COMMITTEE ON RULES OF PRACTICE AND PROCEDURE
OF THE
JUDICIAL CONFERENCE OF THE UNITED STATES
WASHINGTON, D.C. 20544

TO: Honorable Jeffrey S. Sutton, Chair
Standing Committee on Rules of Practice and Procedure

FROM: Honorable Reena Raggi, Chair
Advisory Committee on Criminal Rules

DATE: May 6, 2015

RE: Report of the Advisory Committee on Criminal Rules

I. INTRODUCTION

The Advisory Committee on the Federal Rules of Criminal Procedure ("the Advisory Committee") met on March 16-17, 2015, in Orlando, Florida, and took action on a number of proposals. The Draft Minutes are attached. (Tab B).

This report presents three action items for Standing Committee consideration. The Advisory Committee recommends that:

(1) a proposed amendment to Rule 4 (service of summons on organizational defendants), previously published for public comment, be approved as published and transmitted to the Judicial Conference; and

(2) a proposed amendment to Rule 41 (venue for approval of warrant for certain remote electronic searches), previously published for public comment, be approved as amended and transmitted to the Judicial Conference; and

(3) a proposed amendment to Rule 45 (additional time after certain kinds of service), previously published for public comment, be approved as amended and transmitted to the Judicial Conference.

In addition, the Advisory Committee has two information items to bring to the attention of the Standing Committee.

II. ACTION ITEMS

A. ACTION ITEM—Rule 4 (service of summons on organizational defendants)

After review of the public comments, the Advisory Committee voted unanimously to recommend that the Standing Committee approve the proposed amendment as published and transmit it to the Judicial Conference. The amendment is at Tab C.

1. Reasons for the proposal

The proposed amendment originated in an October 2012 letter from Assistant Attorney General Lanny Breuer, who advised the Committee that Rule 4 now poses an obstacle to the prosecution of foreign corporations that have committed offenses that may be punished in the United States. In some cases, such corporations cannot be served because they have no last known address or principal place of business in the United States. General Breuer emphasized the "new reality": a truly global economy reliant on electronic communications, in which organizations without an office or agent in the United States can readily conduct both real and virtual activities here. He argued that this new reality has created a "growing class of organizations, particularly foreign corporations" that have gained "'an undue advantage' over the government relating to the initiation of criminal proceedings."

At present, the Federal Rules of Criminal Procedure provide for service of an arrest warrant or summons only within a judicial district of the United States. Fed. R. Crim. P. 4(c)(2), which governs the location of service, states that an arrest warrant or summons may be served "within the jurisdiction of the United States."[1] In contrast, Fed. R. Civ. P. 4(f) authorizes service on individual defendants in a foreign country, and Fed. R. Civ. P. 4(h)(2) allows service on organizational defendants as provided by Rule 4(f).

2. The proposed amendment

Given the increasing number of criminal prosecutions involving foreign entities, the Advisory Committee agreed that it would be appropriate for the Federal Rules of Criminal Procedure to provide a mechanism for foreign service on an organization. The Advisory Committee recognized that the government may not be able to prosecute foreign entities that fail to respond to service. Nevertheless, it is expected that entities subject to collateral consequences

[1] Fed. R. Crim. P. 4(c)(2) does provide, however, that service may also be made "anywhere else a federal statute authorizes an arrest."

(forfeiture, debarment, etc.) will appear. The proposed amendment makes the following changes in Rule 4:

(1) It specifies that the court may take any action authorized by law if an organizational defendant fails to appear in response to a summons. This fills a gap in the current rule, without any expansion of judicial authority.

(2) For service of a summons on an organization within the United States, it:

- eliminates the requirement of a separate mailing to an organizational defendant when delivery has been made to an officer or to a managing or general agent, but

- requires mailing when delivery has been made on an agent authorized by statute, if the statute itself requires mailing to the organization.

(3) It also authorizes service on an organization at a place not within a judicial district of the United States, prescribing a non-exclusive list of methods for service.

In addition to the enumerated means of service, the proposal contains an open-ended provision in (c)(3)(D)(ii) that allows service "by any other means that gives notice." This provision provides flexibility for cases in which the Department of Justice concludes that service cannot be made (or made without undue difficulty) by the enumerated means. One of the principal issues considered by the Advisory Committee was whether to require prior judicial approval of other means of service. Civil Rule 4(f)(3) provides for foreign service on an organization "by other means not prohibited by international agreement, as the court orders."(emphasis added). The Committee concluded the Criminal Rules should not require prior judicial approval before service of a criminal summons could be made in a foreign country by other unspecified means. In its view, a requirement of prior judicial approval might raise difficult questions of international law and the institutional roles of the courts and the executive branch.[2]

[2] 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, or even in violation of international agreement. 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). The proposed amendment to Criminal Rule 4 authorizes service "permitted by an applicable international agreement," but does not prohibit service that is not so permitted, as long as service "gives notice."

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, or in violation of international agreement, 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. Rather, a court would consider any legal challenges to such service only when raised in a proceeding before it.

3. Public Comments and Subcommittee Review

a. Public comments

Six written comments on the proposed amendment were received, and one speaker (from the Federal Bar Council for the Second Circuit) testified about the proposed amendment. The Federal Bar Council, the Federal Magistrate Judges Association (FMJA), Mr. Kyle Druding, and the National Association of Criminal Defense Lawyers (NACDL) all supported the proposed amendment, though the FMJA and NACDL suggested revisions. Robert Feldman, Esq. of Quinn Emanuel Urquart & Sullivan opposed the amendment and urged that it be withdrawn. Additionally, the Department of Justice provided written responses. Each comment is summarized at Tab C.

With the exception of Quinn Emanuel, the commenters generally agreed that the amendment (1) addresses a gap in the current rules that may hinder the prosecution of foreign corporations that commit crimes in the United States but have no physical presence here, (2) provides methods of service that are reasonably calculated to provide notice and comply with applicable laws, and (3) gives courts appropriate discretion to fashion remedies.

b. The Subcommittee's review and recommendations

The Rule 4 Subcommittee, chaired by Judge David Lawson, received both summaries and the full text of the comments, and it held a teleconference to review the comments. The

Subcommittee unanimously recommended that the Advisory Committee approve the proposed amendment as published and transmit it to the Standing Committee.

4. Recommended action

After a full discussion, the Advisory Committee concurred in the recommendation that the proposed amendment as published should be approved for transmission to the Standing Committee.

a. Opposition to the proposed amendment

Only one comment opposed the amendment and recommended that it be withdrawn. The law firm of Quinn Emanuel Urquart & Sullivan represents the Pangang Group Company and affiliated entities, a state-owned Chinese corporation. The Department of Justice has been unable to serve process on Pangang under current Rule 4.[3] The proposal to amend the rule would provide a mechanism for effecting service on foreign corporations that commit serious crimes in the United States without having any physical presence here. The amendment is intended to allow reliable service with adequate notice on these organizations so that U.S. courts can adjudicate the merits of criminal allegations and ensure appropriate accountability.

The Committee carefully considered Quinn Emanuel's arguments, and found them unpersuasive. Quinn Emanuel argued that the proposed amendment would essentially foreclose judicial review of the adequacy of notice to foreign corporations, because "the very act of challenging service might be said to conclusively establish the notice that would make service complete." Corporate defendants who wish to contest service, they argued, would face "a Hobson's choice." The Committee agreed that if a lawyer for a corporation appears in a criminal case it may be difficult to convince the court that the corporation did not receive notice. But this

[3] On July 10, 2014, after a two month jury trial, Walter Liew, the owner and president of a California-based engineering consulting company, was sentenced to 15 years in prison for conspiring to steal trade secrets from E.I. du Pont de Nemours & Company ("DuPont") related to the manufacture of titanium dioxide and for the benefit of Pangang. *See, Walter Liew Sentenced to Fifteen Years in Prison for Economic Espionage,* justice.gov (Jul. 11, 2014), www.justice.(_2,ov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espiona2,e. Liew was aware that DuPont had developed industry-leading titanium dioxide technology over many years of research and development and assembled a team of former DuPont employees to assist him in his efforts to convey DuPont's titanium dioxide technology to entities in the People's Republic of China, including Pangang. At Liew's sentencing; the Honorable Jeffrey S. White, U.S. District Court Judge, stated that the 15-year sentence was intended, in part, to send a message that the theft and sale of trade secrets for the benefit of a foreign government is a serious crime that threatens our national economic security. *Id.* Despite the fact that Pangang was indicted years ago along with Liew, and has actual notice of the indictment, to date, the United States has been unable to effectively serve Pangang pursuant to the current Rule 4. *See, e.g., United States v. Pangang Group Co., Ltd,* 879 F. Supp. 2d 1052 (N.D. Cal. 2012).

is appropriate. A court should be able to take into account the appearance of counsel when evaluating a corporation's claim that it did not receive notice. Moreover, nothing in the proposed amendment addresses or limits any authority of the court to allow a special appearance to contest service on other grounds, nor does it address the ability of a corporate defendant to contest notice in a collateral proceeding. Quoting *Omni Capital Int'l v. Wolff & Co.*, 484 U.S. 97, 104 (1987), Quinn Emanuel also argued that in suggesting notice was the sole criterion for service, the Rule would "eliminate a historical function of service." The Committee concluded that the *Omni Capital* decision is fully consistent with the proposed amendment. In the sentence following the language quoted by Quinn Emanuel the Court made it clear that service in compliance with the Civil Rules provided the additional element of "amenability to service." The Court explained, "Absent consent, this means there must be authorization for service of summons on the defendant." Here, the purpose of the proposed amendment is to provide the necessary "authorization for service" (as well as notice to the defendant).

The lawyers from Quinn Emanuel raised another argument that the Committee had considered as it was formulating the proposal, namely, that "other governments may reciprocate by adopting a similar regime" to "ensnare U.S. corporations in criminal prosecutions around the globe." In a related objection, Quinn Emanuel noted that a court might interpret the amendment to permit "a manner of service prohibited by international agreement . . . , so long as it appears to have provided notice to the accused," an interpretation it found objectionable. Both of these concerns were anticipated by the Committee well before the proposal was approved for publication. In response to a specific request from a Committee member, the Department of Justice provided written assurance that it had consulted with appropriate authorities in the Executive Branch about the potential international relations ramifications of the proposed amendment. The Committee agreed that in light of this assurance, concerns about any impact on diplomatic relations were not a basis for rejecting the proposed amendment.

b. Suggested revisions

The FMJA, Quinn Emanuel, and NACDL suggested revisions that the Advisory Committee declined to adopt. The FMJA suggested that an addition to the Committee Note stating that the means of service must satisfy constitutional due process. Quinn Emanuel's attorneys also argued if a corporate defendant did not receive notice and failed to appear, the court might impose sanctions, or appoint counsel and conduct trial in absentia. Similarly, NACDL requested that the amendment be revised to include in the rule's text that actions by a judge upon a corporation's failure to appear must be "consistent with Rule 43(a)," or, in the alternative that this requirement be stated in the Note. The Advisory Committee considered and rejected these suggestions. It is always assumed that a rule will be interpreted against the backdrop of existing rules, statutes, and constitutional doctrine. Absent some compelling reason to believe this point will be misunderstood, adding such a command to a rule's text or Note is unnecessary. Indeed, doing so might have the undesirable effect of suggesting that in the absence of such a cross reference, other statutes and rules are not applicable.

The Advisory Committee also rejected proposed revisions that would add procedural hurdles and might invite extended litigation. NACDL suggested that the proposed amendment be modified to allow service by alternative means only if it was not possible to deliver a copy in a manner authorized by the foreign jurisdiction's law, to a officer, manager or other general agent, or an agent appointed to receive process. The Advisory Committee chose neither to add such a condition nor to prioritize the means of service, as that would invite unnecessary litigation over whether the triggering condition had been met. Similarly, the Committee rejected the further suggestion of NACDL that the new provisions be limited to cases in which "the organization does not have a place of business or mailing address within the United States at or through which actual notice to a principal of the organization can likely be given." As noted by the Department of Justice, litigation in a recent case on the question whether a subsidiary of a foreign corporation could be served took eight months. Finally, the Committee rejected Quinn Emanuel's argument that "any other means that gives notice" renders superfluous the other sections of the proposed amendment. Similarly, the Committee considered and rejected a suggestion that the government be required to show other options were not feasible or had been exhausted before resorting to certain options for service as unnecessarily burdensome and time consuming.

Recommendation–The Advisory Committee recommends that the proposed amendment to Rule 4 be approved as published and transmitted to the Judicial Conference.

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

After review of the public comments, the Advisory Committee voted with one dissent to recommend that Standing Committee approve the proposed amendment as revised after publication and transmit it to the Judicial Conference.

The proposed amendment (Tab D) 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 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 proposal has two parts. The first change is an amendment to Rule 41(b), which generally limits warrant authority to searches within a district,[4] but permits out-of-district

[4] 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").

searches in specified circumstances.[5] 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.

1. Reasons for the proposed amendment

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 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

[5] 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.

search when the location of the computer was not known, and he suggested that the Committee 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.

2. 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.

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),[6] where the media to be searched are "protected computers" that have been "damaged without authorization." The 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 an 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.

[6] 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.

3. Public Comments and Subcommittee Review

a. The public comments

During the public comment period the Committee received 44 written comments from individuals and organizations, and eight witnesses testified at the Committee's hearing in November:

> The Federal Bar Council, the Federal Magistrate Judges' Association, the National Association of Assistant United States Attorneys, and former advocate for missing and exploited children Carolyn Atwell-Davis all supported the amendment without change.
>
> The amendment was opposed by the American Civil Liberties Union (ACLU), the National Association of Criminal Defense Attorneys (NACDL), the Pennsylvania Bar Association, the Reporters Committee on the Freedom of the Press, the Clandestine Reporters Working Group, and several foundations and centers that focus on privacy and/or technology. Twenty-eight unaffiliated individuals wrote to oppose the amendment.

The Department of Justice submitted several written responses to issues raised in the public comments.

A summary of the comments is provided at Tab D. The main themes in the comments opposing the amendment are summarized below.

(i) Fourth Amendment concerns

The most common theme in the comments opposing the amendment was a concern that it relaxed or undercut the protections for personal privacy guaranteed by the Fourth Amendment. These comments focused principally on proposed (b)(6)(A), which allows the court in a district in which activities related to a crime may have occurred to grant a warrant for remote access when anonymizing technology has been employed to conceal the location of the target device or information.

Multiple comments argued that remote searches could not meet the Fourth Amendment's particularity requirement, and others emphasized that they would constitute surreptitious entries and invasive or destructive searches requiring a heightened showing of reasonableness. Many of these comments also challenged the constitutional adequacy of the notice provisions. Finally, several comments urged that the serious constitutional issues raised by remote searches would be insulated from judicial review.

A particular concern raised in many comments was that the use of anonymizing technology, such as Virtual Private Networks (VPNs), would subject law abiding citizens to remote electronic searches.

(ii) Title III

Multiple comments urged that warrant applications for remote electronic searches should be subject to requirements like those under the Wiretap Act, 18 U.S.C. § 2518 (Title III), or a surveillance warrant containing equivalent protections.

