

**ADVISORY COMMITTEE
ON
CRIMINAL RULES**

**Orlando, FL
March 16-17, 2015**

TABLE OF CONTENTS

AGENDA 5

TAB 1 PRELIMINARY MATTERS

D. Minutes of November 2014 Criminal Rules Meeting 17

E. Draft Minutes of January 2015 Standing Committee Meeting..... 35

TAB 2 SUBCOMMITTEE REPORT – RULE 4

A. Reporters’ Memorandum 55

B. Proposed Amendment as Published 59

C. Summary of Public Comment 71

D. Memorandum from the Department of Justice, February 20, 2015 73

E. Memorandum from the Department of Justice, August 23, 2013..... 79

TAB 3 SUBCOMMITTEE REPORT – RULE 41

A. Reporters’ Memorandum 87

**B. Proposed Amendment with Revisions Proposed by
 Subcommittee 107**

C. Proposed Amendment as Published 113

D. Summary of Public Comments 125

**E. Memorandum from the Department of Justice,
 October 20, 2014 133**

**F. Memorandum from the Department of Justice,
 December 22, 2014 139**

**G. Memorandum from the Department of Justice,
 February 20, 2015 153**

TAB 4	SUBCOMMITTEE REPORT – RULE 45	
	A. Reporters’ Memorandum.....	159
	B. Proposed Amendment with Revisions Proposed by Subcommittee	165
	C. Proposed Amendment as Published.....	169
	D. Summary of Public Comments	173
	E. Memorandum from the Department of Justice	175
TAB 5	FULL TEXT OF PUBLIC COMMENTS ON PROPOSED AMENDMENTS TO RULES 4, 41 AND 45	179
TAB 6	SUBCOMMITTEE REPORT – RULE 35	
	A. Reporters’ Memorandum.....	503
	B. Reporters’ Background Memorandum for Subcommittee	505
	C. Supplemental Letter from New York Council of Defense Lawyers.....	523
	D. Letter from New York Council of Defense Lawyers (14-CR-E)	527
TAB 7	SUBCOMMITTEE REPORT – CM/ECF	
	A. Reporters’ Memorandum.....	535
	B. Material from Civil Rules Committee	539
TAB 8	NEW CRIMINAL RULE SUGGESTION	
	A. Reporters’ Memorandum.....	547
	B. 15-CR-A, Post-Sentencing Appeal Waivers.....	549

AGENDA
CRIMINAL RULES COMMITTEE MEETING
MARCH 16-17, 2015
ORLANDO, FLORIDA

I. PRELIMINARY MATTERS

- A. Chair's Remarks and Administrative Announcements
- B. Introduction of Rebecca Womeldorf, Chief of Rules Committee Support Office
- C. Recognition of Members Whose Terms End in 2015
- D. Minutes of November Meeting in Washington, D.C.
- E. Draft Minutes of Standing Committee Meeting in Phoenix, Arizona
- F. Status of Criminal Rules: Report of the Rules Committee Support Office

II. SUBCOMMITTEE REPORT RULE 4 (Service on Foreign Corporations)

- A. Reporters' Memorandum
- B. Proposed Amendment as Published
- C. Summary of Public Comments
- D. Memorandum from Department of Justice, February 20, 2015
- E. Memorandum from Department of Justice, August 23, 2013

III. SUBCOMMITTEE REPORT RULE 41 (Warrant to Use Remote Access to Search Electronic Storage Media and Seize or Copy Electronically Stored Information)

- A. Reporters' Memorandum
- B. Proposed Amendment With Revisions Proposed by Subcommittee
- C. Proposed Amendment as Published
- D. Summary of Public Comments
- E. Memorandum from Department of Justice, October 20, 2014
- F. Memorandum from Department of Justice, December 22, 2014
- G. Memorandum from Department of Justice, February 20, 2015

IV. SUBCOMMITTEE REPORT RULE 45 (Eliminating 3 Extra Days for Action After Electronic Service)

- A. Reporters' Memorandum
- B. Proposed Amendment With Revisions Proposed by Subcommittee
- C. Proposed Amendment as Published
- D. Summary of Public Comments
- E. Memorandum from Department of Justice

V. FULL TEXT OF PUBLIC COMMENTS ON PROPOSED AMENDMENTS TO RULES 4, 41, AND 45

VI. SUBCOMMITTEE REPORT RULE 35 (14-CR-E) (Sentence Reduction for Newly Discovered Evidence, Substantial Rehabilitation During Confinement, or Deterioration of Medical Condition)

- A. Reporters' Memorandum
- B. Reporters' Background Memorandum for Subcommittee
- C. Supplemental Letter from New York Council of Defense Lawyers
- D. Letter from New York Council of Defense Lawyers (14-CR-E)

VII. SUBCOMMITTEE REPORT CM/ECF

- A. Reporters' Memorandum
- B. Material from Civil Rules Committee

VIII. NEW CRIMINAL RULE SUGGESTION

- A. Reporters's Memorandum, Rule 35, 15-CR-A, Post-Sentencing Appeal Waivers
- B. 15-CR-A, Post-Sentencing Appeal Waivers

