of prior judicial approval might raise difficult questions of international law and the institutional roles of the courts and the executive branch.[5]

The Committee considered the possibility that in rare cases the Department of Justice might seek to make service under (c)(3)(D)(ii) in a foreign nation without its cooperation or consent. Representatives of the Department stated that such service would be made only as a last resort, and only after the Criminal Division's Office of International Affairs and representatives of the Department of State had considered the foreign policy and reciprocity implications of such an action. The Department also stressed the Executive Branch's primacy in foreign relations and its obligation to ensure that the laws are faithfully executed. Finally, the Department noted that the federal courts are not deprived of jurisdiction to try a defendant whose presence before the court was procured by illegal means. This principle was reaffirmed in United States v. Alvarez-Machain, 504 U.S. 655 (1992) (holding that abduction of defendant in Mexico in violation of extradition treaty did not deprive court of jurisdiction). Similarly, if service were made on an organizational defendant in a foreign nation without its consent, the court would not be deprived of jurisdiction. Under the Committee's proposal – which does not require prior judicial approval of the means of service – a court would never be asked to give advance approval of service contrary to the law of another state or in violation of international law.

The Committee noted that eliminating a requirement for prior judicial approval may also be preferable from the defense perspective. Prior judicial approval would place a defendant later challenging the effectiveness of the notice provided in a difficult position. In effect, the defendant would be asking the judge who approved the service to change her mind, rather than to consider a question of first impression.

Recommendation–The Advisory Committee recommends that the proposed amendment to Rule 4 be published for public comment.

2. ACTION ITEM — Rule 41 (venue for approval of warrant for certain remote electronic searches)

The proposed amendment (Tab C) provides that in two specific circumstances a magistrate judge in a district where the activities related to a crime may have occurred has authority to issue

[5] These issues would be raised most starkly by a request for judicial approval of service of criminal process in a foreign country without its consent or cooperation, and in violation of its laws. Fed. R. Civ. P. 4(f)(3) may permit such a request. Where there is no internationally agreed means of service prescribed, Fed. R. Civ. P. 4(f)(2) then authorizes service by various means, and Fed. R. Civ. P. 4(f)(3) provides for service by "any other means not prohibited by international agreement, as the court orders." Although Fed. R. Civ. P. 4(f)(2)(C) precludes service "prohibited by the foreign country's law," that restriction is absent from Fed. R. Civ. P. 4(f)(3).

a warrant to use remote access to search electronic storage media and seize or copy electronically stored information even when that media or information is or may be located outside of the district. The proposed amendment was unanimously approved by the Committee in New Orleans. Following the meeting, the reporters circulated style changes and new language for the Committee note, which were unanimously approved by an electronic vote.

The proposed amendment had its origins in a letter from Acting Assistant Attorney General Mythili Raman. The proposal was referred to a subcommittee, which held multiple telephone conference calls before approving a proposal to amend Rule 41(b)(6).

The proposal has two parts. The first change is an amendment to Rule 41(b), which generally limits warrant authority to searches within a district,[6] but permits out-of-district searches in specified circumstances.[7] The amendment would add specified remote access searches for electronic information to the list of other extraterritorial searches permitted under Rule 41(b). Language in a new subsection 41(b)(6) would authorize a court to issue a warrant to use remote access to search electronic storage media and seize electronically stored information inside *or outside* of the district in two specific circumstances.

The second part of the proposal is a change to Rule 41(f)(1)(C), regulating notice that a search has been conducted. New language would be added at the end of that provision indicating the process for providing notice of a remote access search.

A. Reasons for the proposal

Rule 41's territorial venue provisions – which generally limit searches to locations within a district – create special difficulties for the Government when it is investigating crimes involving electronic information. The proposal speaks to two increasingly common situations affected by the territorial restriction, each involving remote access searches, in which the government seeks to obtain access to electronic information or an electronic storage device by sending surveillance software over the Internet.

In the first situation, the warrant sufficiently describes the computer to be searched, but the district within which the computer is located is unknown. This situation is occurring with increasing frequency because persons who commit crimes using the Internet are using sophisticated

[6] Rule 41(b)(1) ("a magistrate judge with authority in the district – or if none is reasonably available, a judge of a state court of record in the district – has authority to issue a warrant to search for and seize a person or property located within the district").

[7] Currently, Rule 41(b) (2) – (5) authorize out-of-district or extra-territorial warrants for: (1) property in the district when the warrant is issued that might be moved outside 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 in a United States territory or a United States diplomatic or consular mission.

anonymizing technologies. For example, persons sending fraudulent communications to victims and child abusers sharing child pornography may use proxy services designed to hide their true IP addresses. Proxy services function as intermediaries for Internet communications: when one communicates through an anonymizing proxy service, the communication passes through the proxy, and the recipient of the communication receives the proxy's IP address, not the originator's true IP address. Accordingly, agents are unable to identify the physical location and judicial district of the originating computer.

A warrant for a remote access search when a computer's location is not known would enable investigators to send an email, remotely install software on the device receiving the email, and determine the true IP address or identifying information for that device. The Department of Justice provided the committee with several examples of affidavits seeking a warrant to conduct such a search. Although some judges have reportedly approved such searches, one judge recently 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, and he suggested that the Committee should consider updating the territorial limitation to accommodate advancements in technology. *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (noting that "there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology").

