved amendments to Rule 41 of the Federal Rules of Criminal Procedure, which shall take effect Dec. 1, 2016, unless Congress intervenes. These amendments if approved will drastically alter the landscape for where and when law enforcement may receive a warrant to search electronic devices by permitting devices located outside of the issuing court's jurisdiction to be searched.

In other words, Congress has until Dec. 1 to reject the recommendations or the amendments become the rules governing the issuance of warrants for remote electronic searches outside a district where the electronic device to be searched is located.

CURRENT RULE 41(B)

Current Rule 41(b) of the Federal Rules of Criminal Procedure authorizes search warrants for property located outside the judicial district where the person or property is located, but only under certain specific enumerated situations. These situations involve:

- Property in the district that might be removed before execution of the warrant can occur.
- Tracking devices installed in the district, which may be monitored outside the district.
- Investigations involving domestic or international terrorism.
- Property located in a U.S. territory or a U.S. diplomatic or consular mission.[1]

AMENDMENTS TO RULE 41(B)

The amendments to Rule 41 intend to address two situations where the current venue requirements cannot be met:

- When there is a known target computer with an unknown location.
- When the investigation requires the coordinated search of numerous computers in several judicial districts.

Accordingly, amended Rule 41(b) includes two additional exceptions to the current list of out-of-district searches permitted under that subsection.

Amendments to Rule 41 of the Federal Rules of Criminal Procedure shall take effect Dec. 1, 2016, unless Congress intervenes.

Amended Rule 41(b)(6) authorizes a court to issue a warrant to use remote access to search electronic storage media and seize electronically stored information inside or outside the district when:

- The target of the investigation has used technology to conceal the location of the media to be searched.
- In an investigation involving a violation of the Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030(a)(5), when the media to be searched include protected computers that have been damaged and are located in five or more judicial districts.[2]

The amendments to Rule 41(b) change only the territorial limitation presently imposed on judges issuing warrants, not the Fourth Amendment constitutional requirements.

To meet the particularity requirement of the Fourth Amendment, a warrant for remotely searching electronically stored media or seizing or copying electronically stored information will still need to describe with particularity both the computer to be searched and the items to be seized.

The amendment involving investigations of Computer Fraud and Abuse Act violations touch a very limited class of investigations. A judge within a district where activities related to a relevant CFAA violation may have occurred can oversee the investigation and issuance of warrants for remote electronic searches if the media to be searched are protected computers that have been damaged and are located in five or more districts.

In those instances, law enforcement could conduct a search and seize electronically stored information by remotely installing software on a large number of affected "damaged" computers (computers the owners potentially do not even know are "damaged"), pursuant to one warrant issued by a single judge.

Currently, the requirements of Rule 41 make it necessary for law enforcement to obtain multiple warrants to conduct searches in each of the districts in which an affected computer may be located.

EXPANDED AUTHORITY UNDER RULE 41(B)

The Department of Justice cited three primary reasons for expanded authority for out-of-district remote electronic searches.

First, this expanded authority will enable law enforcement to obtain warrants where the location of the computer to be searched is unknown, including where a target is using anonymization software or tools like Tor to mask the target's internet protocol, or IP, address and other identifying information.

Second, it will enable law enforcement to obtain warrants to search internet-connected computers in numerous districts simultaneously when those computers are being used as part of a criminal scheme like a "botnet" attack.

A "botnet" is a collection of compromised computers that operates under the remote command and control of a criminal, the target of the investigation. Botnets may range in size from hundreds of compromised computers located within residences, businesses or government computer systems.

Botnets are most commonly used to steal personal financial data, conduct large-scale denial-of-service attacks and distribute malware designed to invade the privacy of users of the host computers.

Third, this expanded authority will help law enforcement obtain a warrant to search a computer in a particular location and to utilize the same warrant to search information that is accessible from that computer but stored remotely in another district, such as information stored on cloud-based services including Dropbox or Amazon Cloud Drive or web-based email, like Gmail or Yahoo Mail.[3]

A search of the computer could lead to the discovery of multiple web-based email addresses, social media accounts and cloud-based services potentially used to commit the crime under investigation or contain evidence of such crime.