IX. RULES AND PROJECTS PENDING BEFORE CONGRESS, STANDING COMMITTEE, JUDICIAL CONFERENCE, AND OTHER COMMITTEES.

- A. Status Report on Legislation Affecting Federal Rules of Criminal Procedure
- B. Other

X. DESIGNATION OF TIMES AND PLACES FOR FUTURE MEETINGS

- A. Fall meeting, September 28-29, Seattle, Washington,

ADVISORY COMMITTEE ON CRIMINAL RULES

<p>Chair, Advisory Committee on Criminal Rules</p>	<p>Honorable Reena Raggi United States Court of Appeals 704S United States Courthouse 225 Cadman Plaza East Brooklyn, NY 11201-1818</p>
<p>Reporter, Advisory Committee on Criminal Rules</p>	<p>Professor Sara Sun Beale Charles L. B. Lowndes Professor Duke Law School 210 Science Drive Durham, NC 27708-0360</p> <p>Professor Nancy J. King Vanderbilt University Law School 131 21st Avenue South, Room 248 Nashville, TN 37203-1181</p>
<p>Members, Advisory Committee on Criminal Rules</p>	<p>Carol A. Brook, Esq. Executive Director Federal Defender Program for the Northern District of Illinois 55 East Monroe Street, Suite 2800 Chicago, IL 60603</p> <p>Honorable Leslie R. Caldwell Assistant Attorney General Criminal Division United States Department of Justice 950 Pennsylvania Avenue, N.W. Washington, DC 20530-0001</p> <p>Honorable James C. Dever III United States District Court Terry Sanford Federal Building 310 New Bern Avenue, Room 716 Raleigh, NC 27601-1418</p> <p>Honorable Morrison C. England, Jr. United States District Court 501 I Street – Suite 14-230 Sacramento, CA 95814-7300</p> <p>Honorable Gary Feinerman United States District Court Everett McKinley Dirksen United States Courthouse 219 South Dearborn Street, Room 2156 Chicago, IL 60604</p>

<p>Members, Advisory Committee on Criminal Rules (<i>cont'd</i>)</p>	<p>Mark Filip, Esq. Kirkland & Ellis LLP 300 North LaSalle Chicago, IL 60654</p> <p>Honorable David E. Gilbertson Supreme Court of South Dakota 500 E. Capitol Pierre, SD 57501</p> <p>Professor Orin S. Kerr The George Washington University Law School 2000 H Street, N.W. Washington, DC 20052</p> <p>Honorable Raymond M. Kethledge United States Court of Appeals Federal Building 200 East Liberty Street, Suite 224 Ann Arbor, MI 48104</p> <p>Honorable David M. Lawson United States District Court Theodore Levin United States Courthouse 231 West Lafayette Boulevard, Room 802 Detroit, MI 48226</p> <p>Honorable Timothy R. Rice United States District Court James A. Byrne United States Courthouse 601 Market Street, Room 3041 Philadelphia, PA 19106</p> <p>John S. Siffert, Esq. Lankler, Siffert & Wohl LLP 500 Fifth Avenue, 33rd Floor New York, NY 10110</p>
<p>Clerk of Court Representative, Advisory Committee on Criminal Rules</p>	<p>James N. Hatten Clerk United States District Court Richard B. Russell Federal Building and United States Courthouse 75 Spring Street, S. W., Room 2217 Atlanta, GA 30303-3309</p>

**Secretary, Standing Committee
and Rules Committee Officer**

Rebecca A. Womeldorf

Secretary, Committee on Rules of Practice &
Procedure and Rules Committee Officer
Thurgood Marshall Federal Judiciary Building
One Columbus Circle, N.E., Room 7-240
Washington, DC 20544
Phone 202-502-1820
Fax 202-502-1755
Rebecca_Womeldorf@ao.uscourts.gov

Advisory Committee on Criminal Rules

Members	Position	District/Circuit	Start Date	End Date
Reena Raggi Chair	C	Second Circuit	2011	2015
Carol A. Brook	FPD	Illinois (Northern)	2011	2017
James C. Dever III	D	North Carolina (Eastern)	2014	2017
Morrison C. England, Jr.	D	California (Eastern)	2008	2015
Gary Scott Feinerman	D	Illinois (Northern)	2014	2017
Mark Filip	ESQ	Illinois	2013	2015
David E. Gilbertson	CJUST	South Dakota	2010	2016
Orin S. Kerr	ACAD	Washington, DC	2013	2016
Raymond M. Kethledge	C	Sixth Circuit	2013	2016
David M. Lawson	C	Michigan (Eastern)	2009	2015
Mythili Raman*	DOJ	Washington, DC	----	Open
Timothy R. Rice	M	Pennsylvania (Eastern)	2009	2015
John S. Siffert	ESQ	New York	2012	2015
Sara Sun Beale Reporter	ACAD	North Carolina	2005	Open