(iii) Extraterritoriality and international law concerns

Some comments focused on the possibility that the devices to be searched–whose location was by definition unknown–might be located outside the United States. They urged that the courts should not authorize searches outside the United States that would violate international law and the sovereignty of other nations, as well as any applicable mutual legal assistance treaties.

(iv) The role of Congress

An additional theme running through many of these comments was that the proposed amendment raised policy issues that should be resolved by Congress, not through procedural rulemaking. Some comments argued that only Congress could balance the competing policies and adopt appropriate safeguards. Others urged that the proposed amendment exceeded the authority granted by the Rules Enabling Act.

(v) Notice concerns

Finally, multiple comments expressed concern that the notice provisions were insufficiently protective, because they required only that reasonable efforts be made to provide notice. This, commenters argued, might lead to no notice being given to parties who were subject to remote electronic searches, or to long delays in giving notice. Some commenters also argued that all parties whose rights were affected by a search must be given notice, not either the person whose property was searched or whose information was seized or copied.

b. The Subcommittee's review and recommendation

The Rule 41 Subcommittee, chaired by Judge Raymond Kethledge, received both summaries and the full text of all comments, and it held multiple teleconferences to review the comments. The Subcommittee unanimously recommended that, with several minor revisions, the Advisory Committee should approve the proposed amendment and transmit it to the Judicial Conference.

4. Recommended action

After extended discussion, the Advisory Committee concurred in the recommendation that the proposed amendment, with minor revisions proposed by the Subcommittee, should be approved for transmission to the Standing Committee.

a. Opposition to the proposed amendment

In general the Committee concluded that the concerns of those opposing the amendment were about the substantive limits on government searches, which are not affected by the proposed amendment. Opposition comments did not address the procedure for designating the district in which a court will initially decide whether substantive requirements have been satisfied in the two circumstances prompting the amendment. Thus they furnished no basis for withdrawing the proposed amendment. The Committee is confident that judges will address Fourth Amendment requirements on a case-by-case basis both in issuing warrants under these amendments and in reviewing them when challenges are made thereafter.

Much of the opposition to the amendment reflected a misunderstanding of current law, the scope of the amendment, and the serious problems that it addresses. First, many commenters who opposed the rule did not recognize that the government must demonstrate probable cause to obtain a warrant. As noted below, the Committee recommends a revision to the caption of the relevant section referring to "venue" in order to draw attention to the limited scope of the amendment. Second, many commenters incorrectly assumed that the amendment created the authority for remote electronic searches. To the contrary, remote electronic searches are currently taking place when the government can identify the district in which an application should be made and satisfy the probable cause requirements for a warrant. Third, the opposing comments do not take account of the real need for amendment to allow the government to respond effectively to the threats posed by technology. Technology now provides the means for identity theft, corporate espionage, terrorism, child pornography, and other serious offenses to jeopardize the economy, national security, and individual privacy. The government can itself use technology to identify the perpetrators of such crimes but needs a rule clarifying the venue where it should make the Fourth Amendment showing necessary for a warrant. At the hearings, those who opposed the amendment were candid in admitting that they could offer no alternative to the proposed amendment (other than the hope that Congress might study the general issues and respond).

The Committee concluded that it was important to provide venue, thus allowing the case law on potential constitutional issues to develop in an orderly process as courts review warrant applications. This is far preferable than after-the-fact rulings on the legality of warrantless searches for which the government claims exigent circumstances. If the New York Stock Exchange were to be hacked tomorrow using anonymizing software, under current Rule 41 there

is no district in which the government could seek a warrant. It would be preferable, the Committee concluded, to allow the government to seek a warrant from the court where the investigation is taking place, rather than conducting a warrantless search. Judicial review of warrant applications better ensures Fourth Amendment rights and enhances privacy. Any concern that judges may be uninformed about the technology to be used in the searches could be addressed by judicial education. The Federal Judicial Center has recently prepared some information materials about topics such as cloud computing, and additional materials could be developed to help judges review applications for remote electronic searches.

In botnet investigations, the amendment provides venue in one district for the warrant applications, eliminating the burden of attempting to secure multiple warrants in numerous districts and allowing a single judge to oversee the investigation. In prior botnet investigations, the burden of seeking warrants in multiple districts played a role in the government's strategy, providing a strong incentive to rely on civil processes. Again, the amendment addresses only a procedural issue, not the underlying substantive law regulating these searches. Allowing venue in a single district in no way alters the constitutional requirements that must be met before search warrants can be issued.

The Committee declined to make any major changes in the provisions governing notice. However, as noted below, it adopted several small changes recommended by the Subcommittee and also revised the Committee Note to address concerns made in the public comments.

Finally, the Committee concluded that arguments urging that the matter be left to Congress are not persuasive. Venue is not substance. Venue is process, and Rules Enabling Act tells the judiciary to promulgate rules of practice and procedure, not to wait for Congress to act. Instead, Congress responds to proposed rules. The Department came to the Committee with two procedural problems, created by the language of the existing Rule, not by the Constitution or other statute, that are impairing its ability to investigate ongoing, serious computer crimes. The Advisory Committee's role under the Rules Enabling Act is to propose amendments that address these problems and provide a forum for the government to determine the lawfulness of these searches.

One member dissented from the Committee's conclusions on these points and voted against forwarding the amendment to the Standing Committee. The dissenting member thought that the amendment is substantive, not procedural, because it has such important substantive effects, allowing judges to make ex parte determinations about core privacy concerns. The amendment, this member argued, would not permit adversarial testing of the underlying substantive law because defense counsel would not participate until too late in the process, in back-end litigation. For many people, computers are their lives, and the member concluded that these privacy concerns should be considered in the first instance by Congress. The remainder of the Committee was not persuaded; computers are no more sacrosanct than homes, and search warrants for homes have long been issued ex parte and reviewed in back-end litigation.

b. Proposed revisions

The Committee unanimously accepted the Subcommittee's recommendations for several revisions in the rule as published, none of which require republication.

(i) The caption

The Committee accepted the Subcommittee's recommendation for a change in the caption of the affected subdivision of Rule 41, substituting "Venue for a Warrant Application" for the current caption "Authority to Issue a Warrant." This change responds to the many comments that assumed the amendment would allow a remote search in any case falling within the proposed amendment (for example, any case in which an individual had used anonymizing technology such as a VPN). The current caption seems to state an unqualified "authority" to issue warrants meeting the criteria of any of the subsections. Many commenters mistakenly interpreted the rule in this fashion, and strongly opposed it on this ground. The Committee considered and declined to adopt alternative language suggested by our style consultant, Professor Kimble, because it would less clearly indicate the limited purpose and effect of the amendment.

The Committee also adopted the Subcommittee's proposed addition to the Committee Note explaining the change in the caption. The new Note explicitly addresses the common misunderstanding in the public comments, stating what the amendment does (and does not) do: "the word 'venue' makes clear that Rule 41(b) identifies the courts that may consider an application for a warrant, not the constitutional requirements for the issuance of a warrant, which must still be met."

(ii) Notice

The Committee adopted the Subcommittee's two proposed revisions to the notice provisions for remote electronic searches and the accompanying Committee Note. The purpose of both revisions to the text is to parallel, as closely as possible, the requirements for physical searches. The addition to the Committee Note explains the changes to the text, and also responds to a common misunderstanding that underpinned multiple comments criticizing the proposed notice provisions.

The Committee added a requirement that the government provide a "receipt" for any property taken or copied (as well as a copy of the warrant authorizing the search). This parallels the current requirement that a receipt be provided for any property taken in a physical search. The Committee agreed that the omission of this requirement in the published rule was an oversight that should be remedied.

The Committee also rephrased the obligation to provide notice to "the person whose property was searched or who possessed the information that was seized or copied." Again, the purpose was to parallel the requirement for physical searches.

On the other hand, the Committee rejected the suggestion in some public comments that the government should be required to provide notice to both "the person whose property was searched" and whoever "possessed the information that was seized or copied, since that is not required in the case of physical searches. For example, if the Chicago Board of Trade is served with a warrant and files containing information regarding many customers are seized, the government may give notice of the search only to the Board of Trade, and not to each of the customers whose information may be included in one or more files. The same should be true in the case of remote electronic searches.

Finally, the Committee endorsed the Subcommittee's proposed addition to the Committee Note explaining the changes made in the notice provisions after publication, and also responding to the many comments that criticized the proposed notice provisions as insufficiently protective. The addition to the Note draws attention to the other provisions of Rule 41 that preclude delayed notice except when authorized by statute and provides a citation to the relevant statute. Professor Coquillette commented that because of the widespread confusion on this point in the public comments, the proposed addition was an appropriate exception to the general rule that committee notes should not be used to help practitioner.

Recommendation–The Advisory Committee recommends that the proposed amendment to Rule 41 be approved as amended and transmitted to the Judicial Conference.

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

After review of the public comments, the Advisory Committee voted unanimously to recommend that the Standing Committee approve the proposed amendment to Rule 45(c), with three revisions from the published version and transmit it to the Judicial Conference. The proposed amendment is at Tab E.

1. Reasons for the proposal

The proposed amendment to Rule 45(c) is a product of the Standing Committee's CM/ECF Subcommittee; parallel amendments to the civil, criminal, bankruptcy and appellate rules were published for comment. The proposed amendment 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 the reasons for allowing extra time to respond in this situation no longer exist. Concerns about delayed transmission, inaccessible attachments, and consent to service have been alleviated by advances in technology and extensive experience with electronic transmission. In addition, eliminating the extra three days would also simplify time

computation. The proposed amendment, as well as the parallel amendments to the other Rules, includes new parenthetical descriptions of the forms of service for which three days will still be added.

2. Public Comments

The public comments are summarized at Tab E.

The Pennsylvania Bar Association and the National Association of Criminal Defense Lawyers (NACDL) opposed the amendment. Each noted that the three added days are particularly valuable when a filing is electronically served at inconvenient times. NACDL emphasized that many criminal defense counsel are solo practitioners or in very small firms, where they have little clerical help, and often do not see their ECF notices the day they are received. The Department of Justice expressed a similar concern about situations in which service after business hours, from a location in a different time zone, or during a weekend or holiday may significantly reduce the time available to prepare a response. The Department did not oppose the amendment, however, and instead suggested language be added to the Committee Note to address this issue.

NACDL also questioned the addition of the phrase "Time for Motion Papers" to the caption to Rule 45(c), suggesting that it may lead to confusion.

Ms. Cheryl Siler suggested that as part of the revision the existing language of Rule 45(c) should be amended to parallel Fed. R. Civ. P. 6(d), FRAP 26(c) and Fed. R. Bank. P. 9006(f). In contrast to Rule 45(c), which requires action "within a specified time *after service*," the parallel Civil and Bankruptcy Rules require action "within a specified [or prescribed] time *after being served*." Siler expressed concern that practitioners may interpret the current rule to mean the party serving a document (as well as the party being served) is entitled to 3 extra days.

The Federal Magistrate Judges Association (FMJA) expressed concern that readers of the amended rule might think that three days are still added after electronic service because of the cross reference to Civil Rule 5(b)(2)(F) "(other means consented to)." It suggested either eliminating all of the parentheticals in the proposed rule or revising the rule to refer to "(F) (other means consented to except electronic service)."

The Advisory Committee's CM/ECF Subcommittee, chaired by Judge David Lawson, held a telephone conference to consider the comments. After discussing the FMJA's concerns it decided not to recommend a change in the published rule. The likelihood of confusion did not seem significant, and any confusion that might arise would be short lived because of the efforts underway to eliminate the requirement for consent to electronic service. The parentheticals will be helpful to practitioners, and any revision to the parenthetical reference would require further amendment in the near future. Language in the proposed Committee Note directly addresses this

issue. The Subcommittee recommended to the Criminal Advisory Committee that no change be made in the published rule on this issue, and the Advisory Committee agreed with that recommendation at its March meeting.

The Advisory Committee did approve three other revisions to the proposal, each recommended by its Subcommittee.

3. Suggested Revisions

a. Addition to Committee Note.

The first change is a proposed addition to the Committee Note that addresses the potential need to grant an extension to the time allowed for responding after electronic service. At the Advisory Committee's March meeting, two members initially opposed forwarding the published amendment to the Standing Committee, finding that the concerns voiced by the Pennsylvania Bar Association, NACDL, and the Department of Justice counseled against an amendment that would eliminate the three added days after electronic service. These members noted that the three added days are important for criminal practitioners because it is often necessary to speak directly with clients before filing responses, but speaking with incarcerated clients takes more time, particularly when clients are incarcerated in distant locations. However, the Committee eventually achieved unanimity on a compromise approach: adding language to the Committee Note. The Committee approved an addition to the Note drafted by the Department of Justice and recommended by the Advisory Committee's CM/ECF Subcommittee. The Committee decided that adding language to the Committee Note that mentioned the potential need for extensions was important not only for the reasons voiced by defense attorneys and the Department of Justice, but also because district court discretion to adjust deadlines in criminal cases is essential in order to address matters on the merits when appropriate. Such flexibility is particularly important when a person's liberty is at stake. Granting extensions in some circumstances may also be more efficient because of collateral challenges that frequently follow missed deadlines. This principal was among those that guided the Committee's recent work on Rule 12. The amendments to Rule 12 emphasized the district court's discretion to extend or modify motion deadlines so that issues can be most efficiently resolved on their merits before trial, avoiding litigation under Section 2255.

To facilitate uniformity in the Committee Note that would accompany the parallel rules making their way through the various Advisory Committees, the Criminal Advisory Committee approved the revised Note language with the understanding that modifications may be required. Indeed, subsequent to the March meeting, a much shorter version of the addition was approved by the Criminal Advisory Committee's Subcommittee on CM-ECF, and then by the Chairs of each Advisory Committee. That new language has been added to the published Committee Note in each Committees' parallel proposal. It reads: "Electronic service after business hours, or just

before or during a weekend or holiday, may result in a practical reduction in the time available to respond. Extensions of time may be warranted to prevent prejudice."

b. Change to the Caption

The Advisory Committee also agreed to amend the caption of the Rule published for comment to eliminate the additional words "Time for Motion Papers." These words do not appear in the caption of the existing Rule 45, and were included in the proposed amendment in order to parallel the current caption of Civil Rule 6, on which Rule 45 was patterned, as well as the caption to Bankruptcy Rule 9006. However, the added words do not describe the text of Rule 45. Instead, Rule 12 deals extensively with the time for motions.

c. Substituting "being served" for "service"

Finally, the Advisory Committee agreed to amend the proposed text of the amendment to Rule 45 as published so that it is parallel to the language of the other rules, referring to action "within a specified time after *being served*" instead of "time after *service*." The Committee is unaware of any substantive reason for the slightly different wording of Rule 45 as compared to the Civil and Bankruptcy Rules. The Committee believes it is prudent to revise the language of Rule 45(c) to eliminate the discrepancy while other changes are being made in Rule 45(c).

Recommendation–The Advisory Committee recommends that the proposed amendment to Rule 45 be approved as amended and transmitted to the Judicial Conference.

