ADVISORY COMMITTEE ON CRIMINAL RULES
MINUTES
April 7-8, 2014, New Orleans, Louisiana

I. Attendance and Preliminary Matters

The Criminal Rules Advisory Committee ("Committee") met in New Orleans, Louisiana, on April 7-8, 2014. The following persons were in attendance:

Judge Reena Raggi, Chair
Carol A. Brook, Esq.
Judge Morrison C. England, Jr.
Mark Filip, Esq.
Chief Justice David E. Gilbertson
Judge John F. Keenan
Professor Orin S. Kerr
Judge David M. Lawson
Judge Donald W. Molloy
Judge Timothy R. Rice
John S. Siffert, Esq.
Jonathan Wroblewski, Esq.
David A. O'Neil, Assistant Attorney General for the Criminal Division
Professor Sara Sun Beale, Reporter
Professor Nancy J. King, Reporter

Judge Jeffrey S. Sutton, Standing Committee Chair
Professor Daniel R. Coquillette, Standing Committee Reporter
Judge Amy J. St. Eve, Standing Committee Liaison

The following persons were present to support the Committee:

Laural L. Hooper, Esq.
Jonathan C. Rose, Esq.
Benjamin J. Robinson, Esq.(by phone)
Julie Wilson, Esq.

II. CHAIR'S REMARKS AND OPENING BUSINESS

A. Chair's Remarks

Judge Raggi introduced new member Professor Orin S. Kerr, and new Standing Committee Liaison Judge Amy St. Eve.

B. Review and Approval of Minutes of April 2013 Meeting

A motion to approve the minutes of the April 2013 Committee meeting in Durham, North Carolina, having been seconded:

The Committee unanimously approved the April 2013 meeting minutes by voice vote.

C. Proposed Amendments Approved by the Supreme Court for Transmittal to Congress

Judge Sutton reported that the proposed amendments to the following Criminal Rules were approved by the Supreme Court and transmitted to Congress and will take effect on December 1, 2014, unless Congress acts to the contrary:

Rule 5. Initial Appearance
Rule 6. Grand Jury.
Rule 12. Pleadings and Pretrial Motions
Rule 34. Arresting Judgment
Rule 58. Initial Appearance

Judge Sutton thanked the Committee in particular for its cooperative work on Rule 12, as did Judge Raggi.

III. CRIMINAL RULES ACTIONS

A. Proposed Amendments to Rule 4

Judge Raggi asked Judge Lawson, Chair of the Rule 4 Subcommittee, to report on the Subcommittee's proposal to amend Rule 4. The proposal responds to a request by the Department of Justice to address the difficulty posed by the requirement in the current rule that service be mailed to an address within the United States, in cases where a corporate defendant has no such address. The Subcommittee's proposed amendment, Judge Lawson reported, eliminates the requirement of a separate mailing except when specified by statute, notes that required mailings need not be to an address in the judicial district, and provides for service outside the United States by means roughly analogous to the methods authorized under the Civil Rules. The amendment also notes that the court may impose those sanctions authorized by law should a corporate defendant fail to appear.

As to means of service outside the district, the amendment permits service (1) by delivery to an officer, managing or general agent, or other agent legally authorized; (2) by stipulation; (3) undertaken by a foreign authority, using letters rogatory, or under request authorized by international agreement and (4) by any means not prohibited by an international agreement. Judge Lawson noted the Subcommittee rejected alternative language that would have allowed service possibly in violation of the foreign jurisdiction's law if authorized by court order.

Professor Beale added that there was agreement on the Subcommittee that an amendment was needed, noting there was no good policy reason to allow certain foreign corporations to evade service because they chose not to have a mailing address in the United States. The discussion in the Subcommittee had focused on the "other means" of service. The proposed amendment does not involve a court order authorizing such service. It does allow a defendant to raise challenges to adequate notice later.

Judge Raggi added that in rejecting the civil rule's language authorizing other means of service when ordered by the court, the Subcommittee recognized that when a person appears in court, the court generally does not question how the party got there, and considers instead whether there was adequate notice. The Subcommittee decided that it would be best to retain this approach to avoid involving courts in ordering action that might violate another nation's laws.

Judge Raggi solicited comments from members of the Subcommittee.

A Subcommittee member noted that one factor supporting the Subcommittee's decision was that the Department has procedures for approving international service, and he asked if the Department planned to include in its procedures review by a Deputy Attorney General or equivalent, rather than just the Office of International Affairs.

Assistant Attorney General O'Neil responded the Department is committed to providing an appropriate level of approval, given the potential impact on foreign relations, and that the Office of International Affairs would give this much thought and consult with appropriate Departments.

Another Subcommittee member reiterated that the Subcommittee's discussion centered on the catch-all means of service at the end of the proposed amendment.

Assistant Attorney General O'Neil expressed gratitude for the Committee's attention to the issue and stated that it was not a theoretical but a very pressing issue for the Department.

Judge Raggi mentioned that the Subcommittee had also addressed what steps might be

taken if a corporation did not appear after being served. She mentioned that the Department had related that corporations do often appear now to contest service because it is in their interest to do so, as they may be involved in other proceedings. She noted that the Department submitted a memorandum included in the materials in the Agenda Book listing the type of actions that might be taken against a corporation that does not appear, including forfeiture. The proposed amendment includes general language on this point, without specifying any particular remedy.

The Subcommittee's recommendation to approve and forward to the Standing Committee an amendment to Rule 4(a) that would add the word "individual" (specifying that the existing language applies to an individual defendant), and a provision referencing actions in response to an organization's failure to appear was moved and seconded. Discussing the motion, a member expressed support for the proposal, noting that she had experience with one of these cases in which the charges had to be dropped as a result of the corporation's objection to service.

The motion to approve the proposed amendment to Rule 4(a) and transmit it to the Standing Committee passed unanimously.

The Subcommittee's recommendation to approve and forward to the Standing Committee language amending Rule 4(c)(2) to add a sentence "A summons may also be served at a place not within a judicial district of the United States under subdivision (c)(3)(D)" was moved and seconded. Without further discussion,

The motion to approve the proposed amendment to Rule 4(c)(2) and transmit it to the Standing Committee passed unanimously.

Turning to the manner of service, the Subcommittee's recommendation to approve and forward to the Standing Committee language amending Rule 4(c)(3)(C), limiting this subsection to service on organizations in the United States, limiting the mailing requirement to mailings required by statute, and eliminating the mailing requirement to the organization's last known address or place of business within the United States, was moved and seconded. Without further discussion,

The motion to approve the proposed amendment to Rule 4(c)(3)(C) and transmit it to the Standing Committee passed unanimously.