However, to access such accounts and information requires accessing information not on the seized computer but on servers located elsewhere. Permission to search the computer does not grant permission to use the computer to search servers located elsewhere.

Accordingly, as soon as a computer is seized that target of the criminal investigation could immediately start deleting information contained on servers that were not part of the initial search.

These proposed amendments would make it possible to obtain a search warrant to search a computer and information the computer can access yet which is actually located elsewhere.

AMENDMENTS TO RULE 41(F)(1)(C)

To coincide with the amendments to Rule 41(b), Rule 41(f)(1)(C) is amended to specify the process to be used for providing notice that a remote access search occurred.

The current version of Rule 41(f)(1)(C) requires the officer executing the warrant to give a copy of it as well as a receipt for the property seized to the owner or place where the search and seizure occurred.

Obviously, the process for providing notice where there is a physical search of property versus the remote access search of property is going to involve differing efforts.

The amendments to Rule 41(f)(1)(C) will require that "reasonable efforts" to provide notice of the physical search be given "to the person from whom, or from whose premises, the property was taken" or left "at the place where the officer took the property."

The term "reasonable efforts" is not defined, and a potential area that will be the subject of needed judicial interpretation. It is also uncertain what the consequences of failing to take such "reasonable efforts" would be.

These amendments if approved will drastically alter the landscape for where and when law enforcement may receive a warrant to search electronic devices.

OBJECTIONS TO THE RULE 41 AMENDMENTS

Initially, the amendments submitted by the Rule 41 subcommittee to the Advisory Committee on Criminal Rules for the Judicial Conference were broader than those amendments suggested by the Advisory Committee, approved by the U.S. Supreme Court and forwarded to Congress.

The original subcommittee proposal sought to add language permitting judges "in any district where activities related to a crime may have occurred ... to issue a warrant to use remote access to search electronic storage media and to seize electronically stored information located within or outside that district."[4]

The wide reach of the exception triggered numerous objections from civil rights organizations, digital rights groups and businesses such as Google. These objections asserted that the overbreadth of the rule would lead to violations of the Fourth Amendment's protections against unreasonable searches and seizures.

The Advisory Committee took these objections seriously, but maintained its position that the rules should not alter any of the rights or protections afforded by the Fourth Amendment. The rule was only meant to extend the circumstances where a court could consider issuing a search warrant and would not alter the evidentiary requirements for issuing a search warrant, the committee said.

To make clear that the rule and its amendments only concerned venue, the caption of the rule will be changed from "Authority to Issue a Warrant" to "Venue for a Warrant Application," and a committee note will be added explaining:

> The revision to the caption is not substantive. Adding the word "venue" makes clear that Rule 41(b) identifies the courts that may consider an application for a warrant, not the constitutional requirement for the issuance of a warrant, which must still be met.[5]

Adding additional emphasis to the fact that the amendments to Rule 41(b) should not change constitutional jurisprudence, the proposed committee note concludes with the following language:

> The amendment does not address constitutional questions, such as 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.[6]

Despite efforts to make clear that the amendments relate to the venue of the issuing court and do not impact the Fourth Amendment considerations underlying the issuance of a warrant, the potential overuse of the out-of-district search and seizure exceptions and the potential violations of the Fourth Amendment were the primary basis for objections to the revised version of the amendments.

The American Civil Liberties Union's objections, in part, related to the concern that methods used to obtain access to computers would have unpredictable outcomes. As the ACLU explained, to gain access, malware would need to be developed constantly, because as soon as a type of malware is detected appropriate counter-measures are designed.

The government would need to create a strategy of infecting the target computer with the malware. Most methods of deploying malware are not capable of targeting only one single computer but may potentially infect multiple devices, and there can be no way of knowing if the intended target or other computers become infected.

In addition by using malware, the malware itself potentially can get into the hands of criminals that can use it for their own nefarious purposes.

Furthermore, use of certain methods to gain access would be unreasonable because they could create excessive and unnecessary destruction, including destroying non-target computers, the ACLU said.

Additionally, software used to gain access to a computer could, in addition to allowing the collection of data at one point in time, be used for real-time surveillance, including activating a computer's built-in camera, the ACLU said.