III. INFORMATION ITEMS

A. CM/ECF Proposals Regarding Electronic Filing

1. Discussion at the spring meeting

At the time of the Criminal Rules meeting, a proposed amendment to the Civil Rules would have mandated electronic filing, making no exception for pro se parties or inmates, but allowing exemptions for good cause or by local rule. The reporters for the Bankruptcy and Appellate Committees were also preparing parallel amendments. The proposed Civil amendment was of particular concern to the Advisory Committee on Criminal Rules because Criminal Rule 49 now incorporates the Civil Rules governing service and filing. Rule 49(b) provides that "Service must be made in the manner provided for a civil action," and Rule 49(d) states "A paper must be filed in a manner provided for in a civil action." Accordingly, any changes in the Civil Rules regarding service and filing would be incorporated by reference into the Criminal Rules. Also, the Advisory Committee on Criminal Rules has traditionally taken responsibility for amending the Rules Governing 2254 cases and 2255 Cases, and these rules also incorporate Civil Rules.

Committee members expressed very strong reservations about requiring pro se litigants, and especially prisoners, to file electronically unless they could show individual good cause not to do so, or the local district had exempted them from the national requirement.

The Committee's Clerk of Court liaison explained the development of the CM/ECF system, the current mechanisms for receiving pro se filings, and his concerns about a rule that would mandate e-filing without exempting pro se or inmate filers. The liaison explained various features of CM/ECF that work well for attorney users, but could cause significant problems with pro se filers, as well as several issues that may arise if CM/ECF filing were to be extended to those in custody or to pro se criminal defendants.

Some of the concerns raised apply to filings by pro se litigants regardless of whether they were accused of crime or in custody, such as lack of training or resources for training for pro se filers, concerns about ability or willingness of pro se litigants to obtain or comply with training, and increased burden on clerk staff to answer questions of pro se filers, particularly those who, unlike attorneys, are not routine filers. One of the most striking points our liaison made was that a person who has credentials to file in one case may, without limitation, file in other cases even those in which he is not a litigant. This feature of the system may pose much greater problems in the case of pro se filers who have not had legal training and are not bound by rules of professional responsibility.

Other issues raised by our liaison and other members were specific to the criminal/custody contexts. These concerns included the lack of email accounts for those in custody, as well as inability to send notice of electronic filing by email. Many federal criminal defendants, and all state habeas petitioners, are housed in state jails and prisons unlikely to give prisoners access to the means to e-file, or to receive electronic confirmations. Additionally, prisoners often move from facility to facility, and in and out of custody.

Committee members from various districts stated that the majority of pro se filers in their districts would not have the ability to file electronically. There is a constitutional obligation to provide court access to prisoners and those accused of crime, and members expressed very serious concerns about applying to pro se criminal defendants and pro se litigants in custody a presumptive e-filing rule that would condition their ability to file in paper upon a showing by the defendant or prisoner that there is good cause to allow paper filing, or upon the prior adoption of a local rule permitting or requiring pro se defendants and prisoners to paper file. Because of constitutionality concerns, members anticipated that most districts would eventually adopt local rules exempting criminal defendants and pro se litigants in custody from the requirement to file electronically, but they were not in favor of a national rule that would require nearly every district to undertake local rule making to opt out.

Because any change to the e-filing provisions in the Civil Rules would impact criminal cases, habeas cases filed by state prisoners, and Section 2255 applications by federal prisoners,

the Advisory Committee voted unanimously to direct the reporters and chair to share the concerns raised at the meeting with the other reporters, and to request that the Civil Rules Committee consider adding a specific exception for pro se filers to the text of its proposed amendment.

The Advisory Committee recognized that local rules could be adjusted to exempt pro se defendants and plaintiffs in habeas and Section 2255 cases. But there was a strong consensus among the members of the Advisory Committee that the proposed national rule should not be adopted if it will require a revision of the local rules in the vast majority of districts. The Committee members felt that any change in the national rule should carve out pro se filers in the criminal, habeas, and Section 2255 contexts. Although members recognized that a carve out for pro se filers has already been discussed and rejected by those working on the Civil Rules, they favored further consideration of a carve out given the concerns listed above.

Members also expressed support for consideration of revising the Criminal Rules to incorporate independent provisions on filing and service, rather than incorporating the Civil Rules. As demonstrated in the discussion of the issues concerning mandatory electronic filing, the considerations in criminal cases may vary significantly from those in civil cases. This project should also include the Rules Governing 2254 and 2255 cases, for which the Advisory Committee has responsibility.

2. Later events

Following the spring meeting, the reporters and chair shared the Advisory Committee's concerns with their counterparts on other committees, who were very responsive. The Civil Rules Committee received and approved at its spring meeting a revised version of the amendment under consideration that exempts persons not represented by counsel from the requirement to file electronically. The other committees also discussed extensively electronic service and signatures, issues that the Advisory Committee has not yet considered.

The Advisory Committee will benefit from the opportunity to study the provisions now under consideration in by the Civil Rules Committee (as well as the Bankruptcy and Appellate Rules Committee), so that it can determine how best to revise the Criminal Rules. As noted, this will include consideration of new provisions in the Criminal Rules that would replace the current provisions adopting the Civil Rules on filing and service. These issues have been referred to the Advisory Committee's CM/ECF Subcommittee, which will report its views at the Advisory Committee's fall meeting.

The Advisory Committee's goal is to have a proposed amendment that could be published, along with rules from the other committees, in August 2016.

B. New Proposal

The Committee also discussed a suggested amendment to Rules 35 that would bar appeal waivers before sentencing. It declined to proceed further with the proposal.

TAB 2B

THIS PAGE INTENTIONALLY BLANK

ADVISORY COMMITTEE ON CRIMINAL RULES
DRAFT MINUTES
March 16-17, Orlando, Florida

I. Attendance and Preliminary Matters

The Criminal Rules Advisory Committee ("Committee") met in Orlando, Florida on March 16-17, 2015. The following persons were in attendance:

Judge Reena Raggi, Chair
Hon. David Bitkower[1]
Judge James C. Dever
Judge Gary S. Feinerman
Mark Filip, Esq.
Chief Justice David E. Gilbertson
Professor Orin S. Kerr
Judge Raymond M. Kethledge
Judge David M. Lawson
Judge Timothy R. Rice
John S. Siffert, Esq.
Professor Sara Sun Beale, Reporter
Professor Nancy J. King, Reporter
Professor Daniel R. Coquillette, Standing Committee Reporter
Judge Amy J. St. Eve, Standing Committee Liaison
James N. Hatten, Clerk of Court Liaison[2]

In addition, the following members participated by telephone:

Carol A. Brook, Esq.
Judge Morrison C. England, Jr.

And the following persons were present to support the Committee:

Rebecca A. Womeldorf, Rules Committee Officer and Secretary to the Committee on Practice and Procedure
Bridget M. Healy, Rules Office Attorney
Frances F. Skillman, Rules Committee Support Office
Laural L. Hooper, Federal Judicial Center

[1] The Department of Justice was also represented throughout the meeting by Jonathan Wroblewski, Director of the Criminal Division's Office of Policy & Legislation.

[2] Mr. Hatten was present only on March 17.

II. CHAIR'S REMARKS AND OPENING BUSINESS

A. Chair's Remarks

Judge Raggi introduced Rebecca Womeldorf, the new Rules Committee Officer and Secretary to the Committee on Practice and Procedure. She welcomed observers Peter Goldberger of the National Association of Criminal Defense Lawyers and Robert Welsh of the American College of Trial Lawyers. She also thanked all of the staff members who made the arrangements for the meeting and the hearings.

B. Minutes of November 2014 Meeting

Judge Raggi reminded Committee members that the minutes, which were included in the Agenda Book, were approved last fall before their inclusion in the Agenda Book for the Standing Committee's January meeting.

III. CRIMINAL RULES ACTIONS

A. Proposed Amendment to Rule 41

Judge Kethledge, chair of the Rule 41 Subcommittee, reported on the history of the proposed amendment, the Subcommittee's review of the responses submitted during the public comment period, and its recommendations.

In September 2013 the Department of Justice came to the Advisory Committee with two problems. The current version of Rule 41 provides (1) no venue to apply for a warrant to search a computer whose physical location is unknown because of anonymizing technology, and (2) only a cumbersome procedure to apply for warrants to search computers that have been damaged by botnets that extend over many districts. Judge Kethledge emphasized these are procedural—not substantive—problems. The Department proposed an amendment to address these procedural problems.

In April 2014, the Advisory Committee significantly revised the Justice Department's original proposal, crafting a narrowly tailored proposed amendment that closely tracked the contours of the two problems that gave rise to it. The Standing Committee approved the publication of the proposed amendment for public comment.

The Rule 41 Subcommittee received and gave careful consideration to the public comments, including more than 40 written comments and three additional memoranda from the Department of Justice. Several hours of public comments were also presented at hearings before the full Advisory Committee in November 2014. The Subcommittee then held three conference calls in which it discussed the testimony, the written comments, the Department's memoranda, and its own concerns about some of the language of the published amendment.

After careful consideration, the Subcommittee unanimously recommended that the Advisory Committee approve several proposed revisions to the amendment as published, and

approve the revised amendment for transmittal to the Standing Committee.

Judge Kethledge summarized the issues raised in the public comments before stating the Subcommittee's specific recommendations for revisions.

In general, the concerns of those opposing the amendment are substantive, not procedural. Commenters argued that searches conducted under the proposed amendment would not satisfy the Fourth Amendment's particularity requirement, or would be conducted in an unreasonably destructive manner, or would violate Title III's restrictions on wiretaps. These are all substantive concerns on which the amendment expressly takes no position. The amendment leaves these issues for the courts to decide on a case-by-case basis, applying the Fourth Amendment to each application for a warrant.

Similarly, arguments that any changes should be left to Congress are unpersuasive. Venue is not substance. It is process, and Congress has authorized the courts "to prescribe general rules of practice and procedure." This amendment would be an exercise of that authority. Judge Kethledge noted that the Department of Justice had acted in conformity with Judicial Conference policy by using the Rules Enabling Act for these procedural issues rather than going to Congress.

The Department came to the Committee with a procedural problem that is impairing its ability to investigate serious computer crimes that are occurring now. Judge Kethledge respectfully submitted that it would be irresponsible for the Advisory Committee not to provide a venue for the government to make a showing to a judicial officer as to the lawfulness of these searches. He then invited other members of the Subcommittee (Judge Dever, Judge Lawson, Judge Rice, Mr. Filip, Professor Kerr, and the representatives of the Department of Justice) to comment.

Subcommittee members noted that the deliberative process had worked well: the proposed amendment had been narrowed to address the problems created by the current rule, and all of the comments had been reviewed and considered with great care. They expressed support for the amendment (with the proposed revisions to be discussed), and agreed that it addresses procedural—not substantive—issues. One member noted that a proposed revision to be discussed later in the meeting, using the term "venue" in the caption, may help to make this clear to the public. Responding to the concern that these matters should be left to Congress, Judge Raggi commented that under the Rules Enabling Act, Congress will necessarily play a significant role: any proposed amendment must be submitted to Congress before it can go into effect.

Professor Beale stated that the proposed amendment also includes provisions describing how notice of remote electronic searches is to be given. This portion of the proposed amendment will be applicable to all remote electronic searches, including those now being made under Rule 41 when the location of the device to be searched is known. The current notice provisions of Rule 41 are not well adapted to searches of this nature, because they refer to leaving a copy of the warrant and a receipt "at the place where the officer took the property." She noted that some of the comments focused on the adequacy of the proposed notice provisions, and that several of the

Subcommittee's proposed revisions of the amendment concerned the notice provisions.

Professor Beale thanked Ms. Healy for her work in the preparation of the agenda book, and noted that members had before them a hard copy replacement for one tab in the section on Rule 41.

Judge Raggi noted that the Subcommittee members and the staff had worked heroically to review the large number of comments received, including many at the very end of the comment period, and to prepare the agenda book under significant time constraints due to the short interval between the end of the comment period and the date for publication of the Agenda Book. Judge Kethledge concurred and also thanked the reporters.

Judge Raggi then invited comments from members not on the Rule 41 Subcommittee, asking members to focus first on the general issues raised by the proposed amendment. She confirmed that the members on the telephone could hear all of the discussion.

One member, acknowledging the care and hard work that had gone into the drafting and revision of the proposed amendment, nonetheless opposed it, raising concerns heard from the defense community as well as those who filed public comments. The member disagreed with the characterization of this as a procedural rule, arguing that it has too many substantive effects to be regarded as merely procedural. In effect, it opens the door to judges making ex parte decisions about core privacy concerns, and the defense does not participate until too late in the process, in back-end litigation. This is too great a risk. Authority tends to expand, and it is not possible to predict exactly how this authority will develop. Given the importance of the privacy concerns and the many unknowns, it is preferable for Congress to act first, as it did in Title III. In this member's view, the commenters who opposed did not misunderstand the amendment, because the result will not be narrow. In response to an observation that the defense role would be the same under the amendment as it would be for all other searches, the member expressed the view that the privacy concerns are greater here. For many people, computers are their lives, and these privacy concerns should be considered by Congress.

Another member said he was not hearing the same concerns from the criminal defense bar. He emphasized the public's interest in protections against new ways criminals can use technology to jeopardize the economy, national security, and individual privacy by identity theft, terrorism, corporate espionage, child pornography, and other serious offenses. Defense lawyers agree the government must be able to do its job in protecting society. For example, if a trade secret is lost, it is gone forever. The risk of such criminal activity is clear and present. In this member's view, the commenters who opposed the amendment did not recognize that the government must demonstrate probable cause to obtain a warrant, and they did not recognize the importance of affording the government a venue to show that it is entitled to a warrant to take the necessary actions to respond to these threats. There are risks that individual privacy will be invaded, but the greater risk to privacy comes from burgeoning electronic criminal activity, often shielded by anonymizing software, rather than government search warrants that must satisfy probable cause regardless of venue.

Judge Kethledge stated that it is the Committee's role and responsibility to address new problems when they arise, and this venue concern is a serious new procedural problem. There is a gap in Rule 41 that may prevent the government from obtaining a warrant because there is no way to identify the court that would have venue to consider the warrant application. The Committee should act to remedy this gap, which will allow the case law on the constitutional issues to develop in an orderly process as courts review warrant applications, rather than after the fact following warrantless searches based on exigent circumstances. If the New York Stock Exchange were to be hacked tomorrow using anonymizing software, under current Rule 41 there is no district in which the government could seek a warrant, and it would likely conduct a warrantless search under the exigent search doctrine, without prior judicial review.

Judge Raggi agreed that if the New York Stock Exchange were to be hacked by a computer using anonymizing software, it would be preferable to allow the government to seek a warrant from the court where the investigation is taking place, rather than conducting an exigent warrantless search. Concerns that judges may be uninformed about the technology to be used in the searches could be addressed by judicial education. The Federal Judicial Center has recently prepared some materials about topics such as cloud computing, and additional materials could be developed to help judges review applications for remote electronic searches.

A member observed that much of the public response is based, incorrectly, on the view that the amendment itself authorizes remote electronic searches. In fact, courts now issue such warrants under the current rules when the government knows the location of the subject computer. The only question addressed by this rule is how to proceed when anonymizing technology prevents the government from learning the computer's location so that it may go to the proper court to seek a warrant. Judge Raggi agreed, but noted that providing venue when anonymizing technology has been used may increase the number of warrant applications, and we cannot know how many such searches there will be, or how frequently they will be used in various kinds of cases.