Discussion proceeded on the Subcommittee's recommendation to approve and forward the proposed amendments to Rule 4(c)(3)(D). Judge Sutton questioned why the introductory language to (D)(ii) does not read ". . . that gives notice, and that is not prohibited by an applicable international agreement." Professor King and Subcommittee members responded that the means of service could be prohibited by an applicable international agreement but the parties

could still agree to it. Another member expressed the view that service should never be in violation of a treaty. Judge Raggi noted that a court would have jurisdiction over an individual defendant even if he were kidnapped and brought to court, and here the issue is the appropriate rule for a foreign corporate entity. She asked the Department of Justice to clarify whether there are situations in which the United States has an international agreement with another country, but the other country is not honoring that agreement, or perhaps giving "super protection" to their own corporations beyond what is recognized by international law. She expressed her concern about providing more protection in the rules for corporations than for human beings.

Mr. Wroblewski noted, for example, that sometimes a corporation or organization is state-owned, and the state may not enforce an international agreement that is in place. The proposal recognizes such circumstances may arise, and leaves it to the State Department to determine how to proceed. It is appropriate to put in the rule something that references an applicable international agreement. The proposal also notes that service by other means occurs without prior judicial approval, so that a defendant can later come in and raise concerns or constitutional objections. The proposal also parallels the civil rules, he noted, which have a similar provision, though it requires prior court approval.

Professor Beale stated that the Subcommittee also considered a concern about the Rules Enabling Act: could a rule authorize service contrary to a treaty? The Subcommittee decided that the proposed language struck the appropriate balance, by listing any other means consistent with an applicable agreement, recognizing the Department's position that a treaty might have been abrogated, and not precluding later arguments by defendants. It recognizes that a court would not have to bless such service in advance when it would not have heard arguments by both sides.

A member stated that the Subcommittee did not want the rule to effectively authorize the Department to ignore applicable treaties. Another member noted that the word "applicable" allowed the Executive Branch to determine whether the treaty was applicable in the circumstances, or whether it had been abrogated by conduct. Judge Raggi added that the Subcommittee wanted to avoid providing a basis for a defendant to come to court and invoke a treaty and say you haven't served me correctly, noting that the Supreme Court has already expressed concern about Rules of Criminal Procedure giving rights to defendants under foreign treaties.

Judge Sutton pointed out that the list of possible means of service started with "including" so it was already a non-exclusive list.

When Professor Coquillette asked the Department if this proposal had been vetted with the State Department, Mr. Wroblewski indicated that they had many discussions with colleagues

in the Executive Branch. The Department also provided written assurance relating this consultation to the Subcommittee. Those consulted are comfortable with the process. He explained that the United States Attorneys' Manual already provides that whenever prosecutorial steps may implicate foreign policy, such as a foreign deposition, attorneys must consult with the Office of International Affairs.

Discussion turned to the proposed language in (D)(ii)(a) regarding stipulated means of service. Judge Lawson suggested that the word "stipulation" is generally interpreted to be a more formal agreement in writing, and that the style change to the verb "stipulate" may not carry that meaning. Professor Beale noted that the reporters' research found that the noun "stipulation" and the verb "to stipulate," along with the term "agreement," were used throughout the Federal Rules, and do not always signify that writing is required. If the Committee wished to limit the stipulation to a written record, perhaps the words "in writing" should be added. A member suggested that counsel will agree, and that this will not be an issue. Discussion continued on whether either a corporation or the court would benefit if a written stipulation were required. Judge Raggi noted that this could come up if the corporation is not there as well as when the corporation appears.

Without resolving the concern raised about the language referring to stipulated means of service, the discussion returned to the structure of proposed (D)(ii). A member suggested that in response to Judge Sutton's remarks, the proposal be rewritten to require both notice and compliance with international agreement, but also permit the stipulation to trump the international agreement. Another member suggested making notice and applicable international agreement into a catch all. A third member asked for and received clarification that the parties referenced in the stipulation language are the Department of Justice and the indicted defendant.

Judge Raggi postponed further consideration of the proposal until the Subcommittee had a chance to work on new language.

B. Proposed Amendments to Rule 41

Judge Raggi asked Judge Keenan, Chair of the Rule 41 Subcommittee, to introduce the proposal to amend Rule 41. She noted that the Committee had received a detailed memo from the ACLU, which had been distributed by email prior to the meeting.

Judge Keenan explained that this proposal was also initiated by the Justice Department, and involved two aspects of Rule 41: the territorial requirement and the notice requirement. The Subcommittee considered several versions. The revised version it was recommending to the Committee, after styling, was dated April 3. It was circulated before the meeting and was not in

the agenda book. The proposal would amend the Rule 41 to add new subdivision (b)(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.

This amendment would authorize a magistrate to issue a warrant to search allowing officers to remotely search and seize information on a computer, even if that computer is located outside the magistrate's district, so long as criminal activity has occurred within that district. Rule 41 generally limits warrants to searches and seizures within the district, but it already provides authority for a judge to issue a warrant for a search or seizure outside the district in four other situations, including the use of tracking devices. The amendment seeks only to refine the territorial limits; it does not alter the constitutional constraints, such as the particularity requirement. Any constitutional restriction should be addressed by each magistrate with each warrant request.

As to the notice requirement, Judge Keenan continued, the proposed amendment reads:

> 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 it 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.

This amendment would clarify that officers must make reasonable efforts to provide notification of the search or seizure.

Judge Keenan reported that the Subcommittee held four telephone conferences and considered several memoranda, which are included in the agenda book. The materials also include sample warrants. In the fourth conference call, the Subcommittee approved the version of the proposed amendment that was identical to the version before the Committee, except for a few style changes. Judge Keenan noted that Judge Kethledge, who could not be at this meeting, served as a member of the Subcommittee, had indicated approval of the proposal, and that one member dissented from the Subcommittee's proposed amendment. Finally, he recognized that some Committee members may not have had time to read and analyze the memorandum from the American Civil Liberties Union.

Judge Raggi asked the Department of Justice to speak to the proposal.

Assistant Attorney General O'Neil said the proposal is meant to address three scenarios. The first is to provide authority for a magistrate to issue a warrant to search with remote access for the location of a computer whose location is unknown, possibly in another district. The second is to provide authority for a judge to issue a warrant to search multiple computers in known locations outside the district. The third is to provide authority for a judge to issue a warrant to conduct a remote access search in a district outside the district where the warrant is being sought, as an ancillary request to a physical search request.

Assistant Attorney General O'Neil emphasized that the proposal does not provide authority for the government to conduct any new kind of search or to use any new tools. It does not change anything about the substantive standards that the government must satisfy in order to obtain a warrant or address the substantive requirements of particularity or probable cause. All it does, he explained, is address the venue question–the question of which judge can issue a warrant that, as the law develops, the Fourth Amendment allows.

Assistant Attorney General O'Neil spoke to two concerns raised by the proposal. As to forum or judge shopping, he said that the same concern was raised by the Electronic Communications Privacy Act (ECPA), which already allows a judge in one district to issue a warrant in another district. Congress nevertheless approved this scheme, and the Department was not aware of any complaints about this problem under the ECPA. The second concern he noted was that the proposal could be used to circumvent ECPA or as an alternative means that is less protective than ECPA. The Department did not think that was a problem. The same standards of particularity and probable cause apply to both ECPA and warrants under the proposed Rule 41 remote access searches. Also, prosecutors can already obtain warrants for remote access searches under the present rule. The only question is whether the judge who is most familiar with the facts of an investigation can issue a warrant for information stored outside that judge's district.