Principal Staff: Rebecca A. Womeldorf 202-502-1820

* Ex-officio

LIAISON MEMBERS

Liaison for the Advisory Committee on Appellate Rules	Gregory G. Garre, Esq. <i>(Standing)</i>
Liaison for the Advisory Committee on Bankruptcy Rules	Roy T. Englert, Jr., Esq. <i>(Standing)</i>
Liaison for the Advisory Committee on Civil Rules	Judge Arthur I. Harris <i>(Bankruptcy)</i>
Liaison for the Advisory Committee on Civil Rules	Judge Neil M. Gorsuch <i>(Standing)</i>
Liaison for the Advisory Committee on Criminal Rules	Judge Amy J. St. Eve <i>(Standing)</i>
Liaison for the Advisory Committee on Evidence Rules	Judge Paul S. Diamond <i>(Civil)</i>
Liaison for the Advisory Committee on Evidence Rules	Judge James C. Dever III <i>(Criminal)</i>
Liaison for the Advisory Committee on Evidence Rules	Judge Richard C. Wesley <i>(Standing)</i>

ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

Rebecca A. Womeldorf

Secretary, Committee on Rules of Practice &
Procedure and Rules Committee Officer
Thurgood Marshall Federal Judiciary Building
One Columbus Circle, N.E., Room 7-240
Washington, DC 20544
Phone 202-502-1820
Fax 202-502-1755
Rebecca_Womeldorf@ao.uscourts.gov

Julie Wilson

Attorney Advisor
Thurgood Marshall Federal Judiciary Building
One Columbus Circle, N.E., Room 7-240
Washington, DC 20544
Phone 202-502-3678
Fax 202-502-1766
Julie_Wilson@ao.uscourts.gov

Scott Myers

Attorney Advisor (Bankruptcy)
Thurgood Marshall Federal Judiciary Building
One Columbus Circle, N.E., Room 4-250
Washington, DC 20544
Phone 202-502-1900
Fax 202-502-1988
Scott_Myers@ao.uscourts.gov

Bridget M. Healy

Attorney Advisor
Thurgood Marshall Federal Judiciary Building
One Columbus Circle, N.E., Room 4-273
Washington, DC 20544
Phone 202-502-1900
Fax 202-502-1988
Bridget_Healy@ao.uscourts.gov

Toni A. Loftin

Administrative Specialist
Thurgood Marshall Federal Judiciary Building
One Columbus Circle, N.E., Room 7-240
Washington, DC 20544
Phone 202-502-1682
Fax 202-502-1755
Toni_Loftin@ao.uscourts.gov

Frances F. Skillman

Paralegal Specialist

Thurgood Marshall Federal Judiciary Building

One Columbus Circle, N.E., Room 7-240

Washington, DC 20544

Phone 202-502-3945

Fax 202-502-1755

Frances_Skillman@ao.uscourts.gov

FEDERAL JUDICIAL CENTER

<p>Tim Reagan <i>(Rules of Practice & Procedure)</i> Senior Research Associate Federal Judicial Center Thurgood Marshall Federal Judiciary Building One Columbus Circle, N.E., Room 6-436 Washington, DC 20002 Phone 202-502-4097 Fax 202-502-4199</p>	<p>Marie Leary <i>(Appellate Rules Committee)</i> Research Associate Research Division Thurgood Marshall Federal Judiciary Building One Columbus Circle, N.E. Washington, DC 20002-8003 Phone 202-502-4069 Fax 202-502-4199 mleary@fjc.gov</p>
<p>Molly T. Johnson <i>(Bankruptcy Rules Committee)</i> Senior Research Associate Research Division Thurgood Marshall Federal Judiciary Building One Columbus Circle, N.E. Washington, DC 20002-8003 Phone 315-824-4945 mjohnson@fjc.gov</p>	<p>Emery G. Lee <i>(Civil Rules Committee)</i> Senior Research Associate Research Division Thurgood Marshall Federal Judiciary Building One Columbus Circle, N.E. Washington, DC 20002-8003 Phone 202-502-4078 Fax 202-502-4199 elee@fjc.gov</p>
<p>Laural L. Hooper <i>(Criminal Rules Committee)</i> Senior Research Associate Research Division Thurgood Marshall Federal Judiciary Building One Columbus Circle, N.E. Washington, DC 20002-8003 Phone 202-502-4093 Fax 202-502-4199 lhooper@fjc.gov</p>	<p>Catherine Borden <i>(Evidence Rules Committee)</i> Research Associate Research Division Thurgood Marshall Federal Judiciary Building One Columbus Circle, N.E. Washington, DC 20002-8003 Phone 202-502-4090 Fax 202-502-4199 cborden@fjc.gov</p>

TAB 1D

**ADVISORY COMMITTEE ON CRIMINAL RULES
MINUTES
November 4-5, Washington D.C.**

I. Attendance and Preliminary Matters

The Criminal Rules Advisory Committee (“Committee”) met Washington D.C. on November 4-5, 2014. The following persons were in attendance:

Judge Reena Raggi, Chair
Carol A. Brook, Esq.
Hon. Leslie Caldwell¹
Judge Morrison C. England, Jr.
Judge James C. Dever
Judge Gary Feinerman Mark
Filip, Esq. (Nov. 5 only)
Chief Justice David E. Gilbertson
Professor Orin S. Kerr
Judge Raymond 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

The following persons were present to support the Committee:

Laural L. Hooper, Federal Judicial Center
Jonathan C. Rose, Rules Committee Officer
Julie Wilson, Rules Office Attorney

II. CHAIR’S REMARKS AND OPENING BUSINESS

A. Chair’s Remarks

Judge Raggi introduced new members Judge James C. Dever, Judge Gary Feinerman, Judge Raymond Kethledge, and Leslie Caldwell, the new Assistant Attorney General for the Criminal Division. She welcomed observers Peter Goldberger of the National Association of

¹ The Department of Justice was represented at various times throughout the meeting by Leslie Caldwell, Assistant Attorney General for the Criminal Division; Marshall Miller, Principal Deputy Assistant Attorney General for the Criminal Division; David Bitkower, Deputy Assistant Attorney General for the Criminal Division; and Jonathan Wroblewski, Director, Office of Policy and Legislation in the Criminal Division.

Criminal Defense Lawyers and Catherine Recker of American College of Trial Lawyers. Judge Raggi noted that Jonathan Rose had indicated he might not be able to attend the March meeting and she therefore wished to thank him for his service now in the event she could not do it then. She also thanked all of the staff members who made the arrangements for the meeting and the hearings.

For the benefit of new members, Judge Raggi reviewed the process by which the Committee considered new or amended rules of procedure and how its recommendations then proceeded to the Standing Committee on the Federal Rules, the Judicial Conference of the United States, the Supreme Court, and Congress.

B. Review and Approval of Minutes of April 2014 Meeting

A motion to approve the minutes of the April 2014 Committee meeting in New Orleans, having been seconded:

The Committee unanimously approved the April 2014 meeting minutes by voice vote.

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

Jonathan Rose 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 12. Pleadings and Pretrial Motions
- Rule 34. Arresting Judgment
- Rule 5. Initial Appearance
- Rule 58. Petty Offenses and Other Misdemeanors
- Rule 6. The Grand Jury

D. Proposed Amendments Published for Comment

The comment period for the proposed amendments to the following rules concludes February 17, 2015. Committee action on these amendments will be deferred until the spring meeting, following the close of the comment period.

- Rule 4. Arrest Warrant or Summons on a Complaint
- Rule 41. Search and Seizure
- Rule 45. Computing and Extending Time; Time for Motion Papers

Judge Raggi reported that the only comment received to date on the proposed amendment to Rule 4 was supportive. A member reported that those to whom he had spoken about the amendment were satisfied that their earlier expressed concerns were addressed by the language

of the published rule. Many comments have been received on Rule 41, and the Committee would conduct a hearing on that rule on November 5. No comments have been received to date on the proposed amendment to Rule 45.

III. CRIMINAL RULES ACTIONS

A. Proposed Amendment to Rule 11

Judge Raggi asked Judge England, Chair of the Rule 11 Subcommittee, to report on the Subcommittee's review of the proposal from Chief Judge Claudia Wilken of the Northern District of California to amend Rule 11 to state that it did not prevent trial judges from referring criminal cases to other judicial officers for the purpose of exploring settlement.

Judge England summarized the proposal and the Subcommittee's work, also described in the memorandum to the Committee in the agenda book. He reported that at least six districts had engaged in settlement conferences before the Supreme Court's decision in *United States v. Davila*, 133 S.Ct. 2139 (2013), indicated that this practice violated Rule 11. He noted that the Committee had already considered, and not acted favorably on, three prior proposals to approve judicial participation in settlement conferences or plea bargaining. He summarized concerns raised by the proposal, including (1) judicial intrusion on the prosecutorial role of the executive, (2) adverse effects on judicial impartiality if a judge is privy to plea negotiations, and (3) the risk of coercing defendants into plea dispositions that they would otherwise not accept.

Judge England reported that the Subcommittee met twice by telephone, and on the second occasion heard directly from Chief Judge Wilken. The Subcommittee also considered memoranda from the Committee's Reporters and from the Department of Justice. The Subcommittee was unable to reach consensus as to how to proceed and sought full Committee discussion to learn whether the proposal should be pursued.

Subcommittee members were then invited to comment.

A subcommittee member reported on an informal survey of eight federal defenders from the districts where judicial officers had participated in settlement conferences. These defenders unanimously thought the practice was valuable and should be permitted. They reported that it was used very rarely, and they did not feel judicial pressure or interference. They mentioned its most frequent use in three types of cases: (1) large, complex cases, particularly those in which the government was seeking a global disposition by all defendants; (2) cases in which parties were close to agreement on disposition but could not quite get there on their own; and (3) cases where parties wanted a plea disposition but were far apart. Judicial involvement was also helpful in rare cases when a defendant was not heeding his attorney and needed to hear the reality of his situation from a neutral third party. The surveyed defenders reported no cases in which a settlement conference failed to produce an acceptable plea agreement. To the extent defenders feel that circumstances such as mandatory minimum sentences and the Sentencing Guidelines slant the "playing field" in favor of the government, they view judicial involvement in plea negotiations as something that helps level the field. The subcommittee member characterized judicial involvement in plea negotiations as a useful tool that each district could

Minutes
Criminal Rules Meeting
November 4-5, 2014
Page 4

decide if and how to use.