Judge Kethledge and another member both noted that commenters who opposed the rule offered no alternative solution to the real venue problem the government has presented. A member noted that some opponents stated candidly that they did not want to provide a forum. This may immunize people who use anonymizing technology to commit serious crimes. Given the serious nature of the criminal threats requiring investigation, it would be irresponsible for the Committee to decline to take action to fill the current gap in the venue provisions. Here, as in many other situations, judges reviewing search warrants in any venue will have the duty to apply the substantive law to new situations.

On behalf of the government, Mr. Bitkower addressed the opponents' privacy concerns. He challenged the apparent assumption of many commenters that digital privacy concerns are greater than traditional privacy concerns. To the contrary, he said, cases such as the Supreme Court's decision in *Riley v. California* (2014) have recognized that the privacy rights in technology may be *on a par with* traditional privacy rights in the physical world. In the

government's view we should apply the same rules, as much possible, to technology as to the physical world: the same probable cause rules, the same particularity rules, and as much as possible the same procedural rules. Remote searches are conducted today, and by themselves do not present new issues. What is new is the ease with which someone can conceal his location by anonymizing technology, and the amendment addresses the venue gap created by that reality. The proposed amendment is privacy enhancing, because it provides a venue in which the government can seek advance judicial authorization of a search, just as it would before conducting a search of someone's home. This process allows the courts to apply the basic principles of the Fourth Amendment to new forms of technology, as they have done, for example, with heat sensors and tracking devices. The government's goal here is to secure a warrant, a privacy enhancing process.

Although several commenters argued that the Committee should follow the precedent of Title III and wait for Congress to act, Professor Beale observed that the history of Title III cuts the other way. Title III was enacted *after* the case law on wiretaps developed, just as the case law is doing now with other forms of technology in cases such as *Riley v. California*. In general, Congress has legislated after a sufficient number of cases have been litigated to shed light on the policy issues. In the case of new technology, the courts are grappling with questions of what information is protected by the Fourth Amendment as well as how requirements such as particularity apply in new contexts. The proposed venue provision would permit the same process to operate with remote electronic searches, allowing the courts to rule on the issues of concern to the commenters. Although it is possible that providing venue will increase the number of remote searches, Professor Beale noted that it may instead increase the number of remote searches reviewed by the courts ex ante in the warrant application process, rather than only ex post following a search yielding information that the government seeks to introduce at trial.

Judge Sutton complimented the Committee on narrowing the proposed amendment and being responsive to the public concerns. He observed that approving venue for warrant applications is not the same as approving remote electronic searches. Rather, it permits more litigation as to search warrants that will shed light on the process and issues. He emphasized that the Rules Enabling Act tells the judiciary to promulgate rules of procedure, not to wait for Congress to act first. Instead, Congress responds to proposed rules.

The member who had stated opposition to the proposed amendment acknowledged that courts must deal with the issues raised by new technology but remained unable to support the amendment, characterizing it as substantive and reiterating there are many unknowns.

Discussion turned to the question what would be known or unknown in the warrant applications covered by the amendment. Mr. Bitkower noted that to obtain any warrant the government must know what crime it is investigating and what it is looking for. In the anonymizing software cases covered by the amendment, the only new unknown is the physical location of the device to be searched. Because Rule 41 currently provides no venue for a warrant application in such cases, if the government deems a situation serious but not "exigent," it must

now either wait or pursue other investigative techniques that may in some cases be more invasive. In botnet cases, he noted, the problem is the large number of computers, not the lack of information.

A member expressed the view that the most significant unknowns would arise in the botnet cases: what information might be sought from thousands or even millions of computers that had been hacked. Moreover, the technology required for different botnets may vary. He also noted that the Committee was being forward thinking in addressing these issues, since there have been relatively few botnet investigations and only one decision holding that a court cannot issue a warrant when anonymizing software has disguised the location of the device to be searched. It was sensible, he concluded, to address both problems with a narrowly tailored "surgical" amendment.

Agreeing that each criminal botnet is unique, Mr. Bitkower explained that one function of warrants under the proposed amendment could be to map a botnet before seeking to shut it down, collecting the IP addresses of the affected computers to determine the botnet's size and where the computers are located. In previous botnet investigations, the cumbersome requirement of seeking a warrant in each district played a role in determining the government's strategy, and civil injunctions were used. He also noted that warrant applications under the amendment would vary widely: in some cases they may be quite simple and narrow (as in the case of a single email account when the government has already obtained the password), but in other cases there will be more significant complications and new issues on which courts will have to rule.

Members compared the procedural options under the current rule and the proposed amendment in the investigation of the hacking of a major corporation or institution such as the New York Stock Exchange. If the NYSE were hacked and anonymizing software disguised the location of a device the government had probable cause to search, members speculated that the government would conduct a search under some legal theory. They identified three possible scenarios under the current rule: (1) the government might persuade a court in the Southern District of New York to grant the warrant, and then claim good faith reliance if the warrant were later invalidated for lack of venue; (2) a court in the Southern District might find probable cause but determine it had no authority to issue a warrant, in which case the government might conduct a warrantless search and argue that the failure to obtain a warrant was harmless error because the search was nevertheless supported by probable cause; or (3) the government might search without a warrant under a claim of exigent circumstances. Members expressed the view that these examples showed why it would be preferable to amend Rule 41 to provide venue for warrant applications, so that courts asked to approve such warrants would be able to focus on the constitutional issues presented by remote computer searches. Concerns about the judiciary's understanding of the technology could be addressed by judicial education.

In response to the question how frequently the government expects to seek warrants under the proposed amendment, Mr. Bitkower noted the use of anonymizing technology by criminals is likely to become much more common. Until recently only sophisticated criminals employed

anonymizing software, but the technology is now more readily available and easier to use. In the case of botnets, in prior cases the government used non-criminal tools, but the lack of efficient venue provisions skewed the government's choices. So that authority might be employed in future cases.

Judge Raggi then called for a vote on the question whether to move forward with the proposed amendment.

By a vote of 11 to 1, the Committee voted to approve the amendment for transmission to the Standing Committee (subject to further discussion of the minor revisions proposed by the Subcommittee).

At Judge Kethledge's request, Professor Beale described the revisions proposed by the Subcommittee. The first revision was to substitute "Venue for a Warrant Application" for the current caption "Authority to Issue a Warrant." This proposal responded to the many comments that assumed the amendment would allow a remote search in any case falling within the proposed amendment (for example, any case in which an individual had used anonymizing technology such as a VPN). These commenters mistakenly viewed the amendment as providing substantive authority for such remote electronic searches, which they strongly opposed.

Beale noted that after the final Subcommittee call agreeing to amend the caption, Professor Kimble, the style consultant, first opposed making any change on the ground that no reasonable reader of Rule 41 as a whole could fail to see the many additional requirements. When advised that much of the opposition to the rule was founded on this misunderstanding, Kimble proposed an alternative caption "District from Which a Warrant May Issue." Professor King suggested that Professor Kimble may have believed this language would be clearer to lay readers than the term "venue."

Discussion focused on the need for a change in the caption, and the difference between the alternative captions. Professor Beale reminded the Committee that if there were no substantive difference, but only a question of style, it would ordinarily accept the style consultant's proposed language.

Judge Kethledge stated his strong support for amending the caption and using the Subcommittee's language. The current caption is overbroad and misleading, seeming to state an unqualified "authority" to issue warrants meeting the criteria of any of the subsections. Although Professor Kimble suggested this reading would be unreasonable, Judge Kethledge asserted that the current caption is unclear and is causing serious public opposition. By retaining the reference to "issu[ing]" warrants, Professor Kimble's language may perpetuate the misunderstanding. "Venue" is much clearer.

Members discussed the impact of different words and phrases. Several expressed support for the use of "venue," though another noted that it may not be known to non-lawyers and "venue" for the filing of a criminal case is defined differently than "venue" for the warrant applications under Rule 41(b). Judge Raggi observed that "venue" would be very clear to the

judges applying the rule. A member who agreed with the Subcommittee's recommendation also noted that other references to "authority" in the existing subsections of Rule 41(b) are also unclear; he observed that at some point it might be helpful for the Committee to revise and clarify all of the subsections.

Professor Coquillette commented that the discussion had made it clear that the Committee was grappling with a question of substance, not mere style.

The Committee voted unanimously to amend the caption of Rule 41(b) to "Venue for a Warrant Application."

Professor Beale explained that the Subcommittee also recommended two small changes in the notice provisions, Rule 41(f)(1)(C), both of which are intended to make notice of remote electronic searches parallel to the notice provided for physical searches to the extent possible.

The first change adds the requirement that the government serve a "receipt" for any property taken (as well as the warrant authorizing the search). In drafting the published notice provisions, the Committee had inadvertently omitted this requirement. Since this addition would parallel the requirements Rule 41(f)(1)(C) now imposes when the government makes a physical search and provide an additional protection for privacy, the reporters were confident it would not require republication.

The second change rephrased the obligation to provide notice to "the person whose property was searched or <u>who possessed the information that was seized or copied</u>." Again, the Subcommittee's intent was to parallel the requirement for physical searches. The Subcommittee rejected the suggestion in some public comments that the government should be required to provide notice to both "the person whose property was searched" <u>and</u> whoever "possessed the information that was seized or copied," since that is not required in the case of physical searches. For example, if the Chicago Board of Trade is served with a warrant and files containing information regarding many customers are seized, the government may give notice of the search only to the Board of Trade, and not to each of the customers whose information may be included in one or more files. The same should be true in the case of remote electronic searches. Discussion followed on how the current notice provisions applied to various hypotheticals.

The Committee voted unanimously to revise the amendment as published to require the government to serve a "receipt" as well as the warrant, and to provide notice to "the person whose property was searched or <u>who possessed the information that was seized or copied</u>."

Professor Beale then turned to two proposed revisions to the Committee Note. The first addition explained the new caption:

> **Subdivision (b).** 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 requirements for the issuance of a warrant, which must also be met.

Members emphasized that the first sentence was not inconsistent with their earlier conclusion that the language of the caption presented a substantive, not merely a style issue. The

point made in the Committee Note is that the change in the caption does not alter the meaning of the existing provisions in Rule 41(b). Rather, it clarifies the effect of the amendment, making clear what the amendment does and does not do. The last sentence responds directly to the many public comments misunderstanding the effect of the amendment, stating that there are also constitutional requirements that must be met. A member suggested that the meaning would be clearer if the last sentence were revised to state that the constitutional requirements must "still" be met, and Judge Kethledge accepted this as a friendly amendment.

The Committee voted unanimously to add the following language to the Committee Note:

> **Subdivision (b).** 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 requirements for the issuance of a warrant, which must still be met**.**

Finally, Professor Beale asked for approval of the Subcommittee's proposed addition to the Committee Note regarding notice. The proposed addition explains the changes after publication, and also responds to the many comments that criticized the proposed notice provisions as insufficiently protective because they required only reasonable efforts to provide notice. The addition draws attention to the other provisions of Rule 41 that preclude delayed notice except when authorized by statute and then provides a citation to the relevant statute. Professor Coquillette commented that because of the widespread confusion on this point in the public comments, the proposed addition was an appropriate exception to the general rule that committee notes should not be used to help practitioners. Members agreed that the citation "See" is appropriate because at present the statute referenced is the only authority for delayed searches (though other provisions might at some point be added).

The Committee voted unanimously to add the underlined language to the Committee Note:

> **Subdivision (f)(1)(C).** The amendment is intended to ensure that reasonable efforts are made to provide notice of the search, seizure, or copying<u>, as well as a receipt for any information that was seized or copied, to the person whose property was searched or who possessed the information that was seized or copied. Rule 41(f)(3) allows delayed notice only "if the delay is authorized by statute." See 18 U.S.C. § 3103a (authorizing delayed notice in limited circumstances).</u>

B. Proposed Amendment to Rule 4

Judge Lawson, chair of the Rule 4 Subcommittee, described the public comments on the proposed amendment and the Subcommittee's recommendation that the amendment be approved as published and transmitted to the Standing Committee. One speaker at the hearings in November 2014 supported the proposed amendment, and there were six written comments. One comment urged that the proposal be withdrawn. The others supported the amendment, though some suggested modifications in the text or committee note. The Subcommittee met by telephone to consider the comments.

Judge Lawson reminded the Committee that the proposed amendment is intended to fill a

gap in the current rules, which provide no means of service on an institutional defendant that has committed a criminal offense in the United States but has no physical presence here.

Judge Lawson explained the Subcommittee's views on various issues raised by the law firm of Quinn Emanuel Urquhart & Sullivan (which represents a foreign corporation that the Justice Department has been unable to serve) in support of its recommendation that the proposed amendment should be withdrawn. First, Quinn argued, by stating that any means which provides actual notice is sufficient, the rule creates a situation in which any institutional defendant that appears to contest service has in effect admitted it has been served. The Subcommittee agreed with the Justice Department's response: the point of the amendment is to provide a means of service that gives notice, and there is no legitimate interest in allowing a procedure in which an institutional defendant can feign lack of notice. If the amendment were adopted, there would be, however, objections an institutional defendant might assert by a special appearance (such as a constitutional attack on Rule 4, an objection to a retroactive application of the amendment, or a claim that an institutional defendant has been dissolved.) And, Judge Lawson said, the Subcommittee also found unpersuasive the Quinn law firm's reliance on the Supreme Court's decision in *Omni Capital Int'l v. Wolff*. The Court simply required that service be made in compliance with the Rules of Civil Procedure. Here, by amending Rule 4 to provide for service, the amendment will allow the government to make service in a manner provided for in the Rules of Criminal Procedure.

The Subcommittee was not persuaded by comments of the Quinn firm and the National Association of Criminal Defense Lawyers (NACDL) expressing concern about the consequences of not honoring a summons, particularly a concern that this would permit trials in absentia. Judge Lawson noted that Rule 43 generally prohibits trial in absentia. Institutional defendants may appear by counsel, but their counsel must be present. NACDL suggested that the amendment or Committee Note be revised to include a reference to Rule 43. Noting the general principle that the Rules are to be read as a whole, the Subcommittee concluded it would not be wise to cross reference here to a single rule. Indeed, doing so might have negative implications when other provisions are not cross referenced. Judge Lawson also noted that trial in absentia was not among the long list of possible remedies that the Department of Justice identified in the August 2013 memorandum (included on pages 79-84 of the Agenda Book), which included criminal contempt, injunctive relief, the appointment of counsel, seizure and forfeiture of assets, as well as a variety of non-judicial sanctions (such as economic and trade sanctions, diplomatic consequences, and debarment from government contracting).

The Subcommittee also declined to adopt suggestions that the amendment be revised to provide an order of preference among the permitted methods of service. This issue, Judge Lawson noted, had been considered by the full committee, which previously determined that a requirement of this nature could generate burdensome litigation. The Subcommittee agreed.

The Subcommittee declined the Federal Magistrate Judges Association's suggestion that the committee note be revised to state that the manner of service must comply with Due Process. Judge Lawson explained the Subcommittee's view that this was unnecessary, since the Constitution must always be honored.