Mr. Wroblewski stated that when investigators don't know where the computer is, it is very important to be able to learn that information. He recognized that the ACLU has argued that there ought to be oversight of the code that the government uses to do this, that there ought to be more transparency, and that the code has potential to do harm. The Department recognizes those concerns, he explained, but this Committee is not the place to address them. Some of the issues are Constitutional and will be addressed by magistrate judges one warrant at a time. Some of them will ultimately be addressed by Congress in determining what is and is not permissible. What this proposal tries to address are the three practical realities summarized earlier and in the memos included in the materials.

On the first of those scenarios, Mr. Wrobleski continued, there was agreement in the Subcommittee there should be a rule change. The ACLU also suggested that the second scenario involving the botnets should be addressed and that the government should take steps to respond to this important practical reality. Their concern was the proposal would change practice beyond these two particular circumstances, he said, and the Department disagrees.

Mr. Wroblewski stated that there have been concerns that the Department might use a search warrant issued pursuant to the proposed amendment to secretly search for information, rather than proceeding pursuant to ECPA. That won't happen, he argued, because the Department needs to cooperate constantly with the internet service providers. It will be the rare circumstance, he argued, where agents would get a search warrant rather than an ECPA warrant, possibly in a case involving a business, when a stored communications site is open and available, or when the government already has the credentials to obtain access. The proposal seeks the authority the government already has under ECPA to go to the magistrate judge in the district where the crime is being investigated and ask for a warrant. It only identifies the magistrate who can consider the warrant application. There is a practical enforcement problem on the ground that needs to be addressed, he concluded, and the proposed amendment will address it.

Judge Keenan added that the proposal will also allow a magistrate to issue a warrant that would authorize investigators to search computers in several districts simultaneously.

Judge Raggi observed that the Subcommittee at times used the word "hacking" to discuss remote access searches. To the extent it suggests illegality, it is unfortunate, because the proposal is talking about what judges would authorize. She also noted that the Subcommittee's discussion considered concerns about the government's satisfaction of its Fourth Amendment requirements wherever these warrants were sought, whether under the present rule or under an expanded venue rule. That's why the Committee Note says the proposal is not intended to in any way affect the government's obligations under the Fourth Amendment.

Experts joined some of the Subcommittee's phone conferences to try to explain these remote access searches, she said, and judges would have to be educated about what to ask when the government seeks these warrants. She said she spoke to the Federal Judicial Center about possibly providing judges with more relevant information. For example, to the extent that these searches would involve transmittals, should the judge be asking about Title III? She reiterated that these concerns are with us now already under the present rule, and the question before the Committee is whether to expand the venue and change the notice requirement.

One member raised various concerns with the proposal, noting that he opposed the current version because it is far broader than the reasons that have been proposed to justify it. The first scenario, when the location of a computer is not known, is the strongest case the government has for a change in the rule because the alternative is that the government may not

be allowed to obtain any warrant. Warrants to obtain information from computers of unknown location have been obtained, he stated, so it may be premature to conclude from a single magistrate judge's opinion rejecting this authority that the government cannot obtain such a warrant under the existing rule. But accepting that one opinion as correct, he thought there is a very good case for changing the rule to address this problem.

The second scenario, the member continued, involves sending many communications to computers around the world that are infected as part of a botnet, remotely taken over by hackers. There could be thousands of these affected computers. The warrant applications provided to the Subcommittee authorize obtaining limited information from those computers affected by that botnet and then sending it back to the government. But as far as he is aware there has never been a judicial opinion stating that a warrant is required in that situation. There may be no reasonable expectation of privacy in this information or the government may argue that reason for the search is to protect the victim-owner of the infected device. Accordingly there are various exceptions that might authorize obtaining this information without a warrant. It is premature to act on the assumption that a warrant is required, he argued.

The third scenario is when the government executes a warrant at one place, and then finds there are servers elsewhere with information relevant to the investigation. The member said it would be helpful to have precedent on how Rule 41 applies to this situation before amending the rule. This same concern arises with physical searches, he said, so it is not clear why an amendment is needed for on-line searches and not physical searches. For example, if the government searches a business and discovers there is a warehouse in another district where more records are stored off site, the government would ordinarily go to the other district and obtain a second warrant to search the warehouse. Why shouldn't the venue requirements for Rule 41 should be eliminated for all such searches, so that the first warrant would support the second search as well? The arguments for and against the venue requirements are the same off-line as online, so it is not clear why Rule 41 should authorize the second search under one warrant in the online setting but not in the physical setting.

Finally, he said he feared that the language as drafted has much broader implications than these three scenarios. On its face the draft allows remote access for all searches. Even if the government does not plan on using these more broadly, he warned, it could. The government might get a warrant, he suggested, to search a person's physical places and virtual places all at once. The drafted language would seem to allow that dramatic shift in practice. He noted that the Department said it has no intent to engage in that practice, but he stated his preference for a version of the rule that on its face does not appear to authorize that possibility. He recognized that the Justice Department has a good relationship with major providers now, but that ten years from now it is difficult to know how the rule might be used.

The member explained that there are narrower options to respond to this problem. One would be allowing case law to develop to see if the current rule will be interpreted to allow the practices the government is seeking, or if the Fourth Amendment requires warrants in all of these situations. Another option would be to propose language that would address the unknown location problem. A slightly broader version of that would be to say if data is in multiple districts, a warrant could be issued to reach that.

The member concluded by raising a concern about the proposed language defining the district in which the warrant could be sought: "where activity related to a crime may occur." This phrase is used earlier in Rule 41, but if it is an effort to identify where there would be venue, the venue in computer crimes cases is tremendously uncertain. He mentioned a case in which the government is asserting that there is effectively universal venue for computer-related crime. He was concerned about using a phrase with an unknown meaning.

Judge Keenan noted that the key aspects of the proposal are contained in the memo from the Department on p. 261 of the agenda book, dated March 5, stating the three scenarios. He asked that if there is agreement on scenario number one, perhaps the Committee could move to scenario number two. He asked the Department to explain why an amendment was needed to address scenario number two.

Mr. Wroblewski responded, stating that he agreed that it is possible courts will decide no warrant is required for scenarios one or two, but the Department thinks the better practice is to get the warrants.

Responding to concern about changing the venue rule for online searches but not physical searches, Mr. Wroblewski noted that Congress has already recognized this in several different aspects, including ECPA. Congress already authorized one judge to issue a warrant in one district for searches for electronic information in another district. There are valid concerns about particularity and universal venue, and how many locations can be identified in a particular warrant, but they aren't something this amendment will impact. All this amendment will determine is which judge can be asked to issue the warrant.