Another subcommittee member reported that surveyed prosecutors in the districts where judges participated in settlement discussions had mixed reactions, with the vast majority opposed, mostly because they felt the process was designed to put pressure on both the defendant and the prosecution to come to an agreement and to avoid trial. In some cases this is uncomfortable for all parties, and not a healthy dynamic. The member emphasized that the vast majority of cases are already disposed of by plea, so there is no urgent need for the procedure to ensure efficient use of court resources.

A third subcommittee member also expressed concern about the potential for coercion on both parties. When there is a global plea offer that one defendant is reluctant to accept, judicial involvement could exert tremendous pressure on that defendant. This concern can be minimized somewhat by not allowing the trial judge to become involved in the plea negotiation. But a referral judge will not be as familiar with the evidence and the strengths or the weaknesses of the case. The effort necessary for the referral judge to familiarize herself with the case will reduce the efficiencies cited to support the process. The member also agreed with concerns about separation of powers, judicial neutrality, and the perception that this is more a docket management tool than one focused on securing a “right outcome.”

A subcommittee member reported that the practice is not followed in this member’s district. Despite the government’s concerns, this member was of the opinion that if the procedure is limited to cases where there has been a joint request by parties who agree that they need help, it is a good idea for a judge not involved in the case to provide help. State courts have been doing this for years, and the Committee can build sufficient safeguards into a rule to avoid possible abuse.

Another subcommittee member opposed the proposal on three grounds. First, the need for a rule change had not been demonstrated. If there is no significant difference in guilty plea rates as between districts that do and do not involve judges in plea bargaining, why amend the Rule? If defendants now feel coercion to plead from the prosecutor, exposing them to pressure from a judge is not a good idea. Second, although judges routinely mediate civil cases to encourage settlement, criminal cases are different. The former can often be resolved with monetary compensation, while what is at stake in the latter is liberty. The role played by the judiciary in the criminal process thus needs to be purely neutral. Third, there may be troubling consequences if dissatisfied defendants challenge convictions based on judicial conduct in plea negotiations. Will judges have to testify regarding what was said at the conference? Must there be a transcript of what goes on? If there is a transcript, will people speak as freely about offers and demands, and, if they do not, will that compromise the process? In sum, even if judicial

involvement in plea bargaining might increase dispositions in some cases, the member concluded that efficiency should not drive the decision to adopt an amendment.

Another subcommittee member stated that even if there is no constitutional prohibition on judicial involvement in the plea process, a risk remains that, at some point, judicial participation can cross the line and interfere with the voluntariness of the plea. How will the judge accepting the plea know whether that line was crossed in the settlement conference?

A subcommittee member saw no need for this procedure, which no court in his circuit employs. The clarity of the present rule is beneficial; judges know what they can and cannot do. Even a true joint request does not eliminate concerns about the independence of the executive's prosecutorial role. This member was also concerned about how the process might work. In cases in which the plea is not pursuant to an agreed-upon Rule 11(c)(1)(C) sentence, any defendant who receives a more severe sentence than that discussed with the settlement judge will be upset and likely try to challenge his conviction. A Magistrate Judge might say a certain sentence would be fair based on the information available at the settlement conference, but later at sentencing the District Judge who received the presentence report (PSR) would have more information and might impose a higher sentence. This will result in an appeal or a 2255 motion. There are also practical issues about either transcribing the conferences or later requiring a Magistrate Judge to submit an affidavit stating what he or she said.

Judge Raggi then reminded the Committee of the specific language of Judge Wilken's proposal and opened the floor for discussion by all Committee members. She noted that it would be particularly helpful to hear whether members who favored the proposal thought the Committee should set safeguards in a rule or whether that should be left to each district that chose to involve judges in plea bargaining. Specifically, should a rule require that settlement conferences be recorded and that the defendant be present? Should a rule indicate whether statements made during negotiations can or cannot be used at any subsequent proceeding?

A Committee member stated that defense attorneys did not have a problem with Judge Wilken's proposal. He noted that the dynamic in criminal cases is different from that in civil cases, where the dispute is often about money, and the parties are eager to have a neutral intermediary help them reach a reasonable settlement. Nevertheless, in criminal cases, defendants often have difficulty accepting the reality of what they have done and what they are facing. At the point of charging and plea, counsel is sometimes helping a defendant pass from someone with no record and a good self-image, to someone who admits he has been guilty of a criminal offense. It is a very emotional and trying experience. Having a third party assist with that transition can be very helpful. There are times when the defense wants help, and if the government consents, why not make this process available to help some defendants with this transition? Maybe the practical difficulties are too difficult to overcome, but the Committee should consider the proposal further.

When another Committee member asked what a judge could do in this situation to help, other than suggest a better offer for the defense, the member responded that when a client has a crisis of confidence in his attorney, just hearing counsel's position reiterated by someone else helps.