The Quinn law firm argued that the amendment was unwise because it would lead to reciprocal action by foreign governments against U.S. firms. Judge Lawson reminded the

Committee that it had discussed this issue at length before voting to approve the amendment for publication. As explained by the Justice Department's representatives and described in detail in the Department's August 2013 memorandum, federal prosecutors would be required to consult with the Justice Department's Office of International Affairs (which consults with the Department of State) in effecting international service.

Judge Lawson noted a final suggestion by NADCL fell outside the current proposal.

After considering all of the comments, Judge Lawson said, the Subcommittee voted unanimously to recommend that the proposed amendment be approved as published and transmitted to the Standing Committee. He then called on the Subcommittee members, Judge Rice, Mr. Siffert, and Mr. Wroblewski (representing the Department of Justice) for any additional comments.

Mr. Wroblewski thanked Judge Lawson, the Subcommittee members, and the reporters for their efforts, and he noted that the Justice Department's original proposal had been revised and improved. He commented on the reciprocity concerns, noting that federal prosecutors face reciprocity concerns every day in a variety of contexts, such as arrests and witness interviews. The United States Attorneys' Manual provides that whenever a federal prosecutor attempts to do any act outside the United States relating to a criminal investigation or prosecution or takes any other action with foreign policy implications the prosecutor is required to consult with the Office of International Affairs.

Judge Raggi observed that because that the government cannot try a defendant who has not filed a notice of appearance, the amendment might not result in a significant increase in prosecutions if non-U.S. entities don't file a notice of appearance. In such cases, however, if service has been made the government will be able to take a variety of collateral actions. The amendment is not radical. It simply provides a means of service, filling a gap in the rules.

Professor Coquillette recalled occasions when foreign governments raised objections to proposed amendments for the first time very late in the process (even at the point of Congressional consideration). He was happy to hear that the Departments of Justice and State had already consulted about this rule, and he urged the Department of Justice to do whatever it could to encourage counterparts at the State Department to bring to light now any possible objections from other nations. The Department's representatives agreed this was important, noting there had been long discussions between the Departments of State and Justice before the proposal was submitted, and throughout its consideration.

Judge Lawson added one final observation. The Quinn law firm proposed withdrawing the amendment without providing any alternative, which would mean that it would not be possible to make effective service on entities such as the Pangang Group (which the government has been unable to serve under the current rules). He noted that the Quinn law firm represents the Pangang Group, and in effect was seeking to defend it by preventing the initiation of the prosecution. This case, he said, demonstrates the necessity for the amendment. Without it, foreign entities can violate U.S. law with impunity.

Judge Sutton inquired into the breadth of the language in the proposed amendment to Rule 4(a), allowing the court to take "any action authorized by United States law" if an organization defendant fails to appear after service. Should it be limited to actions against the organizational defendant? Judge Raggi explained that not all appropriate responses would be actions against the organizational defendant itself. Notably, in rem sanctions might be available. And Professor Beale noted that United States law would not authorize sanctions that lacked a sufficient connection to the organizational defendant. Judge Sutton indicated he was satisfied that the broad language was appropriate.

On Judge Lawson's motion, the Committee voted unanimously to approve the proposed amendment as published and transmit it to the Standing Committee.

C. Proposed amendment to Rule 45

Judge Lawson, chair of the CM/ECF Subcommittee, presented the Subcommittee's recommendations regarding the previously published amendment to Rule 45 that would eliminate the three extra days provided after electronic service. The amendment reflects the view that electronic transmission and filing are now commonplace and no longer warrant additional time for action after service. It was published for comment in the fall of 2014. Similar proposals will be considered at the spring meetings of the other Rules Committees.

Judge Raggi noted that with this and other uniform rule changes being considered by all of the Rules Committees, the Criminal Rules Committee ought to consider whether criminal cases require different treatment. For example, in criminal cases there may have to be more play in the procedural joints, both as a matter of fundamental fairness when someone's liberty is at stake, and to avoid collateral challenges when convictions are obtained.

Judge Lawson discussed the Subcommittee's review of the comments received on the amendment to Rule 45. He first noted that the Subcommittee had rejected the Federal Magistrate Judges Association's suggestion either to eliminate all of the parentheticals in the proposed rule or to revise the rule to refer to "(F) (other means consented to except electronic service)." The Subcommittee concluded that the parentheticals were helpful, not confusing, and that the Committee Note clearly states that no extra time is provided after electronic service.

The Subcommittee recommended one change to the Committee Note that was published for comment and two changes to the text.

Judge Lawson first addressed the Subcommittee's recommended change to the Committee Note, which responded to concerns raised in the public comments. The Pennsylvania Bar Association and the National Association of Criminal Defense Lawyers had opposed the proposed amendment's elimination of the additional three days because of the difficulty it would cause practitioners and their clients. They emphasized that many criminal defense counsel are solo practitioners or in very small firms, where they have little clerical help, and do not see their ECF notices the day they are received. The Department of Justice expressed a similar concern

about situations in which service after business hours or from a location in a different time zone, or an intervening weekend or holiday, may significantly reduce the time available to prepare a response. In those circumstances, a responding party may need to seek an extension.

The Subcommittee recommended that in light of these legitimate concerns, the Committee Note to Rule 45(c) be revised to include language addressing this problem drafted by the Department of Justice:

This amendment is not intended to discourage courts from providing additional time to respond in appropriate circumstances. When, for example, electronic service is effected in a manner that will shorten the time to respond, such as service after business hours or from a location in a different time zone, or an intervening weekend or holiday, that service may significantly reduce the time available to prepare a response. In those circumstances, a responding party may need to seek an extension.

Judge Lawson noted that the Subcommittee thought added language encouraging judges to be flexible when appropriate and to expand those deadlines would allow judges to address matters on the merits. This was consistent with the position the Committee adopted for Rule 12. Liberality is especially important in the criminal context, he explained, because overly rigid application would inevitably result in Section 2255 motions and other collateral attacks. The note language keeps the text of the rule the same among committees but recognizes the particular need for flexibility in this context.

A member opposed to the amendment objected to this "compromise," arguing that Note language is not the same as leaving the extra three days in the text of the Rule. A client may be incarcerated and cannot be reached, and if the lawyer learns about it late Friday night, but the judge says no once there is a chance to seek an extension on Monday, three or four days to respond is not enough. Another member noted that local rules may have seven day limitations even if there are no seven day limitations in the Criminal Rules.

Professor Coquillette asked the Committee to focus on why the criminal rule should be different, if the other committees are comfortable with the elimination of the three extra days after electronic service. A member explained that the client in a criminal case is often incarcerated, which restricts counsel's access, and that responses often must be run by the client face to face in order to be accurate. Another member voiced opposition to eliminating the three days in criminal cases for two reasons. First, it is much more difficult to talk to the client before filing a response because of the distance to the location where the client is incarcerated and second, in some places local rules are interpreted liberally and some not.

Judge Raggi emphasized that there is a strong preference for uniform timing rules, so that a departure for the Criminal Rules must be justified.

After a short break, a member previously expressing opposition to the amendment to the text of the Rule withdrew that opposition based on the expectation that the note language would be included.

The Committee then unanimously approved adding to the Committee Note as published the additional language concerning extensions that had been proposed by the Department of Justice.

Professor Beale noted that the chair and reporters might need some latitude in moving forward with the new note language, given that each of the other committees will be considering this in the weeks to come and some tweaks might be necessary to achieve uniformity.

Judge Lawson then presented the Subcommittee's two recommendations to modify the text of the published amendment, each based on comments received during the publication period. The Subcommittee did not believe either change required republication.

The first recommended change was to eliminate the added phrase "Time for Motion Papers" from the caption of Rule 45, and keep the caption as it is now. Rule 12 deals extensively with the time for motions and Rule 45 does not.

The second recommendation was to modify the language of Rule 45(c) to parallel the language used in other sets of rules, referring to action "within a specified time after being served" instead of "after service." There was no reason for different phrasing in the Criminal Rule.

A motion was made to approve the text of the rule as published, with these two changes, and adopted unanimously.

D. CM/ECF Subcommittee

Judge Lawson presented the Subcommittee's recommendation regarding a mandatory electronic filing amendment being considered by the Civil Rules Committee (as well as the Appellate and Bankruptcy Committees). He explained that the proposed Civil amendment is of particular concern to the Criminal Rules Committee because Criminal Rule 49 now incorporates the Civil Rules governing service and filing. Rule 49(b) provides that "Service must be made in the manner provided for a civil action," and Rule 49(d) states "A paper must be filed in a manner provided for in a civil action." Accordingly, changes in the Civil Rules regarding service and filing will be incorporated by reference into the Criminal Rules. Also, the Criminal Rules Committee has traditionally taken responsibility for amending the Rules Governing 2254 Cases and 2255 Cases, and these rules also incorporate Civil Rules.

Judge Lawson explained that the Civil Rules Committee is considering a proposal mandating e-filing that does not exempt as a class pro se filers or inmates. Exemption is allowed either by local rule or by a showing of good cause. There are a number of districts that do not permit pro se e-filing except upon motion, and particularly discourage prisoners from e-filing because of the potential for mischief. There are also issues regarding electronic signatures. The question for the Committee is whether criminal cases warrant a different rule than that being considered by the Civil and Appellate Committees.

Professor King added that the issue is on the agenda now so that the Criminal Rules Committee's views on these issues can be conveyed to the other committees which will be considering this in the weeks to come. Also, she noted that the CM/ECF Subcommittee discussed the pro se issue and was unanimous in rejecting for criminal cases any rule that would require either a local rule or a showing of good cause in order to exempt pro se and prisoner filers. The reporters have conveyed our Subcommittee's view to those working on the rules for the other committees but so far they have not been sympathetic. Professor Beale added that the members of the working group for the Civil Committee preferred allowing districts to handle rules for pro se filers on a district-by-district basis.

The Committee's Clerk of Court Liaison, Mr. Hatten, who had been asked to share his views and experience on this issue with the Committee, presented several concerns raised by a rule that did not include an exception for pro se or inmate filers.

Mr. Hatten noted that because the CM/ECF system is a national platform that individual districts cannot modify, problems raised by extending e-filing to pro se filers will become embedded, and allowing courts to opt out will not avoid those structural problems. He noted various districts have been able to extend e-filing at their own pace, adapting to resource constraints and local challenges, and he knows of no court that extends e-filing to prisoners. Among the variations are differences in whether attorney filers may e-file sealed documents and case initiating documents.

As to pro se electronic filing, Mr. Hatten doubted the system was ready for a mandatory rule. We do not know the number of courts that presently allow this, and the extent of their experience. Many courts, perhaps even a majority, do not allow any electronic filing by pro se litigants. We really don't know how this would work because the experience with it has not been evaluated. He reviewed the history of the development of the CM/ECF system, designed for attorney use, and expressed the concern that many courts may find as a matter of policy that e-filing by pro se litigants is inappropriate or that the system is inadequate. A transition to pro se e-filing, he suggested, would not be facilitated by an opt-out rule, but instead would require further study and adequate resources, including staff resources.

Next, Mr. Hatten reviewed a number of potential problems that might arise. First, the current system anticipates a certain level of legal training and knowledge on the part of the person using the system, including knowledge of the rules as to what to file, when, and in what format. Non-lawyer, untrained filers may incorrectly characterize or describe their filings, tasks that are already a challenge for some lawyers. Pro se filers may file the same thing multiple times, fail to attach required documents, or attach the wrong document. This difficulty would be enhanced if the person is not a recurring user. Judges must use these designations, which may not be clear. Lawyers who must respond to the filing also may experience additional burdens. Court staff review docket entries for accuracy, and if there is an error, the staff must make a separate entry to rename the docket entry; they do not change the original filing. Increased errors would require increased staff resources for review and correction of docket entries. His court has had experience with pro se filers inferring some nefarious motive on the part of court staff when a docket entry is changed. This is in addition to the increased resources needed to train pro se filers.

Judge Raggi asked whether electronic filing or paper filing is a more efficient use of clerk's office staff. Mr. Hatten responded that for attorney filers there is a great advantage in electronic filing, but there will not be the same advantages for pro se filers. Pro se filers will be calling staff with normal questions you would expect from someone with less experience about how to file and other aspects of the system. And the quality control will be a very significant burden because pro se litigants will not understand the significance of what they are filing.

Mr. Hatten continued that in contrast to paper documents which can be screened before entry in the system, there is no ability to pre-screen materials before they are e-filed to identify any pornographic, confidential, libelous, or otherwise offensive or objectionable materials. E-filing results in immediate access via the internet to whatever is filed, through PACER or through subscription services such as Lexis or RSS feeds. There is no filter on the PACER system, which anyone can use. There are services that provide to a subscriber instantaneous access to anything filed in a particular case. Once captured and broadcast by these services, documents cannot be re-captured. This could lead to the release of personal data or materials that should not have been filed. Because electronic filings made late Friday are not reviewed by staff until Monday, there is a period of time when the unreviewed information would be available to anyone. Issues created by a pro se filer's use of the system could be addressed by a court after the fact, but any harm through unretrievable dissemination of offensive, confidential, or sealed materials would already have taken place. If the filing was in paper and screened first, the staff would review the document, then scan it, give it an appropriate name, and docket it.

Additionally, Mr. Hatten raised the potential of the "loss of docket integrity" if login and password information is made available to non-lawyers. Once issued a password in CM/ECF, any individual using that login information may access and file in any case in the system, regardless whether that person is a party to the case or whether the case is open or closed. For example they can file in any defendant's case. That login and password could be used by anyone who obtains it. There are no means to verify the identity of the actual individual accessing the system, if someone were to suggest that the login information was used without authorization. Potentially, with login information, someone unconstrained by the rules governing attorneys could maliciously interfere in unrelated cases. Expanded access by non-attorneys could even lead to denial of service attacks on the system, he noted, emphasizing that this was speculation. He did not know if expanding access would raise the risk of the introduction of malware or other viruses into the system, which until now has been very reliable. He noted that courts can block use of a password, but it would be "shutting the door after the cow's left the barn." Any information, such as information about a victim, or sealed materials that someone had filed electronically after obtaining them in paper form, would have already been released.

Judge Raggi asked if this ability to file in any case has been the subject of previous discussion. Mr. Hatten noted that it hadn't been a problem as far as he knew, because all filers were attorneys. Judge Lawson noted that this was one of the main reasons his district restricted CM/ECF access to attorneys.

Mr. Hatten continued that electronic notice of filing requires an individual email account, and it is not known whether pro se filers filing from an institution will be able to receive such notices, because of capacity limits or spam filters. Even in instances with a good lawyer email address, those email accounts are sometimes so full the court gets a bounce back. Sources a pro se party may use for filing, such as a public library, may be unavailable to receive email. The CM/ECF system requires the ability to contact a filer regarding missing information such as address or phone number. If delivery is not available, a paper notice would be required, which would reduce any advantage from e-filing.

Electronic filing, Mr. Hatten observed, may also require that the filer qualify for electronic payment. Those who lack credit cards, such as inmates, may not be able to file case-initiating documents.

Another concern, Mr. Hatten stated, was that the round-the-clock availability of the e-filing system. Past experience with some pro se paper filings suggests that extending e-filing to pro se litigants would significantly increase the volume of prisoner and pro se filings. Courts have experience measuring the filings of vexatious litigants in pounds not pages. Many examples are readily available. He mentioned two in his district: one, using paper filings only, filed 964 appeals in eleven regional circuits and the Federal Circuit and 2637 civil actions nationwide; another, using paper filings only, filed 76 appeals in four circuits, and 33 civil actions in 17 districts.