Assistant Attorney General O'Neil added that a botnet (which he defined as a collection of computers infected by the same malware, remotely controlled and commanded by a criminal) will usually affect computers in all 94 districts. The question is whether one prosecutor investigating the case can get a warrant from one judge rather than many going to judges in 94 different districts. On scenario three, he said, the fundamental difference between physical searches and searches for electronic evidence is that electronic information can be destroyed instantaneously. If investigators are conducting a search in one district and want to obtain electronic evidence, they need to do that without going all the way to a district on the other side

of the country, educating the judge, and obtaining the warrant, he explained. By the time they could do that the digital evidence may be destroyed.

Another member expressed gratitude for all of the work that has been done and sympathy for the Justice Department's need to disable botnets, which are used to commit crimes and attack businesses by disrupting service. He took the Department's representations about their intent to use this authority sparingly at good faith, but remained troubled by some of the concerns raised by the ACLU. He suggested that Congress will be interested in the resolution of these issues, which reminded him of the controversy about the Justice Department's practice in the attorney client privilege area. He noted some of the ACLU's concerns (such as judge shopping) were not troubling or were far afield from the Committee's work. But there is the possibility that the authority in Rule 41 will be transformed over time to do things that are not intended. He supported the proposal because it is important to get public comment to confirm whether a limited fix is possible, and the Committee can't wait several years.

Another member expressed his agreement that the proposal is modest. He stated that he was surprised at the suggestion that the rule should not be amended because scenarios two and three may not even require a warrant. In his view, anytime judicial review of searches and seizures can be encouraged that is a good thing. He was concerned about the risk of doing nothing given the reality that computers are how people do business and communicate on the most basic levels. He said this amendment addresses a venue question and a notice issue, it has been unfairly demonized, and a lot of red herrings have been thrown into the debate.

Judge Keenan moved to approve the Subcommittee's recommendation to forward the proposed amendment to Rule 41 to the Standing Committee, the motion was seconded, and discussion on the motion continued.

A member expressed appreciation for the importance of the issue and the work that has been done, but she argued that the proposal was premature and she expressed strong opposition to adopting any amendment. Noting that the Committee has identified only one relevant judicial opinion, she suggested waiting a year or two. Also, she argued, the proposal is too broad, with ramifications that can't be anticipated. She observed that the Committee has been asked to wait on the Rule 53 tweeting proposal to allow more information to develop, but stated that she found the need for more information and law to develop is even more acute in the Rule 41 context. Finally, the member believed the proposal will make what is now the exception–ECPA– into the rule. If Congress wants that to be the rule, it should make it the rule. Congress is the appropriate forum for resolving these conflicting concerns.

Judge Raggi asked the member to specify where the proposal is too broad. The member explained that whatever is intended when something is passed, it almost inevitably gets bigger and bigger and bigger over time. The government may choose a judge far away making it

difficult to defend, and they'll be allowed to pick in a way they can't now, because the "may have occurred language" is very broad.

Another member said he was in favor of seeking public comments now. He explained there is not likely to be more case law developing, because notices of searches aren't given right way when there is ongoing criminal activity, and once it is unsealed the issue is seldom whether there was probable cause. He noted that the government already gets to choose where to bring the case even if it is inconvenient for the defendant. He explained that concerns about privacy are understandable, but that shouldn't matter when the government can show that there is probable cause to believe there is evidence of a crime at a particular place. He also didn't see how the right of a second person on a shared site could cause the government to lose its rights to search a computer when it had probable cause for the search. A valid warrant to search a home is not defeated if one of the owners objects. Although he has confidence in the current administration's good will, we would be giving them a tool that we don't entirely understand, with a standard that is not explained. Judges may not know what questions to ask. If there was a way to publish a rule to seek comment but not a rule we approve, that would be good.

Another member asked the Department if it was really having problems with this. He noted a case in which the destruction of electronic evidence occurred but investigators were able to find a copy of the information from a foreign source. The member also expressed concern that the proposed changes to the territorial authority of magistrates were substance not merely procedure.

Mr. Wroblewski responded that use of anonymizing sites, which transmit information disguising the real addresses, is increasing. The government cannot trace the source without the authority to send something back through the anonymizing site. This is a real problem. He explained that it might be possible to litigate and hope the courts will create an exception to a rule that on its face does not work with these realities. But the better approach is to come to the Committee and change the rule that is creating the issue.

Another member explained that he was opposed to the proposal because it introduced a concept not before mentioned in the rules, that is, using remote access to search electronic media. He said the proposal untethers the venue provision, the former limiting principle governing searches, without replacing it with another principle. This idea is similar conceptually to the problem that arose after the Supreme Court's *Katz* decision, which eventually spawned Title III. Congress should address this problem. Maybe Article III judges should have the authority to approve remote access searches, and there are other issues that the Committee cannot address. Releasing an amendment for comment does not solve the problem. The process authorized by the amendment is complex, raises genuine issues of privacy, and is largely ex parte, without the advantage of adversarial argument. Limits have to be firmly in place before authority is granted, and even a focused rule poses the risk of unintended consequences.

Judge Raggi remarked that the limiting principle under both the old and proposed rule is the probable cause requirement, and a venue change won't leave Rule 41 with no limiting principle. If the overlap with Title III became a sticking point, we could add language to the Committee Note that the Committee is not expressing any view as to Title III as well as the Constitution.

Judge Raggi asked if the reporters would comment.

Professor Beale spoke to the comparison of the Rule 41 and Rule 53 proposals earlier in the discussion. She argued that the proposals are very different and can be distinguished. She stated Rule 41 appears to be a much more serious problem than Rule 53, and is a problem that is caused by the language of the rule. The government is reporting that they are being hampered or at least there is uncertainty about investigations in an important and growing class of cases because of language in Rule 41, while the Rule 53 proposal is based on reporters who want to tweet from the courtroom. The need for us to figure out whether reporters can tweet from the courtroom is on a different scale than whether the government can get access when anonymizing software is used, and where botnets are used in attacks. The present Rule 41 creates the problem, at least scenario one.

Second, she responded to the concern that changing the territorial restriction on magistrate warrant authority might violate the Rules Enabling Act. She noted that Rule 41(b) already contains other narrow exceptions to the territorial authority to issue warrants, and concluded this aspect of the proposal is not a substantive change that would violate the Act.

Third, she noted that there seemed to be agreement that scenario one is a problem, caused by the text of the rule. For scenario two, the Committee has always preferred that a warrant be sought. On scenario three, it does not seem premature to start the three-year rules amendment process now, she concluded.

Professor King agreed with Professor Beale and added that in her view the Committee should not forward a proposed rule to the Standing Committee for publication simply to generate public comment, there needs to be some consensus behind an amendment in order to send it on.

Judge Raggi asked Judge Sutton to comment generally on the rule-making process. Judge Sutton explained that if the Committee cannot agree on all aspects of a proposal, but can agree on some of it, one option would be to limit the proposed amendment to the part the Committee endorses, and ask questions for comment about other aspects on which there is no agreement. When the Civil Rules Committee sent out Rule 37, they were unanimous about some aspects, but they weren't sure about others. So they put five questions at the end of the proposal to try to focus public comments on these issues.