Given these possibilities the ACLU asserted that remote access may implicate Title III of the Omnibus Crime Control and Safe Streets Act. Title III regulates the interception of communications of public officials and private persons.[7] Title III prohibits the interception, use or disclosure of electronic communication and requires government officials to obtain judicial authorization through a specific process.

Similarly, New America's Open Technology Institute objected to the amendments based on a concern that they would authorize searches lacking adequate procedural safeguards. The organization argued for a need to create procedural safeguards similar to those established under Title III.[8]

The Center for Democracy & Technology also raised concerns regarding potential Fourth Amendment violations.

The CDT claimed that by authorizing the issuance of warrants for computers in concealed locations, the rule ignored the fact no such warrant could meet the particularity requirement of the Fourth Amendment because the place to be searched could never be described. Because of this, an authorized search could affect multiple innocent parties, the CDT said.

Additionally, the CDT argued the searches authorized pursuant to the proposed rule would inadvertently authorize the search of computers located abroad in violation of the processes established by the Mutual Legal Assistance Treaty and Mutual Legal Assistance Agreements, which require that extraterritorial searches take place in coordination with foreign governments. The CDT also raised a concern that the amendments would lead to forum-shopping.[9]

Access, an international digital rights non-governmental organization, and the Electronic Frontier Foundation jointly raised concerns regarding search warrants targeted at botnets. Search warrants targeted at botnets may affect a large number of computers not part of a botnet scheme, they said. Once again, a Fourth Amendment concern regarding the authorization of unreasonable searches affecting innocent persons was raised.

CONCLUSION

The proposed amendments to Rule 41 provide law enforcement the ability to obtain a warrant to remotely install software on a target computer where the location of the computer has been concealed to block the determination of the true IP address or other identifying information for the computer itself.

It is important to remember that the amendments to Rule 41(b) affect the venue of the court issuing a warrant and only in specific situations.

The proposed amendments to Rule 41 are procedural and not intended to alter the constitutional mandates concerning searches and seizures.

However, the objections to the proposed amendments sent to Congress portend the issues certain to arise in future challenges to warrants issued for the remote search of computers. With new power comes the potential for overuse. Our courts are the appropriate place for constitutional precedence to be set.

Courts and practitioners evaluating these new applications for searches using remote technology should be mindful of the objections raised in response to the proposed amendments to Rule 41.

NOTES

[1] *See* Fed. R. Crim. P. 41(b)(2)-(5).

[2] *See* Proposed Fed. R. Crim. P. 41(b)(6)(A)-(B) (April 28, 2016). Under the Computer Fraud and Abuse Act, the definition of a "protected computer" includes any computer "which is used in or affecting interstate or foreign commerce or communication." *See* 18 U.S.C.A § 1030(e)(2). The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system or information." *See* 18 U.S.C.A. § 1030(e)(8).

[3] *See* COMM. ON RULES OF PRACTICE & PROCEDURE OF THE JUDICIAL CONFERENCE OF THE U.S., REPORT OF THE ADVISORY COMMITTEE ON CRIMINAL RULES (Apr. 7-8, 2014), at 172-73, 261, http://bit.ly/29LgHtA (PDF available for download).

[4] *See id.* at 165.

[5] *See* Proposed Fed. R. Crim. P. 41 Advisory Committee's note, subdivision (b).

[6] *See id.*, subdivision (b)(6).

[7] *See* 18 U.S.C.A. § 2510. *See also* List of Confirmed Witnesses for the Public Hearing on Proposed Amendments to the Fed. R. Crim. P. for Nov. 5, 2014, http://bit.ly/29rhNNi, at Tab 1.

[8] *Id.* at Tab 2.

[9] *Id.* at Tab 3.

John McCaffrey (L) is a former FBI special agent and prosecutor. He is a partner with **Tucker Ellis LLP** in Cleveland, where his practice focuses on white-collar criminal defense and business litigation. He is a fellow of the American College of Trial Lawyers. He can be reached at john.mccaffrey@tuckerellis.com. **Adrienne Kirshner** (R) is an associate with the firm in Cleveland. Her practice focuses on white-collar criminal defense and business litigation. She can be reached at adrienne.kirshner@tuckerellis.com.