Perhaps extending e-filing to pro se filers could overcome some of these issues if the system could be modified to allow pro se filings to drop into a box so that court staff could review them before anybody else would see them. That might be better, but it is not possible in the existing system. Moreover, there are no resources available to court staff to implement a program of this potential magnitude, he said.

Mr. Hatten also raised the concern that if the rule changed to require e-filing unless there was a local rule or a showing of good cause, courts may expect demands by pro se and prisoner filers that they are entitled to access CM/ECF. Finally he raised a concern about the language of the proposed change to the Civil Rule referring to the electronic signature.

Judge Raggi asked the Department of Justice to share its views about extending e-filing to pro se and prisoner filers. Mr. Wroblewski stated that it seems clear the CM/ECF system is just not ready to handle all of the types of cases the Department sees, especially the Section 2255 cases. For example, the courts are in the middle of a retroactive guideline change, and in many districts the prisoners have no attorneys, but all are required to file, and although many have access to email, none have access to the internet. And there are tens of thousands of prisoners who are being held by the Marshal's Service, mostly in county jails, not federal facilities, with no computer access. We are just not ready for this, he stated, and are very concerned that we need to provide access to the courts for all of the pro se litigants, including those incarcerated.

On the electronic signature issue, he noted, there had been concern that it might cause problems with prosecuting bankruptcy fraud, but the Department doesn't see a huge problem with the criminal filings, at this point. But they are not ready to jump to a mandatory system.

In response to a question whether the Department thought the proposed rule provides enough flexibility, Mr. Wroblewski stated they will defer to the courts, but just want to make sure that all criminal litigants, including Section 2254 filers, have a way to access to the courts. If courts want to opt out of a new rule, and guarantee access that way, that is fine, but the courts must be open to these litigants.

Judge Raggi noted that the electronic filing proposal is being advanced with great vigor by the other Committees, but no one has indicated what the fallback plan would be should the system fail, either from an attack on the system itself or some other disaster. There is a real need for courts to operate in times of emergency, such as 9-11 or Hurricane Sandy, but there seems to be no fallback plan should the computers fail. District judges no longer maintain their own dockets, but are subject to the dictates of nationwide technology. She urged that in working with other committees, we should keep in mind that the Criminal Rules' unique concern with liberty. She also observed that requiring e-filing may put more distance between those who use the courts and the courts, and that the added resources needed to allow this to work aggravates these concerns. But the fundamental point is that these are criminal litigants in proceedings about liberty. She encouraged members to think about what is the advantage to them or us of having those papers filed electronically as opposed to hard copy.

In response to her request for input from members about whether this could be handled at the local level, one member related that in his district 10% of pro se filings are being filed electronically. As to pro se filers, this member reported, they have not had any problems. If a pro se filer does not want to file in CM/ECF, it is simple to opt out, and 90% of pro se's do opt out and file with paper. They file a form requesting they not have to file electronically and the magistrate routinely grants it. The good cause is usually "I don't have access to the Internet."

His district also has two state prisons, the member continued, and the state department of corrections has a very new limited pilot program allowing prisoners to file electronically in Section 1983 cases, not habeas actions. This is a good thing, he reported, because it has cut down the many, many pages of hard to decipher handwriting. Prisoners use a computer station to file these documents, so they come in typed in a standard format. Prisoners have time allotted to go to that location and file that document. He noted that there were so many prisoner filings, more than half of the docket, and the program was driven by that volume. He reiterated that the program is in "an infant stage," and that it could go sideways.

Another member noted that her district allows pro se filing in civil cases but requires training first, and she thought that a few districts were working on pilot projects allowing persons in custody to make filings. But this member could not imagine how this could possibly be required in habeas cases because state facilities don't give access.

Another member noted that if there is a top-down rule that says e-filing is required but you can opt out, at least 92 districts will opt out. Those who are detained but not yet convicted are in county jails in his district, with no computers. The state doesn't even have electronic filing for lawyers, and his district doesn't allow pro se e-filing, for some of the reasons stated before. There are ways to work toward this gradually, but having a top-down rule that everyone opts out of is not

good process, and reflects badly on the credibility of the rules process.

Professor Coquillette noted that local rules have been a matter of concern for Congress for decades, because they don't have the oversight provided by the Rules Enabling Act. Sometimes, however, there is a national rule that says go out and make local rules. This occurs in two situations: where there are real differences district to district, and where the subject matter is so premature it requires experimentation. Both of those conditions may apply here.

Another member noted that in 90% of situations the mandatory e-filing rule is ill advised and out of touch for people in county jails. His state has a tremendous budget crisis, won't fund providing prisoners with facilities to file electronically, and prisoners would file suits alleging denial of access to the courts. It is a top-down rule to fix a problem that doesn't exist. Already there are functioning local rules, and no need for this massive energy to change a system that seems to be working. This member was not aware of any reason that providing internet access to prisoners would be a priority, or that prisoner filings should be lock step with filings in civil cases.

Professor Beale suggested that we could amend Rule 49 in various ways to accommodate a different rule for criminal cases if the Civil Rules Committee proceeds with the existing draft. However, the Civil Rules Committee might put their proposed rule on hold, and study it more, or decide it is ready to publish something now, but agree to slow down later.

Professor Coquillette stated that the Standing Committee would want to hear what the Criminal Rules Committee thinks is best for criminal cases.

Judge Raggi asked the Subcommittee to meet again before the Standing Committee meets to consider what sections might be amended to deal with these concerns as to Rule 49 and also the 2254 and 2255 Rules to the extent we are responsible for them.

A member added that our goal would be to have our own amendment to Rule 49 take effect before 92 districts had to opt out of a mandate.

Judge Lawson expressed appreciation for Mr. Hatten's contribution. He noted the Subcommittee was comfortable with requiring e-filing for lawyers, and had not addressed prisoner filings in 1983 cases. The Subcommittee opposed a Civil Rules amendment that provided no carve out for pro se or prisoner filers. He agreed with the many concerns discussed, and noted that not all of those who file in criminal cases are parties. Witnesses, law enforcement, and third party owners would not necessarily have CM/ECF access. Most importantly, he argued, the rule implicates constitutional rights that do not arise in civil cases, and requiring pro se prisoner filers to demonstrate good cause before they can access the courts would probably raise constitutional issues. He asked the Committee to convey its preference for an approach that carves out pro se filers from any mandatory rule.

A member noted that he is in favor of that motion, that in his district this is not done, and that a top-down rule is a bad idea if clerks and local committees in almost every district wonder how out of touch this is. On the ground, pro se litigants are not filing through CM/ECF.

Judge Raggi agreed we can make these suggestions to the Civil Rules Committee, and she favored doing so, noting that a litigant who wants to go into every case in a judge's docket could cause a fair amount of trouble. But she also urged that the Criminal Rules Committee should also have an alternative plan in reserve.

A member said our alternative should be to work on delinking our rule from the Civil Rules. Another member noted the Committee may have to recommend amendments to 49(b) and (d), and a third noted that 49(e) may need work as well.

There was discussion about whether the Committee favored retaining current Rule 49(e), to preserve status quo. Judge Lawson thought there may need to be different treatment for those who are incarcerated and those who are not, and said that his initial proposal was not to preserve status quo.

A member stated he was unprepared to vote on specifics. He did not favor going beyond conveying the Committee's concerns to the other Committee at this point. He specifically did not agree with any rule stating pro se or prisoners may have CM/ECF access.

Judge Lawson agreed with Judge Raggi's suggestion that the committee vote on whether to inform the other committees that the Criminal Rules Committee has reservations about requiring mandatory electronic filing for pro se litigants and pro se criminal litigants, because we predict that almost every district would create an exception.

A member agreed that if a Rules Committee gets out in front of what is happening on the ground in 92 of 94 districts, that's a problem. Now Rule 49 allows local rulemaking, and all districts have local rules that are working well. It doesn't make sense to require the local rules committees in all of these districts to reconvene and do something else.

The resolution of the sense of the Committee was adopted unanimously.

Judge Raggi stated that she would voice these concerns,[3] and our Subcommittee will continue to look at our own rule.

E. Proposed Amendment to Rule 35 (15-CR-A)

In a law review article submitted to the Committee in February, Professor Kevin Bennardo urged that Rule 35 be amended to bar appeal waivers before sentencing. Judge Dever, the chair of

[3] Following the meeting, the reporters and chair conveyed these concerns. The chairs, reporters, and members working on the proposed Civil Rule and parallel changes in the Bankruptcy and Appellate Rules were very responsive to the Advisory Committee's concerns, and a revised version of the proposed Civil Rule excluding persons not represented by counsel was presented to the Advisory Committee on Civil Rules. Representatives of all committees will continue to collaborate as the rules on electronic service, filing, and signature move forward.

the subcommittee that reviewed another recent proposal to amend Rule 35, was asked to comment on Professor Bennardo's proposal.

Judge Dever concluded that the proposal is trying to solve a nonexistent problem by creating a second Rule 11 process that will not save the appellate courts any time. He recommended that the proposal not be referred to a subcommittee and that it not be pursued further. He noted several problems with the assumptions underlying the proposal. First, the circuits uniformly accept waivers of appeal in plea agreements, rejecting one of the article's central premises, namely that there cannot be a knowing waiver of appeal until the sentence is imposed. Second, the article erroneously assumes that judges do not consider the Section 3553(a) factors if there is an appellate waiver. Finally, the proposal is intended to save the appellate courts time, because it assumes that the appeal would be stayed while the government negotiations an appeal waiver after sentencing, after which there would be a new process in the trial court by which the defendant will receive a lower sentence. The article also asserted that this will lead to fewer defendants who breach the appeal waiver by asking their lawyer to file the notice of appeal.

Judge Raggi asked for members to comment. Hearing no comment, she called for a vote on the recommendation not to pursue this further.

The motion not to pursue the proposal passed unanimously.

F. Other Business

Judge Raggi stated that if the Rule 41 changes are adopted, that would be a good time to help the Federal Judicial Center work on a primer on how electronic searches work. She stated that Judge Kethledge, Chair of the Rule 41 Subcommittee, Professor Kerr, the Department of Justice, Mr. Siffert and she would work with the FJC on this project.

Finally, Judge Raggi noted the next meeting of the Committee will be September 28-29 in Seattle, Washington.

The meeting was adjourned.

TAB 2C

THIS PAGE INTENTIONALLY BLANK

PROPOSED AMENDMENTS TO THE FEDERAL RULES OF CRIMINAL PROCEDURE*

Rule 4. Arrest Warrant or Summons on a Complaint

(a) Issuance. If the complaint or one or more affidavits filed with the complaint establish probable cause to believe that an offense has been committed and that the defendant committed it, the judge must issue an arrest warrant to an officer authorized to execute it. At the request of an attorney for the government, the judge must issue a summons, instead of a warrant, to a person authorized to serve it. A judge may issue more than one warrant or summons on the same complaint. If an individual defendant fails to appear in response to a summons, a judge may, and upon request of an attorney for the government must, issue a warrant. If

* New material is underlined in red; matter to be omitted is lined through.

an organizational defendant fails to appear in response to a summons, a judge may take any action authorized by United States law.

* * * * *

(c) Execution or Service, and Return.

(1) ***By Whom.*** Only a marshal or other authorized officer may execute a warrant. Any person authorized to serve a summons in a federal civil action may serve a summons.

(2) ***Location.*** A warrant may be executed, or a summons served, within the jurisdiction of the United States or anywhere else a federal statute authorizes an arrest. A summons to an organization under Rule 4(c)(3)(D) may also be served at a place not within a judicial district of the United States.

(3) ***Manner*****.**

(A) A warrant is executed by arresting the defendant. Upon arrest, an officer possessing the original or a duplicate original warrant must show it to the defendant. If the officer does not possess the warrant, the officer must inform the defendant of the warrant's existence and of the offense charged and, at the defendant's request, must show the original or a duplicate original warrant to the defendant as soon as possible.

(B) A summons is served on an individual defendant:

(i) by delivering a copy to the defendant personally; or

(ii) by leaving a copy at the defendant's residence or usual place of abode with a person of suitable age and discretion residing at that location and by mailing a copy to the defendant's last known address.

(C) A summons is served on an organization in a judicial district of the United States by delivering a copy to an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process. ~~A copy~~If the agent is one authorized by statute and the statute so requires, a copy must also be mailed to the organization~~organization's last known address within the district or to~~

~~its principal place of business elsewhere in the United States~~.

(D) A summons is served on an organization not within a judicial district of the United States:

(i) by delivering a copy, in a manner authorized by the foreign jurisdiction's law, to an officer, to a managing or general agent, or to an agent appointed or legally authorized to receive service of process; or

(ii) by any other means that gives notice, including one that is:

(a) stipulated by the parties;

(b) undertaken by a foreign authority in response to a letter rogatory, a letter of request, or a request

submitted under an applicable international agreement; or

(c) permitted by an applicable international agreement.

* * * * *

Committee Note

Subdivision (a). The amendment addresses a gap in the current rule, which makes no provision for organizational defendants who fail to appear in response to a criminal summons. The amendment explicitly limits the issuance of a warrant to individual defendants who fail to appear, and provides that the judge may take whatever action is authorized by law when an organizational defendant fails to appear. The rule does not attempt to specify the remedial actions a court may take when an organizational defendant fails to appear.

Subdivision (c)(2). The amendment authorizes service of a criminal summons on an organization outside a judicial district of the United States.

Subdivision (c)(3)(C). The amendment makes two changes to subdivision (c)(3)(C) governing service of a summons on an organization. First, like Civil Rule 4(h), the amended provision does not require a separate mailing to the organization when delivery has been made in the United States to an officer or to a managing or general agent. Service of process on an officer, managing, or general agent is in effect service on the principal. Mailing is required when delivery has been made on an agent authorized by statute, if the statute itself requires mailing to the entity.

Second, also like Civil Rule 4(h), the amendment recognizes that service outside the United States requires separate consideration, and it restricts Rule 4(c)(3)(C) and its modified mailing requirement to service on organizations within the United States. Service upon organizations outside the United States is governed by new subdivision (c)(3)(D).

These two modifications of the mailing requirement remove an unnecessary impediment to the initiation of criminal proceedings against organizations that commit domestic offenses but have no place of business or mailing address within the United States. Given the realities of today's global economy, electronic communication, and federal criminal practice, the mailing requirement should not shield a defendant organization when the Rule's core objective—notice of pending criminal proceedings—is accomplished.

Subdivision (c)(3)(D). This new subdivision states that a criminal summons may be served on an

organizational defendant outside the United States and enumerates a non-exhaustive list of permissible means of service that provide notice to that defendant.

Although it is presumed that the enumerated means will provide notice, whether actual notice has been provided may be challenged in an individual case.

Subdivision (c)(3)(D)(i). Subdivision (i) notes that a foreign jurisdiction's law may authorize delivery of a copy of the criminal summons to an officer, to a managing or general agent. This is a permissible means for serving an organization outside of the United States, just as it is for organizations within the United States. The subdivision also recognizes that a foreign jurisdiction's law may provide for service of a criminal summons by delivery to an appointed or legally authorized agent in a manner that provides notice to the entity, and states that this is an acceptable means of service.