Judge Raggi reminded members that if the Committee were to approve a proposed amendment at the meeting, even if everything goes smoothly, it will be a three-year process. She suggested taking the package apart to attempt to identify where there was agreement and where there wasn't.

Turning to the situation in which the government doesn't know where the computer is, she said that declining to modify the rule leaves the government without a way to get a warrant. One issue is whether the rules should require the government to make a showing that they don't know where the computer is. One member suggested that the proposal require such a showing, while the government sees this as an undue burden.

Judge Raggi asked the Department to comment its opposition to a preliminary showing. Mr. Wroblewski indicated that the Department is concerned that depending upon how it is crafted this requirement could lead to litigation over how much the government knew or could learn, but he noted that it might be possible to draft language that referred to the type of technology.

Judge Raggi asked for an explanation of the rationale for requiring a preliminary showing. A member said that adding language that "the location cannot reasonably be ascertained" would respond to Magistrate Smith's opinion, and would operate like other judicial assessments that a judge makes in the warrant process, none of which form the basis for later litigation. It is not a constitutional argument so there could be no basis for suppression, nor is suppression a remedy for violation of the rule.

Another member pointed out that there are limited resources the government can use to track down the location of a computer that had been disguised by anonymizing software. If there is a showing required, it should be clear that the NSA and CIA need not get involved. The entire federal government shouldn't have to gear up to prove this for each warrant.

Mr. Wroblewski commented that language that does not turn on the government's knowledge but rather on the type of technology used would avoid these concerns. Assistant Attorney General O'Neil suggested that something like "an investigation involving the use of technological means to conceal identity" might work.

A member asked those supporting a preliminary showing why this would be unlike Title III, where the failure to comply with procedural requirements forms the basis for defense litigation. A member favoring a preliminary showing responded that this assessment would be the same as other judicial assessments under the current rule concerning the property's location, which are not currently litigated because suppression is not a remedy for violations of the rule.

A member expressed continuing concern that a rule is not the correct means of authorizing remote access to electronic storage media. Does it authorize eavesdropping on digital communications? The seizure of intellectual property that is already in existence?

Judge Raggi asked the Department to explain why remote access searches do not fall under Title III. Mr. Wroblewski responded that remote access searches are happening under the rule now, and the amendment concerns only the venue for judicial approval. Rule 41(e)(2)(b), the provision governing warrants seeking electronically stored information, authorizes the seizure of electronic storage media *or* the seizure or copying of electronically stored information. He emphasized that warrants under Rule 41(e)(2) do not authorize the interception of communications, but rather the search and then seizure or copying of previously stored information. Assistant Attorney General O'Neil agreed that the Department is already using remote access searches to seize or copy electronically stored information.

There was further general discussion of remote electronic searches and Title III. A member commented that the means authorizing remote access ought to be prescribed by legislation like Title III, rather than the Rules process. Judge Keenan suggested that something could be added to the Committee Note indicating that there is no intent to affect the limitations imposed by Title III. The first member agreed, offering that the Note could say that the amendment authorizes no more than what is already authorized by Rule 41(e)(2)(b).

Judge Raggi asked for discussion of any concerns about the language defining the district in which a warrant could be sought: "where activities related to a crime that may have occurred." A member expressed concern about the breadth of the language, though she agreed the Committee should not wait to address scenario one. She asked how the government would know where activities related to the crime may have occurred.

Mr. Wroblewski responded with an example that was included in the agenda book. In that case, someone made a threat against a building in Philadelphia. No one knew where the perpetrator was, only the victim's location was known, because the perpetrator was using anonymizing software.

The reporters pointed out that the language in question is already in Rule 41 in the other exceptions to the venue limitation, i.e., Rule 41(b)(3) and (5). Professor Beale noted that departing from that language would generate questions about why this exception is different than the others.

Mr. Wroblewski observed that there are other possible ways to express this idea. ECPA § 2703 refers to "a court with jurisdiction over the offense under investigation," and the concept is the same. A member offered that he had looked for judicial precedent explaining or interpreting the language in question and couldn't find any.

Judge Raggi adjourned the meeting for lunch.

After lunch, Judge Raggi noted that discussion among the members suggested that agreement might be reached on language tailored to meet the problem of anonymizing software, though the Department of Justice needed time to consult its experts about appropriate language. Accordingly, further discussion on that issue would be deferred until Friday.

Discussion then focused on the second scenario, the botnet investigation, in which the Department seeks authority to get a single warrant rather than separate warrants in many districts. Judge Raggi asked members what concerns this part of the proposal raised.

A member stated that if courts have ruled that a warrant is required in this scenario and also that such warrants are permitted, then it makes sense as a matter of policy to allow a single warrant to be issued in one district. He asked if the Department knew of any instances in which the application for such a warrant in one district had been denied. Mr. Wroblewski responded that he was not aware of such a denial. The member who raised the issue commented that perhaps an amendment is not yet needed.

Judge Raggi noted that the Committee was aware of concerns about the need to require probable cause and particularity to protect privacy interests, and she emphasized that the rule does not address these constitutional considerations. She asked the Committee to focus on the question whether in principle the venue requirements for warrant applications should be amended in the specific situations where technology has been used to disguise the district and there are multiple computers in many districts, as in the case of a botnet investigation.

A member asked whether the government is seeking to disable malware in a botnet investigation, and, if so, what is it "searching" for. Mr. Wroblewski responded that the government may seek to disable malware inserted on many victim computers, but it may also search for and copy information, such as the IP address, from the victim computers. In response to the question whether a warrant is needed to remediate by removing malware, Mr. Wroblewski stated that this is an open question. The Department would like to be able to obtain warrants in these cases and to act under the supervision of the courts. He noted that the ACLU says that such remediation does raise Fourth Amendment concerns, though these interests are not as heightened as they would be if the government were seeking evidence of a crime.

Professor Beale noted that the current draft refers to the authority to issue a warrant to search, seize, and copy; it does not mention remediation. Mr. Wroblewski agreed.

Mr. Wroblewski then described the third scenario, where the government conducts a physical search of a business, the computers are on, and it finds that some files are stored in the cloud on a server in a different district. Because the machines are on and access is available at

the moment, the government wants to be able to get the files by remote access from the cloud. Under ECPA, in contrast, the government must go back to the district court, and then obtain and serve an ECPA warrant on the provider. The proposal here is in limited circumstances to continue the search on site and access the data remotely and directly.

Discussion then turned to the relationship between the proposal and ECPA. Concerns have been expressed that allowing a remote search in the government's third scenario would permit evasion of ECPA and also effectively reduce the probable cause requirement.

