



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 18, 2016

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

This responds to your letter to the Attorney General, dated October 27, 2016, regarding proposed amendments to Rule 41 of the Federal Rules of Criminal Procedure, recently approved by the Supreme Court. We are sending identical responses to the Senators and Members who joined in your letter.

The amendments to Rule 41, which are scheduled to take effect on December 1, 2016, mark the end of a three-year deliberation process, which included extensive written comments and public testimony. After hearing the public's views, the federal judiciary's Advisory Committee on the Federal Rules of Criminal Procedure, which includes federal and state judges, law professors, attorneys in private practice, and others in the legal community, approved the amendments and rejected criticisms of the proposal. The amendments were then considered and unanimously approved by the Standing Committee on Rules and the Judicial Conference, and adopted by the United States Supreme Court.

It is important to note that the amendments do not change any of the traditional protections and procedures under the Fourth Amendment, such as the requirement that the government establish probable cause. Rather, the amendments would merely ensure that venue exists so that at least one court is available to consider whether a particular warrant application comports with the Fourth Amendment.

Further, the amendments would not authorize the government to undertake any search or seizure or use any remote search technique, whether inside or outside the United States, that is not already permitted under current law. The use of remote searches is not new, and warrants for remote searches are currently issued under Rule 41. In addition, courts already permit the search of multiple computers pursuant to a single warrant, so long as the necessary legal requirements are met with respect to each computer. Nothing in the amendments changes the existing legal requirements.

The amendments apply in two narrow circumstances. First, where a criminal suspect has hidden the location of his computer using technological means, the changes to Rule 41 would ensure that federal agents know which magistrate judge to go to in order to apply for a warrant. For example, if agents are investigating criminals who are sexually exploiting children and uploading videos of that exploitation for others to see—but concealing their locations through anonymizing technology—agents will be able to apply for a search warrant to discover where they are located.

An investigation of the Playpen website—a Tor site used by more than 100,000 pedophiles to encourage sexual abuse and exploitation of children and to trade sexually explicit images of the abuse—illustrates the importance of this change. During the investigation, authorities were able to wrest control of the site from its administrators, and then obtained approval from a federal court to use a remote search tool to undo the anonymity promised by Tor. The search would occur only if a Playpen user accessed child pornography on the site (a federal crime), in which case the tool would cause the user’s computer to transmit to investigators a limited amount of information, including the user’s true IP address, to help locate and identify the user and his computer. Based on that information, investigators could then conduct a traditional, real-world investigation, such as by running a criminal records check, interviewing neighbors, or applying for an additional warrant to search a suspect’s house for incriminating evidence. Those court-authorized remote searches in the Playpen case have led to more than 200 active prosecutions—including the prosecution of at least 48 alleged abusers—and the identification or rescue of at least 49 American children who were subject to sexual abuse. Nonetheless, despite the success of the Playpen investigation, Federal courts have ordered the suppression of evidence in some of the resulting prosecutions because of the lack of clear venue in the current version of Rule 41. In other cases, courts have declined to suppress evidence because the law was not clear, but have suggested that they would do so in future cases.

Second, where the crime involves criminals hacking computers located in five or more different judicial districts, the changes to Rule 41 would ensure that federal agents may identify one judge to review an application for a search warrant rather than be required to submit separate warrant applications in each district—up to 94—where a computer is affected. For example, agents may seek a search warrant to assist in the investigation of a ransomware scheme facilitated by a botnet that enables criminals abroad to extort thousands of Americans. Such botnets, which range in size from hundreds to millions of infected computers and may be used for a variety of criminal purposes, represent one of the fastest-growing species of computer crime and are among the key cybersecurity threats facing American citizens and businesses. Absent the amendments to Rule 41, however, the requirement to obtain up to 94 simultaneous search warrants may prevent cyber investigators from taking needed action to liberate computers infected with such malware. This change would not permit indiscriminate surveillance of thousands of victim computers—that is not permissible now and will continue to be prohibited when the amendment goes into effect. This is because other than identifying a court to consider the warrant application, the amendment makes no change to the substantive law governing when a warrant application should be granted or denied.

The amended rule limits forum shopping by restricting the venue in which a magistrate judge may issue a warrant for a remote search to “any district where activities related to a crime may have occurred.” Often, this language will leave only a single district in which investigators can seek a warrant. For example, where a victim has received death threats, extortion demands, or ransomware demands from a criminal hiding behind Internet anonymizing technologies, the victim’s district would likely be the only district in which a warrant could be issued for a remote search to identify the perpetrator.