A Committee member asked how the referral judge will be sufficiently educated about a case to make an informed plea recommendation. A Subcommittee member responded that some federal defenders write memos for the judge laying everything out. The member was not sure whether that memo also goes to the prosecution, but assumed it does. The settlement judge's main contribution is not providing sentencing information. Defenders reported that the Magistrate Judges conducting these sessions were prior defense attorneys or prosecutors, and are able to comfort the defendant in a way that his attorney cannot. The member emphasized that settlement conferences are not used for clients who are maintaining their innocence; no attorney would agree to it in that situation. It is helpful for a client who has authorized plea discussions, or who says, "I want to see what is out there, but I don't know how."

Another Committee member expressed concern and skepticism, noting how simple it was for a judge to telegraph a preference for plea negotiations, thereby overcoming the safeguard of joint consent. Counsel appearing frequently before the court would be motivated to conform to the apparent wish of the referring judge for a settlement conference or to the recommendation of the referral judge. The member stated that he did not understand how judges are supposed to help with the "transition" defense counsel are talking about.

A Subcommittee member stated that there is already tremendous pressure under the Guidelines to plead guilty in order to get acceptance of responsibility consideration.

A Committee member reported that in state court, judges have long participated in plea negotiations, and it did not produce more appeals or habeas petitions perhaps because the process is initiated by the lawyers, the defendant has bought into the process, and it is always about sentencing.

A Subcommittee member noted a significant difference between state and federal criminal proceedings. The member expressed concern about cases in which a District Judge did not agree with the Magistrate Judge who conducted the settlement conference. The member also voiced concern about conferences at which the defendant was not present or that were not on the record. Acknowledging that judges in some districts had used the practice and favored it, the member nevertheless stated that he did not see the need for it.

Another Subcommittee member stated that the point of negotiating an agreement is to come to an agreement. But the sentencing judge has to be part of the process for there to be a true agreement. In the courts of the member's state it is common for the parties to have a conversation with the judge about sentence and to get an indication from the judge about the likely sentence. This process works because the parties are dealing directly with the decision

maker. In the proposal for the federal system, however, the ultimate decision maker would not conduct the conference, and the member opined that will not work.

Judge Raggi advised the Committee that District Judge Jed Rakoff of the Southern District of New York had recently published an article (copies of which were circulated to the Committee) that, inter alia, also advocated judicial involvement in plea bargaining. But unlike the N.D. Cal. proposal, which emphasized that such involvement facilitated guilty pleas, Judge Rakoff urged judicial involvement to counter what he perceived as too many guilty pleas, including guilty pleas from “innocent” persons, which he attributed in part to the inadequate plea allocutions conducted by “most judges.” Judge Raggi noted her own disagreement with the last assertion and observed that, even if such a concern were warranted, it was not apparent that the solution to that problem was to get another judicial officer involved in plea negotiations.

Judge Raggi then suggested that the Committee consider whether to pursue the pending proposal by reference to two questions, focusing first the threshold inquiry for all rules amendments -- Is there a problem that needs to be addressed by a rule?—and second, Would the benefits of the proposed rule outweigh any concerns?

As to need, the N.D. Cal. proposal urged an amendment to Rule 11 to facilitate plea dispositions, particularly in complex cases. Judge Raggi noted that the national guilty plea rate is over 95% (a number that had climbed steadily in recent decades), and that districts urging judicial involvement in plea negotiations were right in the mainstream. So there appears to be no problem of courts being overwhelmed with trials that needs to be addressed by amending Rule

Thus, the benefits of the amendment would seem to apply in only a small number of cases.

Turning to concerns, Judge Raggi attempted to summarize the concerns raised in memoranda received by the Committee and in the Committee discussions.

1. Separation of Powers. The responsibility for prosecuting crimes---which includes discretion to decide what crimes to charge and the pleas satisfactory to dispose of the charges---vests in the Executive branch, just as the responsibility for sentencing vests in the judiciary. Should the judiciary assign itself a role in the former area?

2. Competency. How equipped are judicial officers to make sound plea recommendations, given the need for a thorough knowledge of the case and its context? Acquisition of such knowledge may require a substantial expenditure of resources (both by judges and probation departments). Thus, predictions that judicial plea bargaining will save resources in an area of judicial competence (trials) must be considered in light of increased demands on resources in an area of lesser competence (crafting plea bargains).

3. Transforming Judicial Role. The neutrality that characterizes the judicial rule is nowhere more important---as a matter of fact and of perception---than in criminal cases. That neutrality must be manifested by every judicial officer whom the defendant encounters. Will that

neutrality by undermined once any judicial officer is seen as urging a particular disposition? Will that concern be aggravated if the judicial recommendation matches that of the prosecution?

4. Intrusion on Attorney-Client Relationship. This may be mitigated by the parties' consent. Nevertheless, having judges reinforce or undermine the recommendation made by counsel intrudes on the attorney-client relationship in a way that warrants pause. Further, to the extent it has been suggested that judicial involvement in plea bargaining is helpful because many defendants do not "trust" court-appointed lawyers and will be more inclined to accept recommendations from a neutral judge, query how likely it is that a defendant who does not trust his appointed attorney will trust the judge who appointed his attorney?