Subdivision (c)(3)(D)(ii). Subdivision (ii) provides a non-exhaustive list illustrating other permissible means of giving service on organizations outside the United States, all of which must be carried out in a manner that "gives notice."

Paragraph (a) recognizes that service may be made by a means stipulated by the parties.

Paragraph (b) recognizes that service may be made by the diplomatic methods of letters rogatory and letters of request, and the last clause of the paragraph provides for service under international agreements that obligate the

parties to provide broad measures of assistance, including the service of judicial documents. These include crime-specific multilateral agreements (e.g., the United Nations Convention Against Corruption (UNCAC), S. Treaty Doc. No. 109-6 (2003)), regional agreements (e.g., the Inter-American Convention on Mutual Assistance in Criminal Matters (OAS MLAT), S. Treaty Doc. No. 105-25 (1995)), and bilateral agreements.

Paragraph (c) recognizes that other means of service that provide notice and are permitted by an applicable international agreement are also acceptable when serving organizations outside the United States.

As used in this rule, the phrase "applicable international agreement" refers to an agreement that has been ratified by the United States and the foreign jurisdiction and is in force.

Changes after publication

No changes were made after publication.

THIS PAGE INTENTIONALLY BLANK

Public Comments – Rule 4

CR-2014-0004-0006. Robert Anello, Federal Bar Council (letter). Supports amendment, stating it fairly addresses gaps that currently prevent effective prosecution of foreign corporations that commit crimes in the U.S. but have no physical presence here, provides methods of service that are reasonably calculated to provide notice and comply with applicable laws, and gives courts appropriate discretion to fashion remedies.

CR-2014-0004-0015. Robert Anello, Federal Bar Council (prepared testimony). Supports amendment, stating it fairly addresses gaps that currently prevent effective prosecution of foreign corporations that commit crimes in the U.S. but have no physical presence here, provides methods of service that are reasonably calculated to provide notice and comply with applicable laws, and gives courts appropriate discretion to fashion remedies.

CR-2014-0004-0019. Karen Strombom, Federal Magistrate Judges Association. The FMJA "endorses" the proposed amendment, which addresses a gap in the rules and responds to a growing need in a global economy, but suggests that the committee note expressly state that the means of service must satisfy constitutional due process.

CR-2014-0004-0017. Kyle Druding. Supports amendment, noting that although an amendment is needed to close a gap in the current rule, Due Process concerns require reasonably limited means of service under Rule 4 and the responsible exercise of prosecutorial discretion.

CR-2014-0004-0028. Robert Feldman, Quinn Emanuel Urquhart & Sullivan, LLP. Opposes the amendment, stating that it "could foreclose judicial review at any stage in the process, leaving the supposed validity of service entirely in the hands of the executive"; argues that it will be impossible to challenge service for lack of actual notice, because "the very act of challenging service might be said to conclusively establish the notice that would make service complete"; argues that the system of special appearances "may be effectively eviscerated," placing responsible corporate defendants who wish to contest service with "a Hobson's choice." Also notes that other governments may respond with a similar regime.

CR-2014-0004-0031. Peter Goldberger, National Ass'n of Criminal Defense Lawyers. Supports amendment with several revisions (1) adding clarification to Rule 4(a) that the court's actions must be "consistent with Rule 43(a)"; (2) providing that service within the United States under Rule 4(c)(3)(C) is preferred if likely to give actual notice; and (3) providing that service under Rule 4(c)(3)(D)(i) is preferred over service under (c)(3)(D)(i).

THIS PAGE INTENTIONALLY BLANK

TAB 2D

THIS PAGE INTENTIONALLY BLANK

PROPOSED AMENDMENTS TO THE FEDERAL RULES OF CRIMINAL PROCEDURE*

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

* New material is underlined in red; matter to be omitted is lined through.

information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

* * * * *

(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.

* * * * *

Committee Note

Subdivision (b). 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 requirements for the issuance of a warrant, which must still be met.

Subdivision (b)(6). The amendment provides that in two specific circumstances a magistrate judge in a 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 seize or copy electronically stored information even when that media or information is or may be located outside of the district.

First, subparagraph (b)(6)(A) provides authority to issue a warrant to use remote access within or outside that district when the district in which the media or information is located is not known because of the use of technology such as anonymizing software.

Second, (b)(6)(B) allows a warrant to use remote access within or outside the district in an investigation of a violation of 18 U.S.C. § 1030(a)(5) if the media to be searched are protected computers that have been damaged without authorization, and they are located in many districts. Criminal activity under 18 U.S.C. § 1030(a)(5) (such as the creation and control of "botnets") may target multiple computers in several districts. In investigations of this nature, the amendment would eliminate the burden of attempting to secure multiple warrants in numerous

districts, and allow a single judge to oversee the investigation.

As used in this rule, the terms "protected computer" and "damage" have the meaning provided in 18 U.S.C. §1030(e)(2) & (8).

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.

Subdivision (f)(1)(C). The amendment is intended to ensure that reasonable efforts are made to provide notice of the search, seizure, or copying, as well as a receipt for any information that was seized or copied, to the person whose property was searched or who possessed the information that was seized or copied. Rule 41(f)(3) allows delayed notice only "if the delay is authorized by statute." See 18 U.S.C. § 3103a (authorizing delayed notice in limited circumstances).

Changes after publication

The revised caption including the term "venue" makes clear the limited function of the amendment, which determines only which courts may consider warrant applications, not the standards for the approval of remote electronic search warrants. The notice provision for remote electronic searches was revised to parallel more closely the

notice presently required for physical searches. As revised, the government must provide not only a copy of the warrant but also a receipt for any property seized or copied in a remote search. It must provide notice to either the person whose property was searched or who possessed the information that was seized or copied. The Committee notes were revised to explain these changes, and to draw attention to restrictions on delayed notice in Rule 41(f)(3).

Public Comments Proposed Amendment to Rule 41

CR-2014-0004-0003. Keith Uhl. Raises a question: If a warrant approved in one district is served on a computer in a second district, must the defense travel to the first district to challenge the warrant.

CR-2014-0004-0004. Mr. Anonymity. Opposes the amendment, stating that anonymous speech serves an important constitutional purpose, protecting unpopular people from retaliation; perfect anonymity technology would be widely adopted, facilitating routine communications and financial transactions; attempts to surreptitiously install malware will generate retaliatory responses.

CR-2014-0004-0005. Former Federal Agent. Opposes the amendment, stating many law-abiding people employ anonymizing technology, and the amendment will be read expansively, allowing the government to pierce their anonymity and distribute malware to them.

CR-2014-0004-0006. Robert Anello, Federal Bar Council (letter). Supports the proposal, stating it is "necessary and will be effective in permitting law enforcement to properly investigate crimes involving computers and electronic information"; constitutional questions "can and will be addressed by the courts in due course."

CR-2014-0004-0007. Carolyn Atwell-Davis. Ms. Atwell-Davis, who previously worked for the National Center for Missing & Exploited Children, supports the amendment, stating it provides a necessary and constitutionally valid tool allowing law enforcement to stop the sexual exploitation of children by persons who use technology to evade detection.

CR-2014-0004-0008. Amie Stephanovich, Access and the Electronic Frontier Foundation. Opposes the amendment, stating that allowing a single warrant application for damaged computers in five or more districts would effectively expand investigations of the overbroad Computer Fraud and Abuse Act to victim computers, would give the state access to the personal data of journalists**,** dissidents, whistleblowers, and world leaders, and would subject victims to a wide range of potentially harmful measures that may interfere with the operation of their computers or their communication with other devices.

CR-2014-0004-0009. Joseph Lorenzo Hall, The Center for Democracy & Technology. Opposes the amendment, stating that the proposal "would make policy decisions about important questions of law that are not currently settled and would best be resolved through legislation"; legal issues include the Fourth Amendment particularity requirement and the effect of treaties and international law on extraterritorial searches; policy issues include implications for users of common technology (such as virtual private networks, or VPNs) and the potential for damage to devices, data, or independent systems.

CR-2014-0004-0010. Alan Butler, Electronic Privacy Information Center (epic.org). Opposes the amendment, stating that the proposed amendment "would authorize searches beyond the scope permissible under the Fourth Amendment," by allowing "surreptitious searches without the required showing of necessity," and not requiring that "notice be served within a

reasonable time after the search."

CR-2014-0004-0011. Kevin S. Bankston, New America's Open Technology Institute. Opposes the amendment, stating that "the proposed amendment authorizes searches that are unconstitutional for lack of adequate procedural protections tailored to counter those searches' extreme intrusiveness."

CR-2014-0004-0012. Steven Bellovin, Matt Blaze and Susan Landau. Opposes the amendment as circulated, stating that the proposal raises serious concerns that require further study and perhaps legislative action: the use of malware in botnet investigations may cause unanticipated damage to the victim computers and is indistinguishable from a general search; the amendment authorizes searches of legitimate users of VPNs as well as foreign searches; courts must be better informed regarding search techniques; chain of custody and preservation issues will necessarily arise; notice for remote searches is problematic; and computer vulnerabilities should be disclosed to vendors for corrective action, not withheld to provide a means for remote searches. If the proposal is adopted, significant changes are recommended, including greater specification of the area of the computer that is to be searched, requiring cooperation of the host country for most international searches, more explicit guidance regarding the conditions when notice can be omitted, and reworking of authorization to use malware to investigate victims' computers.

CR-2014-0004-0013. Nathan Wessler, American Civil Liberties Union. Opposes the amendment, stating the proposal "raises myriad technological, policy, and constitutional concerns," and constitutes a "dramatic expansion of investigative power." Argues that the proposal should be authorized only by legislation because the use of zero day malware may constitute an unreasonable search; some searches authorized by the amendment require Title III wiretap orders; authorized searches will violate the particularity requirement and result in searches of individuals for whom there is no probable cause; the notice requirement is insufficient; and the courts will not address and resolve these constitutional issues in the foreseeable future.

CR-2014-0004-0014. Duplicate comment. Withdrawn.

CR-2014-0004-0015. Robert Anello, Federal Bar Council (prepared testimony). Supports the amendment, stating the proposal is "necessary and will be effective in permitting law enforcement to properly investigate crimes involving computers and electronic information"; constitutional questions "can and will be addressed by the courts in due course."

CR-2014-0004-0016. Nathan Wessler, American Civil Liberties Union. Letter of April 4, 2014, "recommends that the Advisory Committee exercise extreme caution before granting the government new authority to remotely search individuals' electronic data," stating that "the proposed amendment would significantly expand the government's authority to conduct searches that raise troubling Fourth Amendment, statutory, and policy questions" for consideration at the Advisory Committee's April 2014 meeting.

CR-2014-0004-0018. Anonymous. Opposes the amendment stating that the government should

not be able to conduct warrantless searches of private computers merely because someone is using a VPN.

CR-2014-0004-0019. Karen Strombom, Federal Magistrate Judges Association (FMJA). The FMJA "endorses" the amendment because it fills a significant gap in authority, noting that the meaning of "remote access" and "reasonable efforts" will be developed as specific cases arise.

CR-2014-0004-0020. Anonymous. Opposes the amendment, stating that the government should not spy on everyone and should mind its own business.

CR-2014-0004-0021. Dan Teshima. Opposes the amendment stating that it will "weaken" the Fourth Amendment.

CR-2014-0004-0022. George Orwell. Opposes the amendment, stating it will allow the government to "hack into our computers for practicing internet privacy," and reflects the view that the "Government must know all, must see all."

CR-2014-0004-0024. Ladar Levison. Opposes the amendment because he believes it permits the issuance of a warrant whenever an individual has used encryption tools that are common, legal, and in some cases industry standards, such as the Payment Card Industry Data Security Standards. Additionally, he states, it "[c]ould be used to legalize the practice of infiltrating service provider networks to ex-filtrate private user data that was previously intercepted as it traveled along trunk lines, but has since been protected by a VPN."

CR-2014-0004-0027. Robert Gay Guthrie/ Bruce Moyer, National Association of Assistant United States Attorneys. Supports the amendment because of "the need to improve Rule 41's territorial venue limitations"; states that increasingly sophisticated technologies pose challenges to law enforcement investigations of offenses such as financial fraud, child pornography, and terrorism, which often require remote electronic searches when sophisticated technology or proxy servers have been used to hide the true IP addresses; supports the change in venue requirements for botnet investigations to avoid wasting judicial and investigative resources and delays.

CR-2014-0004-0029. Richard Salgado, Google Inc. Opposes the amendment; states that it is a substantive expansion of the government's search capabilities that should be left to Congress; asserts that the government cannot seize evidence outside the U.S. pursuant to a search warrant that permits remote access of servers abroad; argues that the amendment "alters constitutional rights and violates the Rules Enabling Act" and "is vague and fails to specify how searches may be conducted and what may be searched"; states that case law addressing the constitutional issues will be slow to develop; contends that proposed (b)(6)(B) would extend beyond botnet searches and reach "millions of computers."

CR-2014-0004-0030; Pennsylvania Bar Association. Opposes the amendment; states that it "substantively expand the government's investigative powers,"conferring authority for "a category of searches that the government is currently barred from conducting"; asserts that these

issues should be addressed by Congress.

CR-2014-0004-0032. Edward Mulcahy. Opposes the amendment; states that "[t]he government's power is already too vast and secret," and asserts that the amendment "would make using a VPN or TOR sufficient evidence of wrongdoing to justify a search warrant."

CR-2014-0004-0033. Kati Anonymous. Opposes the amendment; states that "The government or who ever has no right to enter someone's home without a warrant therefore entering a private space on a citizens electronic devices is also out of the question and without the owners permission or warrant unlawful."

CR-2014-0004-0034. Jeff Cantwell. Opposes the amendment; states that the government may not "spy on" communications "just from the fact that I try to enforce my right to privacy," which he likens to "saying the government has a right to read my mail just because I've sealed the envelope."

CR-2014-0004-0035. Benoit Clement. Opposes the amendment; states that it is "yet again another move to infringe upon the privacy and freedoms of citizens," and "an unfair practice."

CR-2014-0004-0036. Yani Yancey. Opposes the amendment; states that the federal government "funded development of TOR and encourages people to use both it and VPN for legitimate security reasons," but now "seeks to paint their use as criminals and strip away the 4th amendment rights of people without any real suspicion of wrongdoing"; states that "[a]ttempting to safeguard your personal information and online activity is not a criminal or suspicious act."

CR-2014-0004-0037. Jeffrey Adzima. Opposes the amendment; states that it "appears to be in direct conflict with our current Constitutional protections, specifically, amendment 4 against unwarranted search and seizure of private property," which states 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."

CR-2014-0004-0038. Peter Goldberger, National Ass'n of Criminal Defense Lawyers. Opposes the amendment "because it overreaches the authority of judicial branch, which is limited in its rulemaking authority to purely procedural matters – a limitation that calls for particularly sensitive attention in the area of search and seizure – and because it would upset the appropriate balance that must be struck between law enforcement methods and the protection of privacy in a civil society now become digital"; argues that "the rule dismisses the foundational principle that due process has a "place" dimension"; argues that a restriction to the "district where activities related to a crime may have occurred" is too broad and promotes forum shopping; suggests why "reliance on later litigation is not a solution" to the amendment's constitutional infirmities; urges that if the amendment is not rejected, it at least be "revised to ensure that other computers connected to the anonymized computer cannot be within the scope of a warrant specially authorized under Rule 41(b)(6)(A)," and that the warrant be limited to "ascertaining the concealed location" of the media to be searched.