In cases involving widespread criminal conduct, activities related to the crime may have occurred in multiple districts, and thus there may be multiple districts in which investigators may seek a warrant under the new amendment. For many years, however, existing laws have

recognized the need for warrants to be issued in a district connected to criminal activity even when the information sought may not be present in the district. The language of the new Rule 41(b)(6) amendment limiting warrant venue to “any district where activities related to a crime may have occurred” was copied verbatim from the existing warrant venue provisions in Rule 41(b)(3) and (b)(5), which authorize judges to issue out-of-district warrants in cases involving terrorism and searches of U.S. territories and overseas diplomatic premises. Thus, the new venue provision of Rule 41(b)(6) for remote searches is consistent with existing practices in these other contexts. Similarly, warrants for email and other stored electronic communications are sought tens of thousands of times a year in a wide range of investigations. Such warrants may be issued in any district by a court that “has jurisdiction over the offense being investigated.” 18 U.S.C. §§ 2703 & 2711(3).

As with law enforcement activities in the physical world, law enforcement actions to prevent or redress online crime can never be completely free of risk. Before we conduct online investigations, the Department of Justice (the Department) carefully considers both the need to prevent harm to the public caused by criminals and the potential risks of taking action. In particular, when conducting complex online operations, we typically work closely with sophisticated computer security researchers both inside and outside the government. As part of operational planning, investigators conduct pre-deployment verification and validation of computer tools. Such testing is designed to ensure that tools work as intended and do not create unintended consequences. That kind of careful consideration of any future technical measures will continue, and we welcome continued collaboration with the private sector and cybersecurity experts in the development and use of botnet mitigation techniques. The Department’s anti-botnet successes have demonstrated that the Department can disrupt and dismantle botnets while avoiding collateral damage to victims. And of course, choosing to do nothing has its own cost: leaving victims’ computers under the control of criminals who will continue to invade their privacy, extort money from them through ransomware, or steal their financial information.

Law enforcement could obtain identifying information (such as an IP address) from infected computers comprising a botnet in order to make sure owners are warned of the infection (typically, by their Internet service provider). Or law enforcement might engage in an online operation that is designed to disrupt the botnet and restore full control over computers to their legal owners. Both of these techniques, however, could involve conduct that some courts might hold constitutes a search or seizure under the Fourth Amendment. In general, we anticipate that the items to be searched or seized from victim computers pursuant to a botnet warrant will be quite limited. For example, we believe that it may be reasonable in a botnet investigation to take steps to measure the size of the botnet by having each victim computer report a unique identifier; but it would not be lawful in such circumstances to search the victims’ unrelated private files. Whether or not a warrant authorizing a remote search is proper is a question of Fourth Amendment law, which is not changed by the amendments to Rule 41. Simply put, the amendments do not authorize the government to undertake any search or seizure or use any remote search technique that is not already permitted under the Fourth Amendment. They merely ensure that searches that are appropriate under the Fourth Amendment and necessary to help free victim computers from criminal control are not, as a practical matter, blocked by outmoded venue rules.

The amendment's notice requirement mandates that when executing a warrant for a remote search, “the officer must make reasonable efforts to serve a copy of the warrant on the

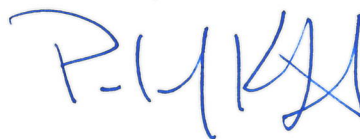
person whose property was searched or whose information was seized or copied,” and that “[s]ervice may be accomplished by any means, including electronic means, reasonably calculated to reach that person.” What means are reasonably available to notify an individual who has concealed his location and identity will of course vary from case to case. If the remote search is successful in identifying the suspect, then notice can be provided in the traditional manner (following existing rules for delaying notice where appropriate in ongoing investigations). If the search is unsuccessful, then investigators would have to consider other means that may be available, for example through a known email address. In an investigation involving botnet victims, the Department would make reasonable efforts to notify victims of any search conducted pursuant to warrant. For example, if investigators obtained victims’ IP addresses at a particular date and time in order to measure the size of the botnet, investigators could ask the victims’ Internet service providers to notify the individuals whose computers were identified as being under the control of criminal bot herders. Under such an approach, it would not even be necessary for investigators to learn the identities of specific victims. The Department will, of course, also consider other appropriate mechanisms to provide notice consistent with the amended Rule 41.

Under the Federal Rules of Evidence, the government must establish the authenticity of any item of electronic evidence it moves to admit in evidence. To do so, it must offer evidence “sufficient to support a finding that the item is” what the government claims it to be, and a criminal defendant may object to the admission of evidence on the basis that the government has not established its authenticity. The amendments to Rule 41 do not make any change to the law governing the admissibility of lawfully obtained evidence at trial, whether on the basis of authenticity or any other basis, and to our knowledge authenticity objections have not played a substantial role in prior federal criminal trials at which evidence obtained as a result of remote searches was introduced.

Protecting victims’ privacy is one of the Department’s top priorities. To the extent that investigators collect any information concerning botnet victims, the Department will take all appropriate steps to safeguard any such information from improper use or disclosure. The Department presently and vigorously protects the private information collected pursuant to search warrants for computers and documents seized from a home or business and the Department will follow the same exacting standards for any warrant executed under the amendments to Rule 41.

We hope that this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,



Peter J. Kadzik
Assistant Attorney General