5. Legal and Ethical Considerations.

- Does defendant have a right to be present for plea negotiations. It had not been N.D. Cal. practice to require.
- What protections should be afforded defendant for statements he or counsel make to the judicial officer in settlement discussions?
- Are there limits on what the judge can say? Can the judge ask about guilt?
- If defendant or counsel maintains innocence, can a judge ever recommend a guilty plea?
- If defendant later testifies contrary to what he or counsel said during conference what are the referral judge's responsibilities regarding perjury?
- Although the N.D. Cal. had not required settlement conferences to be recorded, query whether any contact between a judicial officer and a criminal defendant should be "off the record." Does a record of the conference stifle candor?

6. Accepting a Guilty Plea. To the extent proponents contemplate that plea negotiations are not revealed to the trial judge, does this apply only if the case proceeds to trial? If negotiations result in a guilty plea, can a trial judge responsibly conclude that the plea is knowing and voluntary without reviewing the record of proceedings before the referral judge? Consider this in light of the error in Davila, which rendered the plea involuntary.

7. Increased Litigation. Will defendants who now invariably bring collateral challenges to conviction based on the ineffective assistance of counsel likely find fault with the conduct of judicial officers during plea negotiations, giving rise to increased litigation about judicial promises or coercion?

Judge Raggi indicated that she herself thought that these concerns, along with the advantages of uniformity, far outweighed the benefits of the proposed amendment.

The Committee's Liaison member opined that having a judge than the sentencing judge

making recommendations about sentencing is asking for trouble. The referral judge will not have the benefit of the PSR, an important document to give a full picture of the defendant. Sometimes the PSR raises criminal history points that the parties may not know about, and the settlement judge would not have the benefit of that information. In addition, judges have different views of sentencing, and may not agree with one another on the appropriate sentence. Plus, whatever efficiency you get on the front end, you will lose on the 2255 end. The member did not want to see judges having to submit affidavits. Finally, the member expressed concern with allowing diverse district practices respecting guilty pleas. The Standing Committee has traditionally favored uniformity on major issues.

Professor Coquillette agreed that the Standing Committee has been concerned about local rules on matters where judicial procedures should be uniform throughout the courts. Congress has also expressed concern that local rules might be used to evade its power to review rules pursuant to the Rules Enabling Act. Thus, local rules may be appropriate when they reflect real demographic or geographic differences between districts, but nothing has been said about why certain districts have a special need for the proposed settlement procedure.

A Committee member questioned how the process would work. Would the defendant be promised a particular sentence during the settlement conference? At the plea colloquy, before the defendant says "yes I am guilty," does the judge accept the agreement reached at the conference, including the sentence expected by defendant? Members agreed that the process would play out differently in cases in which the parties agreed to an 11(c)(1)(C) plea. Some thought judicial involvement would pose fewer problems in such cases because the sentencing judge would not need to know about the give and take during the negotiation. On the other hand, any 11(c)(1)(C) plea must be accepted by the sentencing judge, and injecting a second judge into this process could create problems. A member noted that in one district in New York, 11(c)(1)(C) pleas are unusual, disfavored, and subject to a special review in the U.S. Attorney's Office. That USAO has a committee that reviews all 11(c)(1)(C) proposals before submitting them for approval by the United States Attorney. This process ensures uniformity within a large office, something that could be adversely affected if a judge were to participate in the plea process, and make a recommendation before committee and U.S. Attorney review.

Another member observed that under current practice the District Judge would be telling only the United States Attorney that she is not prepared to accept the plea agreement, but with the proposed amendment, that judge could be telling another judicial officer she is not prepared to accept what that referral judge had agreed to.

With discussion concluded, Judge Raggi asked the Committee to vote on the question of whether the Rule 11 Subcommittee should be asked further to consider Chief Judge Wilken's proposal to amend Rule 11.

The question of whether to pursue further the proposal to amend Rule 11 was put the Committee; it failed with 4 in favor and 6 opposed to continued consideration.

B. Proposed Amendment to Rule 52

Judge Raggi invited Judge Kethledge, Chair of the Rule 52 Subcommittee, to report the Subcommittee's recommendation regarding the proposal from Judge Jon Newman of the Second Circuit Court of Appeals to amend Rule 52 to allow for review of defaulted sentencing errors without satisfying the requirements of plain error if the error caused prejudice and correction would not require a new trial.

Judge Kethledge summarized the proposal and the questions addressed by the Subcommittee and detailed in the Reporters' Memorandum to the Committee included in the agenda book. These questions focused on the frequency with which sentencing errors are not being corrected under the present rule; the scope of the proposal, particularly which types of error would be included; and the extent to which the proposal would generate additional litigation in circuit and district courts. Judge Kethledge noted the Subcommittee's receipt of a memorandum from the Department of Justice responding to the proposal, and that the deliberations of the Subcommittee were informed by the perspective of trial judges and defense attorneys, as well as the government. At the end of its first telephone meeting, the Subcommittee was skeptical of the proposal, but scheduled a second telephone meeting to hear from Judge Newman. Before that call, Judge Newman provided the Subcommittee with a memorandum responding to the points raised by the Department of Justice and revising his proposal to apply only to sentencing errors that increased a defendant's sentence. After hearing from Judge Newman, the Subcommittee discussed the proposal further, and ultimately voted unanimously to recommend that the Committee not take any action on the proposal.