Mr. Wroblewski argued that in some circumstances it is important not to delay the search of material stored remotely on the cloud, because it can be destroyed or encrypted if there is a delay. He also noted that within the Department there is a debate about whether ECPA already permits the procedure the government recommends. As the ACLU has argued, ECPA itself allows law enforcement to send a preservation request immediately. Mr. Wroblewski stated that this procedure is not always practical. The ECPA process is not instantaneous, and there can be delay in getting a provider to preserve. Accordingly, the government is seeking the authority to immediately access and copy the electronically stored information to prevent its destruction.

A member observed that if there were reasonable grounds to believe a third party would delete the information from a cloud there are exigent circumstances and no warrant would be required. Thus the proposed amendment seems to be addressed to cases in which such a showing could not be made in advance, but the government fears that destruction might occur during the process of seeking an ECPA warrant.

Another member noted that as a practical matter there has to be probable cause to search the second server on which the material in the cloud is actually being stored. Members discussed the question whether that means a second warrant is constitutionally required. Mr. Wroblewski stated that of course probable cause is required for any search or seizure, and this does not change when there are computers in more than one district. The main point for the government, he emphasized, is to be able to get the initial warrant and any subsequent related warrant from a single judge.

Judge Raggi noted that if the government is authorized to extend its search from the physical computer to information stored on a server based in another district it will still have to satisfy the probable cause and particularity requirements. Many warrants now allow a search of more than one location. Similarly, a court might conclude that probable cause had been shown to search one computer and others linked to it as to which probable cause had also been shown. But all seem to agree that the government must show probable cause and meet the particularity requirement for any search of a new device. A member responded that the case law is fluid on the application of the particularity requirement, in some cases allowing a search of all laptops or desktop computers in person X's home.

Another member observed that the third scenario was the most difficult part of the current proposal. Because of the increasing use of cloud computing, we no longer have separate devices that are analogous to individual locked chests.

Mr. Wroblewski noted that from the government's perspective the problem is that when its investigators remove the storage media (computers) they leave the people behind, and those people can go to a different computer and quickly access and destroy or encrypt any information stored elsewhere. Information stored on the cloud is simply stored in another computer, which is often located in a different judicial district. What the government seeks is the authority to go back to the same magistrate judge, who is familiar with the facts, if it needs an second warrant.

Judge Raggi noted that the Committee Note could even more strongly emphasize that the proposed amendment is addressed only to venue, and not to probable cause or particularity. Professor Coquillette agreed that committee notes can properly be used to emphasize the limited nature of an amendment in order to prevent courts from reading in something that is not there.

These issues were referred back to the Subcommittee with the request that it report back to the Committee later in the meeting.

C. Further Discussion of Proposed Amendments to Rule 4

Judge Raggi asked the Committee to return to the issues raised by Rule 4.

The Rule 4 Subcommittee presented two alternative approaches to proposed Rule 4(c)(3)(D)(ii). The first would shorten the text of the rule by moving the illustrative list of means of service to the Committee Note. The text would refer only to "any other means that gives notice." The second alternative would retain the illustrative list of means of service but rephrase the last, about which Judge Sutton had raised questions. Rather than using a double negative, it would recognize service by a means "permitted by an applicable international agreement."

Subcommittee members spoke in favor of each version. One member stated that he preferred the second option because the rule itself (not merely the note) should give guidance, and inclusion in the text implicitly states the listed means of service are good (if not the only) ways to proceed. This would encourage prosecutors to employ the listed means, and their inclusion would also signal our adherence to the rule of law. He later referred to this as a matter of "optics," urging we are best served by rules that clearly emphasize compliance with international processes and laws. Speaking for the Department of Justice, Mr. Wroblewski disagreed. Illustrations belong in a note, not the rule, and putting them into the text suggests that the list is not merely illustrative. If any means that give notice are permitted, then the text of the rule should not hint otherwise.

Judge Raggi observed that in the case of corporate prosecutions there are special concerns about collateral consequences if the corporation fails to appear. No one suggests that any defendant (human or corporate) can be prosecuted without appearing before the court. The cases involving individual defendants hold that the courts' jurisdiction is not affected by the means used to bring an individual before the court, and she is reluctant to think that a corporate defendant should have more due process rights than an individual. On the other hand, the government might someday seek to forfeit the assets of a foreign corporation that it says received sufficient notice but did not appear. This raises the question whether we should be satisfied if the government can act in such a case without complying with U.S. treaty obligations.

Discussion turned to what other means of service the government might use. Mr. Wroblewski suggested, for example, that the government might use electronic service, or it might be able to serve a person with a strong relationship to the entity when that person was present in a third country.

Professor Beale noted that as a matter of logic there is no difference between the two versions. But professors often see students read in more than is there in language, and courts and litigants may do the same. Here, the intuition is that enumeration may slightly constrain how the rule would be applied and interpreted. A member noted that the Subcommittee had discussed whether there was any priority or need to exhaust the listed means, and he wondered if the option enumerating certain means of service might suggest that.

Professor King took up the question how the proposal compares to the Civil Rule. On the one hand, the proposed amendment expressly requires that any means of service must give notice. This feature is absent from the residual clause of the Civil Rule. On the other hand, the residual clause in the Civil Rule requires that the court approve service by other means in advance, a requirement that the Subcommittee had considered and rejected.

After brief expressions of support for the second alternative, Judge Raggi asked for a motion. Judge Rice moved that the Committee approve the second alternative for amending Rule 4(c)(3)(D)(ii), containing the non-exhaustive list of means by which service can be made.

The motion to was seconded and it passed unanimously.

Judge Lawson then moved that the Subcommittee's proposal, as amended, be transmitted to the Standing Committee with the recommendation that it be published for public comment.'

The motion to transmit the revised proposal to amend Rule 4 to the Standing Committee with the recommendation that it be published passed unanimously.

Judge Sutton complimented the Committee on its work on the proposed amendment.

D. Proposal to Study an Amendment to Rule 53

Judge Raggi then asked Judge England to present the recommendation of the Rule 53 Subcommittee, which he chaired. Judge England explained that as originally adopted Rule 53 banned "radio broadcasting" of judicial proceedings from the courtroom, but in the restyling of the Criminal Rules this was shortened to "broadcasting." In one case brought to the Subcommittee's attention a magistrate judge concluded that the term broadcasting includes Twitter, and accordingly he denied a reporter's request to Tweet from the courtroom. Tweets are limited to 140 characters, and they are a live method of providing information. The reporter sought to use this method to provide quick reports from inside the courtroom. Judge England noted that except for limited pilot programs the federal courts prohibit radio or television broadcasts from the courtroom. In contrast, in the California state court on which he previously served each judge had discretion to decide what to allow, including multiple cameras, a pool camera, and limitations on what could be recorded (excluding for example any views of witnesses or jurors). His view and that of the Subcommittee is that we do not have enough information at this point to consider revising Rule 53 to take account of new technologies, and we should wait for more experience to develop.

Judge Raggi stated that unless there is a need for a one-size-fits-all rule, she did not favor an amendment that would tell judges how to run their courtrooms. She asked if any members felt that there was such a need.