CR-2014-0004-0039. Tadeas Liska. Notes his business routinely uses and accesses VPN's for

data transfer and meeting sessions to provide confidentiality and privacy, and urges that using this technology should not be treated as suspicious activity.

CR-2014-0004-0040. Jonathan Wroblewski, U.S. Department of Justice. Supports amendment; discusses how remote search warrants can satisfy the Fourth Amendment's particularity requirement, describing investigative scenarios and explaining how warrants can be drafted in those scenarios to satisfy the Fourth Amendment; states that amendment "does not modify the delayed-notice statute,"18 U.S.C. § 3103a; explains that there may be unusual difficulty in providing appropriate notice in cases where the district in which the computer is located is unknown, but when government can provide notice using reasonable efforts, it must do so; states that notice requirements are "consistent with Rule 41's existing requirements for both standard search warrants and for tracking device warrants"; states that search warrants do not permit law enforcement to intercept wire, oral, or electronic communications (unless one of several statutory exceptions), and amendment would make no change in relevant law; notes that some commentators misunderstand reference to concealment by technological means, which is the basis for venue but does not by itself provide a basis for a search warrant; argues that Department is committed to balancing risks involved in technical measures against the importance of the objectives of an investigation in stopping crime and protecting public safety," accordingly its remote searches "have not resulted in the types of collateral damage that the commenters hypothesize," and "careful consideration of any future technical measures will continue."

CR-2014-0004-0041. Martin MacKerel. Opposes amendment; states it dramatically expands law enforcement powers and "should be subject to robust public debate in the appropriate legislative forum," rather that the subject of an administrative rule change.

CR-2014-0004-0042. Timothy Doughty. Opposes amendment; argues that it is "the digital equivalent of "your front door is locked, therefore, you're under suspicion of being a criminal," despite the fact that VPNs are widely used for many legitimate purposes; argues the amendment will drive the tech companies out of the U.S.

CR-2014-0004-0043. Stephen Argen. Opposes amendment; argues that it is "an unconstitutional overreaching," noting that many businesses rely on VPN's for encrypted communication to protect trade secrets and journalists using Tor to protect their identities whilst abroad.

CR-2014-0004-0044. Weymar Osborne. Opposes amendment; states that '[u]sing a VPN or some other way is not a sufficient reason to authorize the warrant."

CR-2014-0004-0045. Anonymous Anonymous. Opposes amendment; states that the amendment violates Fourth Amendment prohibitions against unreasonable searches and general warrants; argues that protecting one's privacy does not create probable cause for a search.

CR-2014-0004-0046. Ryan Hodin. Opposes amendment; notes that the U.S. government has funded research into, and supported the use of, TOR and VPNs, which have many legitimate and wholly legal uses; urges that their use is not illegal and does not constitute "probable cause."

CR-2014-0004-0047. Hannah Bloch-Wehba, Reporters Committee for Freedom of the Press. Opposes amendment; argues that it implicates the constitutional and statutory rights of journalists in multiple ways that should be addressed by Congress if they are to be altered.

CR-2014-0004-0048. Cormac Mannion. Opposes amendment; states that technology such as Tor or VPN encryption to engage in private communications is used by many innocent people and should not be treated as misconduct or suspicious behavior.

CR-2014-0004-0049. Raul Duke. Opposes amendment; states it is "an infringement on first, fourth, and fifth amendment grounds, if not illegal in other ways."

CR-2014-0004-0050. Michael Boucher. Opposes amendment; argues that because anyone's computer can become the victim of a botnet, anyone's computer would become "subject to sweeping new surveillance"; contends that common activities such as the use of cloud computing services conceal the location of media or information not be sufficient to obtain a warrant; contends that procedural safeguards for searches under the amendment are far less protective than those applicable to wiretaps, despite the potential for access to intimate personal information and ability to obtain ongoing surveillance by a camera or recording device.

CR-2014-0004-0051. Staff, Clandestine Reporters Working Group, LLC. Opposes amendment; states that it improperly treats "secret" or "hidden" activity as ipso facto "illicit" activity.

CR-2014-0004-0052. Andrew Gordon. Opposes amendment; states that "[t]he use of software and/or hardware readily available to anyone in order to create a more safe and secure online environment should not be grounds for issuing a warrant."

CR-2014-0004-0053. Ahmed Ghappour. Opposes amendment; states that issuance of remote warrants when location is disguised by technological means "will necessarily result in extraterritorial cyber operations"; contends that such extraterritorial operations would be "a radical shift" that "constitutes an enlargement of law enforcement's substantive authority to conduct investigative activities overseas"; if rule is amended, proposes limiting measures: (1) allowing Network Investigative Techniques to return only country information first, prompting the executing FBI agent to utilize the appropriate protocols and institutional devices," (2) requiring a preliminary showing that less intrusive investigative methods have failed or are unlikely to succeed, (3) limiting the range of techniques that are permitted to law enforcement trickery and deception that result in target-initiated access, and (3) limiting search capabilities to monitoring and duplication of data on the target.

CR-2014-0004-0054. Brett Remsen. Opposes amendment in strong general terms.

CR-2014-0004-0055. David Bitkower, U. S. Department of Justice. Supports the amendment. States that it "has no effect on the FBI's authorities outside the United States," and "would not authorize the government to undertake any search or seizure, use any remote search technique, or

restrict any required notice in a manner not already permitted under current law"; notes that "[i]n cases where the Fourth Amendment's warrant requirement applies, the procedures for obtaining a warrant in Rule 41 effectively limit the FBI's ability to conduct searches and seizures"; emphasizes that "the Fourth Amendment's warrant requirement does not apply to searches outside of the United States, even searches of United States persons," which are evaluated under the Fourth Amendment's reasonableness requirement. States that "[n]othing in the proposal changes the government's foreign policy considerations, which are also not governed by Rule 41," but rather are followed by the Department "because they are good policy."

CR-2014-0004-0056. David Bitkower, U. S. Department of Justice. Supports the amendment. States that search warrants authorizing remote searches can satisfy the Fourth Amendment's particularity requirement, and provides sample warrant language for three scenarios to demonstrate how particularity can be established; states proposal, like the present requirement for physical searches, "would require that officers either give notice of the warrant when it is executed or seek judicial approval to delay notice under the procedures of 18 U.S.C. § 3103a"; states that "when investigators seek to conduct surveillance that requires a Title III wiretap order, they will need to obtain such an order, whether or not the proposal is adopted"; explains that "proposed rule would not allow the government to obtain a warrant merely because someone is using anonymization techniques," rather "as with all warrants, the issuing court must find that there is probable cause to search for or seize evidence, fruits, or instrumentalities of crime"; states that "Department is mindful of the potential impact of remote search techniques on computer systems and is careful to avoid collateral damage when executing remote searches."

CR-2014-0004-0057. David Bitkower, U. S. Department of Justice. Supports the amendment. Argues that the Rules Committee is an appropriate forum to address venue for warrant applications; the language of the proposed rule is not vague; the botnet amendment is appropriate; and the proposed amendment does not conflict with the Privacy Protection Act.

THIS PAGE INTENTIONALLY BLANK

Rule 41. Search and Seizure

* * * * *

(b) Authority to Issue a Warrant. 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 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 on the person whose property was searched or whose information was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.

* * * * *

Committee Note

Subdivision (b)(6). The amendment provides that in two specific circumstances a magistrate judge in a 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 seize or copy electronically stored information even when that media or information is or may be located outside of the district.

First, subparagraph (b)(6)(A) provides authority to issue a warrant to use remote access within or outside that district when the district in which the media or information is located is not known because of the use of technology such as anonymizing software.

Second, (b)(6)(B) allows a warrant to use remote access within or outside the district in an investigation of a violation of 18 U.S.C. § 1030(a)(5) if the media to be searched are protected computers that have been damaged without authorization, and they are located in many districts. Criminal activity under 18 U.S.C. § 1030(a)(5) (such as the creation and control of "botnets") may target multiple computers in several districts. In investigations of this nature, the amendment would eliminate the burden of attempting to secure multiple warrants in numerous districts, and allow a single judge to oversee the investigation.

As used in this rule, the terms "protected computer" and "damage" have the meaning provided in 18 U.S.C. §1030(e)(2) & (8).

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.

Subdivision (f)(1)(C). The amendment is intended to ensure that reasonable efforts are made to provide notice

of the search, seizure, or copying to the person whose information was seized or copied or whose property was searched.

THIS PAGE INTENTIONALLY BLANK

TAB 2E

THIS PAGE INTENTIONALLY BLANK

PROPOSED AMENDMENTS TO THE FEDERAL RULES OF CRIMINAL PROCEDURE*

Rule 45. Computing and Extending Time

* * * * *

(c) Additional Time After Certain Kinds of Service. Whenever a party must or may act within a specified time after being served ~~service~~ and service is made under Federal Rule of Civil Procedure 5(b)(2)(C) (mailing), (D) (leaving with the clerk), ~~(E),~~ or (F) (other means consented to), 3 days are added after the period would otherwise expire under subdivision (a).

Committee Note

Subdivision (c). Rule 45(c) and Rule 6(d) of the Federal Rules of Civil Procedure contain parallel provisions providing additional time for actions after certain modes of service, identifying those modes by reference to Civil Rule 5(b)(2). Rule 45(c)—like Civil

* New material is underlined in red; matter to be omitted is lined through.

Rule 6(d)—is amended to remove service by electronic means under Rule 5(b)(2)(E) from the forms of service that allow 3 added days to act after being served. The amendment also adds clarifying parentheticals identifying the forms of service for which 3 days will still be added.

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, electronic service was included in the modes of service that allow 3 added days to act after being served. There were concerns that the transmission might be delayed for some time, and particular concerns that incompatible systems might make it difficult or impossible to open attachments. Those concerns have been substantially alleviated by advances in technology and widespread skill in using electronic transmission.

A parallel reason for allowing the 3 added days was that electronic service was authorized only with the consent of the person to be served. Concerns about the reliability of electronic transmission might have led to refusals of consent; the 3 added days were calculated to alleviate these concerns.

Diminution of the concerns that prompted the decision to allow the 3 added days for electronic transmission is not the only reason for discarding this indulgence. Many rules have been changed to ease the task of computing time by adopting 7-, 14-, 21-, and 28-day periods that allow "day-of-the-week" counting. Adding 3 days at the end complicated the counting, and increased the

occasions for further complication by invoking the provisions that apply when the last day is a Saturday, Sunday, or legal holiday.

Eliminating Rule 5(b) subparagraph (2)(E) from the modes of service that allow 3 added days means that the 3 added days cannot be retained by consenting to service by electronic means. Consent to electronic service in registering for electronic case filing, for example, does not count as consent to service "by any other means of delivery" under subparagraph (F).

Electronic service after business hours, or just before or during a weekend or holiday, may result in a practical reduction in the time available to respond. Extensions of time may be warranted to prevent prejudice.

Changes After Publication

The phrase "Time for Motion Papers" was deleted from the caption as unnecessary, and the phrase "after being served" was substituted for "after service" to parallel the language of Fed. R. Civ. P. 6(d), FRAP 26(c), and Fed. R. Bank. P. 9006(f). Finally, the Committee Note was revised to note that in some circumstances the elimination of the three added days may result in prejudice warranting an extension of time.

THIS PAGE INTENTIONALLY BLANK

Public Comments – Rule 45

CR-2014-0004-0019. Karen Strombom, Federal Magistrate Judges Association. The FMJA "generally endorses the change," but expresses concern that the interplay with existing Civil Rules 5(b)(2)(E) and 5(b)(2)(F) may engender confusion; it suggests eliminating the parentheticals in the proposed rule or revising them to refer to "(F) (other means consented to except electronic service").

CR-2014-0004-0023. Cheryl Siler, Aderant. Suggests the existing language of Rule 45(c) be revised to parallel Fed. R. Civ. P. 6(d), FRAP 26(c) and Fed. R. Bank. P. 9006(f), which require action "within a specified time after being served" or "within a prescribed period after being served." Is concerned practitioners may interpret the current rule to mean the party serving a document as well as the party being served are entitled to 3 extra days.

CR-2014-0004-0030; Pennsylvania Bar Association. Opposes the amendment; states that "the additional three days serves a useful purpose in alleviating the burdens that can arise if a filing is electronically served at extremely inconvenient times."

CR-2014-0004-0031. Peter Goldberger, National Ass'n of Criminal Defense Lawyers. Opposes the amendment; states that eliminating three additional days for response to electronic filing will "provide little if any benefit to the court or the public, while placing additional burdens on busy practitioners"; states that many defense counsel are solo practitioners or in very small firms, with little clerical help, and they may not see their ECF notices the day they are received; also questions change in the caption, suggesting it may lead to confusion.

THIS PAGE INTENTIONALLY BLANK

Rule 45. Computing and Extending Time; Time for Motion Papers

* * * * *

(c) Additional Time After Certain Kinds of Service. Whenever a party must or may act within a specified time after service and service is made under Federal Rule of Civil Procedure 5(b)(2)(C) (mailing), (D) (leaving with the clerk), ~~(E),~~ or (F) (other means consented to), 3 days are added after the period would otherwise expire under subdivision (a).

Committee Note

Subdivision (c). Rule 45(c) and Rule 6(d) of the Federal Rules of Civil Procedure contain parallel provisions providing additional time for actions after certain modes of service, identifying those modes by reference to Civil Rule 5(b)(2). Rule 45(c)—like Civil Rule 6(d)—is amended to remove service by electronic means under Rule 5(b)(2)(E) from the forms of service that allow 3 added days to act after being served. The amendment also adds clarifying parentheticals identifying the forms of service for which 3 days will still be added.

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, electronic service was included in the modes of service that allow 3 added days to act after being served. There were concerns that the transmission might be delayed for some time, and particular concerns that incompatible systems might make it difficult or impossible to open attachments. Those concerns have been substantially alleviated by advances in technology and widespread skill in using electronic transmission.

A parallel reason for allowing the 3 added days was that electronic service was authorized only with the consent of the person to be served. Concerns about the reliability of electronic transmission might have led to refusals of consent; the 3 added days were calculated to alleviate these concerns.

Diminution of the concerns that prompted the decision to allow the 3 added days for electronic transmission is not the only reason for discarding this indulgence. Many rules have been changed to ease the task of computing time by adopting 7-, 14-, 21-, and 28-day periods that allow "day-of-the-week" counting. Adding 3 days at the end complicated the counting, and increased the occasions for further complication by invoking the provisions that apply when the last day is a Saturday, Sunday, or legal holiday.

Eliminating Rule 5(b) subparagraph (2)(E) from the modes of service that allow 3 added days means that the 3

added days cannot be retained by consenting to service by electronic means. Consent to electronic service in registering for electronic case filing, for example, does not count as consent to service "by any other means of delivery" under subparagraph (F).