The second situation involves the use of multiple computers in many districts simultaneously as part of complex criminal schemes. An increasingly common form of online crime involves the surreptitious infection of multiple computers with malicious software that makes them part of a botnet, which is a collection of compromised computers that operate under the remote command and control of an individual or group. Botnets may range in size from hundreds to millions of compromised computers, including computers in homes, businesses, and government systems. Botnets are used to steal personal and financial data, conduct large-scale denial of service attacks, and distribute malware designed to invade the privacy of users of the host computers.

Effective investigation of these crimes often requires law enforcement to act in many judicial districts simultaneously. Under the current Rule 41, however, except in cases of domestic or international terrorism, investigators may need to coordinate with agents, prosecutors, and magistrate judges in every judicial district in which the computers are known to be located to obtain warrants authorizing the remote access of those computers. Coordinating simultaneous warrant applications in many districts–or perhaps all 94 districts–requires a tremendous commitment of resources by investigators, and it also imposes substantial demands on many magistrate judges. Moreover, because these cases concern a common scheme to infect the victim computers with malware, the warrant applications in each district will be virtually identical.

B. The proposed amendment

The Committee's proposed amendment is narrowly tailored to address these two increasingly common situations in which the territorial or venue requirements now imposed by Rule 41(b) may hamper the investigation of serious federal crimes. The Committee considered, but declined to adopt, broader language relaxing these territorial restrictions. It is important to note that the proposed amendment changes only the territorial limitation that is presently imposed by Rule 41(b). Using language drawn from Rule 41(b)(3) and (5), the proposed amendment states that a magistrate judge "with authority in any district where activities related to a crime may have occurred" (normally the district most concerned with the investigation) may issue a warrant that meets the criteria in new paragraph (b)(6). The proposed amendment does not address constitutional questions that may be raised by warrants for remote electronic searches, 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. The amendment leaves the application of this and other constitutional standards to ongoing case law development.

The Committee agreed that 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, describing the computer to be searched with particularity and demonstrating probable cause to believe that evidence to be sought via the remote search will aid in apprehension or conviction of a particular offense. It is appropriate in such cases to make a narrow exception to the general territorial limitations governing the issuance of search warrants. The proposed amendment addresses this problem by relaxing the venue requirements when "the district where the media or information is located has been concealed through technological means." Because the target of the search has deliberately disguised the location of the media or information to be searched, the amendment allows a magistrate judge in a district in which activities related to a crime may have occurred "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.*" (Emphasis added).

In a very limited class of investigations the Committee's proposed amendment would also eliminate the burden of attempting to secure multiple warrants in numerous districts. The proposed amendment is limited to investigations of violations of 18 U.S.C. § 1030(a)(5),[8] where the media to be searched are "protected computers" that have been "damaged without authorization." The

[8] 18 U.S.C. § 1030(5) provides that criminal penalties shall be imposed on whoever:

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

definition of a protected computer includes any computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2). The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). In cases involving an investigation of this nature, the amendment allows a single magistrate judge with authority in any district where activities related to a violation of 18 U.S.C. § 1030(a)(5) may have occurred to oversee the investigation and issue a warrant for a remote electronic search if the media to be searched are protected computers located in five or more districts. The proposed amendment would enable investigators to conduct a search and seize electronically stored information by remotely installing software on a large number of affected victim computers pursuant to one warrant issued by a single judge. The current rule, in contrast, requires obtaining multiple warrants to do so, in each of the many districts in which an affected computer may be located.

Finally, the proposed amendment includes a change to Rule 41(f)(1)(C), which requires notice that a search has been conducted. New language would be added at the end of that provision indicating the process for providing notice of a remote access search. The rule now requires that notice of a physical search be provided "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 Committee recognized that when a electronic search is conducted remotely, it is not feasible to provide notice in precisely the same manner as when tangible property has been removed from physical premises. The proposal requires that when the search is by remote access, reasonable efforts be made to provide notice to the person whose information was seized or whose property was searched.

Recommendation–The Advisory Committee recommends that the proposed amendment to Rule 41 be published for public comment.

3. ACTION ITEM — Rule 45 (additional time after certain kinds of service)

The proposed amendment (Tab D) is part of the work of the Standing Committee's CM/ECF Subcommittee, and it parallels amendments to the civil, criminal, bankruptcy and appellate rules. The proposed amendment of Rule 45 would abrogate the rule providing for an additional three days whenever service is made by electronic means. It reflects the CM/ECF Subcommittee's conclusion that advances in the reliability of technology have undermined the principal justifications for the current rule. Civil Rule 5 was amended in 2001 to allow service by electronic means with the consent of the person served, and a parallel amendment to Rule 45(c) was adopted in 2002. Although electronic transmission seemed virtually instantaneous even then, concerns about the reliability of electronic service were cited as justifications for allowing three additional days to act after electronic service. At that time, there were concerns that (1) the electronic transmission might be delayed, (2) incompatible systems might make it difficult or impossible to open attachments, or (3) parties might withhold their consent to receiving electronic service unless they had three