A member noted one aspect of Twitter that might be relevant: since one can subscribe to a Twitter account, a juror might have subscribed to a reporter's Twitter account and receive messages posted from the courtroom. This poses a slightly different problem than jurors seeking out news accounts.

Professor Beale noted that there is also a significant overlap with traditional forms of reporting, since reporters generally Tweet to their broadcaster's or paper's news site. Judge England noted that in high profile cases we already have the problem of making sure jurors do not read about the case.

Discussion turned to the current practice in various courts. A member reported that in the Northern District of Illinois individuals can bring their phones into the courtroom and there is an executive order permitting individual judges to determine whether Twitter is permitted from their courtroom. In other courts, phones are not permitted without the court's permission. A member noted that in South Dakota's Supreme Court all reporters may Tweet. At the trial level, it is up to the individual judge. If they allow Tweeting, the judges give specific instructions that cover subscribers. There have been no problems with these policies in South Dakota.

Other members stated that they favored taking no action at this time. One commented that although there has been one ruling from a magistrate judge that Rule 53 bars Tweeting, other judges have read the rule differently. Thus the matter is not settled. Another member noted that if the Committee were to take up the matter, it should coordinate with Committee on Court Administration and Case Management (CACM).

Judge Lawson moved that the Committee not further pursue an amendment to Rule 53, and the motion passed unanimously.

E. Proposed Amendment to Rule 45

Discussion then turned to the proposal to amend Rule 45, which is the first action item coming from the work of a special subcommittee established by the Standing Committee to consider changes in the rules related to the CM/ECF system. The CM/ECF Subcommittee is chaired by Judge Michael Chagares, and is composed of all reporters as well as liaison members from all of the Advisory Committees. Judge Molloy is our liaison.

Professor Beale explained that when the rules initially authorized electronic service there were concerns that it might be problematic for a variety of reasons, such as difficulty in opening attachments. Accordingly, all of the rules (including Criminal Rule 45) provided for an additional three days to act whenever service was made electronically. The CM/ECF Subcommittee concluded that the concerns that justified the additional three days were no longer applicable. Moreover, the simplified rules for time computation–which converted all times for action to 7, 14, 21, and 28 days without excluding weekends and holidays–also counsel against adding three days when service is made electronically. Accordingly, the CM/ECF Subcommittee requested that all of the Advisory Committees consider elimination of the three-days-added rules at their spring meetings. Parallel amendments and committee notes are being considered by each Advisory Committee. The Civil Rules Committee approved the proposed change at its fall meeting, and its proposed amendment was approved for publication by the Standing Committee in January. The proposed amendment to Rule 45 tracks the change in the Civil Rule.

The Committee voted unanimously to transmit the proposed amendment to Rule 45 to the Standing Committee with the recommendation that it be published for public comment.

F. Other Suggestions for Possible Amendments

The Committee next turned to suggestions received from members of the public and the judiciary for amendments.

Professor Gabriel Chin proposed a change in the timing of the disclosure of presentence reports to make them available in advance of a guilty plea. As the reporters' memorandum in the agenda book explains, this might be accomplished by amendments to Rule 32 (and perhaps Rule 11). After a brief discussion of the procedures now followed it various districts, the burden on parole officers, and other potential problems, Judge Raggi asked if any member wished to move to place this issue on the Committee's agenda for more study. Since no member made such a motion, the matter will not be pursued at this time.

Judge Jon Newman wrote to urge consideration of an amendment to Rule 52 that would increase the availability of appellate review of sentencing errors. After a brief discussion in which members expressed interest in further consideration, Judge Raggi stated that she would appoint a subcommittee to study the proposal in depth, in coordination with the Appellate Rules Committee. Judge Raymond Kethledge will chair the subcommittee.

Jared Kneitel wrote to propose an amendment to Rule 29 to provide a procedure for making a motion for a judgment of acquittal in a bench trial. After a brief discussion, there was a consensus that there was no pressing need for an amendment at this time.

Judge Raggi then adjourned the meeting for the day.

G. Further Discussion of Proposed Amendments to Rule 41

On Friday morning, Judge Keenan presented the Rule 41 Subcommittee's revised recommendations. He thanked the Department of Justice representatives, the other subcommittee members, and the reporters for what he called yeoman work to develop a revised proposal.

The Subcommittee unanimously agreed that an amendment is warranted in two kinds of cases: those where anonymizing technologies have been used to mask the district in which a computer is located, and botnet investigations in which victim computers are located in a very large number of districts. The revised proposal is tailored to respond to these two problems: subdivision (a) of the proposal deals with the first problem, and subdivision (b) the second. The redrafted amendment is intended to clearly identify for the Standing Committee and general public the limited purpose and effect of the proposed change.

Mr. Wroblewski explained that in botnet investigations a large number of computers have been infected with malware. The language in proposed amendment focuses on these cases in several ways. The proposal is limited to investigations of violations of 18 U.S.C. § 1030(a)(5) where the media to be searched is a protected victim computer. Professor Beale briefly summarized Section 1030(a)(5), which criminalizes various forms of conduct–unauthorized transmission of programs, information, codes or commands as well as intentional access without

authorization–that causes damage to protected computers. The proposal is limited to investigations under § 1030(a)(5) in which warrants are sought in five or more districts, where the burden of seeking separate warrants would be very substantial.

A member spoke in favor of the proposal's targeted approach. He termed it sensible in proposed subsection (6)(a) to allow cross-district remote searches when the district has been deliberately concealed. He thought that proposed subsection (b) was a good effort to draft narrow language. The media to be searched must be "protected computers that have been damaged without authorization" by a violation of § 1030(a)(5). This would cover what is popularly called hacking, when a computer has been harmed by the insertion of code or taken off line. He noted the possibility that (6)(b) it might apply to some investigations that did not involve a botnet, and stated that the particularity requirement is likely to be the real limitation. In his view, if a warrant is constitutionally required, there will be a question whether it can be obtained.

Professor King noted that the terms "damage" and "protected computer" are defined in §§ 1030(e)(2) and (8). An addition to the Committee Note could make clear that the rule is adopting the statutory definitions.

A member expressed strong support for the proposal, which he saw as a very sound approach to real problems. He found the Department of Justice's flexibility very helpful, noting the strong public interest and importance of being clear about what the government is doing and why.

Judge Keenan moved to approve the Subcommittee's revised proposal to the Standing Committee with the recommendation that it be published for public comment. Discussion followed.

A member questioned whether it would be better to use the term "electronic search" rather than "remote access." Judge Raggi and the reporters responded that focus of the proposal was not on all electronic searches, but only those authorizing remote access searches outside the district in which the warrant would be issued. This is proposed as a narrow exception to the general rule that a magistrate judge has authority to issue warrants only within the district.

The member also expressed concern about limiting proposed (6)(a) to cases in which "the district ... has been concealed," because that suggests that the entire district has somehow been hidden. Judge Raggi and others noted that because the focus of the provision is on the authority to issue warrants to search outside the district, the rule needed to refer to the concealment of the district, not merely the location.

The member questioned whether the proposal could be modified to limit the use of remote searches only to the situations specified in (6)(a) and (b). The reporters and other members emphasized that remote searches are now authorized by Rule 41(e)(2)(B), provided that they occur within the district in which the warrant has been issued. Remote electronic searches are not new, and are not being authorized by this proposal. Rather, the proposed language in (6)(a) and (b) seeks *only* to authorize magistrate judges to issue warrants for remote electronic searches *outside the issuing district* in two narrowly defined situations. Another member commented that warrants for remote electronic searches within the issuing district are routinely issued now.

Other members raised various questions about the language of the proposal and suggested alternative phrasing. Judge Raggi requested that the Committee focus first on the substance of the proposal. She noted that if the proposal were adopted it would be subject to review for style, and there would be a further opportunity for members to comment on the language. Professor Beale noted that the committee note would also require revision to refer to the newly tailored language, and Judge Raggi stated that the proposed note language would be circulated.

A member noted that he had not initially thought it would be possible for the Committee to reach agreement on this proposal. He praised the Committee's collaborative effort and expressed support for the approach of narrowing the language to focus on the enforcement of an important statute.

With the proviso that the proposal was subject to review for style and the note would require revision, the Committee unanimously approved the Subcommittee's revised proposal to amend Rule 41(b) for transmission to the Standing Committee.

Discussion then turned to the proposed amendment to Rule 41(f)(1)(C), which requires service of a copy of the warrant and a receipt for property that has been seized.

Noting that the Subcommittee's proposal required service "on the person whose property was searched *or* whose information was seized," a member proposed that the service should be required on both (changing "or" to "and"). Judge Raggi responded that in the case of a physical search of a home, investigators now leave only one notice, even if they seize property belonging to multiple individuals. The member suggested that remote searches are different because they are generally surreptitious, and in the case of cloud computing they take place away from the owner. Thus the owner would not naturally be aware of the search. If only one party is to receive notice, he thought it should be the person whose information was seized or copied. The reporters noted some parallel situations under present law. Professor King noted that the notice of a warrant for a tracking device under Rule 41(f)(2)(C) uses "or." Professor Beale noted that if a warrant were served on Duke University today for a search of information on its servers, Duke

would receive notice, not all of the faculty, staff, and students whose digital files and information on university servers was searched, seized, or copied. Similarly, Judge Raggi noted that in the case of a physical search of a storage unit facility investigators would normally leave a single copy of the warrant and receipt. Mr. Wroblewski noted that under ECPA service is made only on the provider, such as Google, not the subscriber. As a matter of policy, however, many providers provide notice to their subscribers. Professor Beale agreed that in her hypothetical Duke would probably provide notice to its faculty and students.

Judge Raggi observed that whether to expand the existing requirements for providing notice of a search is a policy question. This could be taken up separately, but is not a part of the current proposal.

Discussion turned to the question whether the language of concern to the member (which specified who would receive notice of a remote electronic search) was a necessary part of the proposal. Professor King noted that as drafted the new language in (f)(1)(C) encompassed all remote electronic searches. Mr. Wroblewski explained that although the proposal did not seek to alter *who* should receive notice; in that respect it parallels the current provisions in (f)(1)(C) as well as the notice provisions of ECPA. However, it does seek to change *how* notice would be provided. The current language–which refers to the "premises" where the search is conducted–is not adapted to remote electronic searches. Because there are no premises where a notice may be left, the proposal allows service by "any means, including electronic means, reasonably calculated to reach" the person who must receive notice.

In response to another member's view that the proposal should require service on both the person whose property has been searched "and" the person whose information has been seized or copied, Judge Raggi noted that when the government is investigating the hacking of a provider, this might require the government to notify thousands of account holders. From a practical perspective, this may be too great a burden to impose on the government.

A member expressed support for requiring notice to the target whose information has been seized. More fundamentally, he argued, a remote electronic search is a different animal than a physical search. In his view, a separate rule or statute should deal comprehensively with remote electronic searches, which raise distinctive concerns about technology and privacy that should inform the approach to a range of issues concerning seizure, notice, and copying. The public is sensitized to these issues, and it needs to be reassured that the government is acting to protect privacy while pursuing criminal activity.

Judge Raggi observed that the constitutional requirement of probable cause for the issuance of a warrant is the primary protection for privacy interests.

A member stated that he supported the language proposed by the Subcommittee. It is helpful to be specific about how notice should be given for remote electronic searches. Especially in cases under proposed Rule 41(b)(6), the government may have very little information about whose property it is. It's very hard to be specific here about how notice must be given, but still helpful to have language that does not refer to leaving notice on the "premises." Another member agreed that a new provision on notice is needed. In an investigation of the intrusion at Target that affected thousands of customer accounts, there is nowhere to go to give notice.

Judge Raggi adjourned the meeting to permit the Rule 41 Subcommittee to consider the issues raised in the discussion. Following this recess, Judge Keenan reported the Subcommittee's recommendations concerning the proposed amendment to Rule 41(e)(1)(C). First, the Subcommittee agreed to delete the bracketed language Professor Kimble viewed as redundant. However, the Subcommittee disagreed with another style suggestion. It recommended that the proposed amendment require "reasonable efforts to serve *a copy of the warrant*" (not of "it"). The amendment itself refers to copying in a different sense (seizure or copying of electronically stored information). To avoid confusion, it is necessary to refer to service of a copy of the warrant. This is substance, not a matter of style. Finally, he asked a member of the Subcommittee to summarize the reasons for requiring service on the person whose property was searched "or" the person whose information was seized or copied.

The member explained there were three reasons for the Subcommittee's recommendation for "or" (rather than "and"):

First, the Subcommittee thought it appropriate to follow the precedent for physical searches. In the non-electronic search world the approach recommended by the Subcommittee has long been the rule. If the government had searched the New York Stock Exchange in the 1950s and seized the records of individual accounts, it would have given notice only to the Exchange, and not to individuals whose records might have been seized. The second reason was practicality. It would impose too great a burden to require notifications of all putative victims in a botnet case, which could be 1,000, or 100,000, or more. Finally, it would be possible in some cases only to search and not to seize or copy information, and accordingly the requirement for providing notice should be disjunctive.

Judge Keenan moved the approval of the Subcommittee's proposal to amend Rule 41(f)(1)(C).

A member who had argued in favor of "and" rather than "or" stated that he intended to vote in favor of the proposal. He explained that in the case of a remote electronic search what is really being searched is intellectual property. Once it has been viewed, it has been seized. By

this reasoning, the person whose property has been searched is the same as the person whose property has been seized or copied.

The motion to transmit the Subcommittee's revised proposal to amend Rule 41(f)(1)(C) to the Standing Committee for publication passed unanimously.

Before the meeting concluded, Judge Raggi acknowledged the many contributions of Judge Keenan and Judge Molloy, noting this was their last meeting as members of the Committee.