Judge Kethledge explained that the Subcommittee determined that there was not enough of a problem to warrant an amendment. Judge Newman identified a handful of cases in which, he argued, his proposal would have changed the outcome. The Subcommittee was not convinced it would have made a difference in all those cases. As to Guidelines calculation errors increasing sentences, most of those are being corrected on plain error review. Even if there are a small number of cases where this is not happening, the Subcommittee considered the benefit of a rule amendment outweighed by the additional litigation regarding the exception's reach and the causation question of whether a judge would have imposed a lesser sentence but for the Guidelines error. The Subcommittee also discussed whether the proposed amendment could create incentives for counsel to be less vigilant in raising sentencing errors in the district court. Finally there were questions about how receptive the Supreme Court would be to the proposed amendment in light of its decision in *Puckett v. United States*, 556 U.S. 129 (2009), applying the plain error test of *United States v. Olano*, 507 U.S. 725 (1993) and Rule 52(b) to errors in the plea process.

Thus, after extensive discussion, the Subcommittee unanimously agreed to recommend no further action on the proposal.

The Committee then voted unanimously not to pursue the proposal to amend Rule 52.

Judge Raggi thanked both the Rule 11 and Rule 52 Subcommittees and the reporters for the work they had put into considering both proposals for amendment. She also noted that Chief Judge Wilken and Judge Newman seemed appreciative of the opportunity to be heard orally and in writing by the Subcommittees.

C. Proposal to Amend Habeas Rule 5

Professor Beale described a request received from District Judge Michael Baylson of the Eastern District of Pennsylvania for the Committee to consider amending Rule 5 of the Rules Governing 2254 Proceedings to provide that the state is not required to serve a petitioner with the exhibits that accompany an answer unless the District Judge so orders. A discussion ensued regarding whether the proposal should go to a subcommittee.

A member expressed the view that the creation of a subcommittee and further consideration was not warranted. There is no disagreement in the courts on this issue, which expect the state to serve petitioner with all documents accompanying an answer, and the proposed change would generate different practices and less uniformity.

Another member noted that if this proposal is referred to a subcommittee the Department of Justice would want to consider recognizing judicial discretion to order that certain documents not be provided to habeas petitioners, either because they are voluminous or because there is a special concern about releasing certain documents within a correctional facility.

Another member who had worked in the office of a state attorney general stated that it would never have occurred to the attorneys in that office that they could send something to the court that wouldn't also go to the petitioner.

Judge Raggi asked Professor King for her views in light of her extensive scholarship in the area of 2254 motions. Professor King opined that the current rule is not posing a problem. She noted that no concern about the present Rule was being raised by the states' attorneys, who would be the logical ones to complain if there was a problem.

The Committee then voted unanimously not to pursue the proposal to amend Rule 5 of the Rules Governing 2254 Proceedings.

D. CM/ECF

Professor Beale described the work of the CM/ECF Subcommittee of the Standing Committee, on which Judge Lawson is now the Committee's Liaison (replacing Judge Malloy whose term on the Committee has expired). She reported that this Committee will have to decide whether it is time for a uniform, national rule for electronic filing in criminal cases. Criminal Rule 49(e) (which was based on the Civil Rules) presently leaves the question whether to permit

e-filing to local rules. At its October 2014 meeting, the Civil Rules Committee approved a national rule requiring e-filing in all civil cases (with exceptions). Thus, this Committee might create a subcommittee to consider whether to amend Rule 49. Professor Coquillette explained that with the courts moving to the next generation system for electronic filing, there is a lot of experimentation. But it is difficult to get districts to give up a local rule once they have tried it.

Judge Lawson, the liaison to the CM/ECF effort, noted that Criminal Rule 49(b) incorporates the civil rules. If those rules are amended to require e-filing and electronic signatures, that may no longer work for the Criminal Rules. He noted that his district created a set of CM/ECF policies and procedures that can be changed quickly without going through the local rule changing process, in order to adapt to changes in technology more quickly. He also noted it will be important to address these issues in conjunction with the other advisory committees.

Judge Raggi reported she had asked Judge Lawson to chair a new subcommittee that will consider whether the civil rule adequately addresses the concerns in criminal cases to support this Committee's adoption of an identical criminal rule or whether a different electronic filing rule is necessary to address the distinctive needs of criminal cases.

Professor Coquillette stated that the Department of Justice looks at these issues closely, in the past expressing concern about the use of electronic signatures in certain contexts. The views of defense counsel will also be important to defining where carve outs are necessary.

A member responded that the Criminal Division expects to work on this with the entire Justice Department, including investigative agencies, as it did when considering electronic warrants.

E. New Proposal to Amend Rule 35.

Judge Raggi reported that, after the agenda book closed, the Committee received a proposal from the New York Council of Defense Lawyers to amend Rule 35 to afford judges' discretion to reduce sentences after they became final. She asked a member familiar with the proposal to describe it.

The member explained that the proposal would allow a district judge, upon motion, to reduce the sentence of a defendant who had served two thirds of his term in three circumstances: (1) newly discovered scientific evidence cast doubt on the validity of the conviction; (2) substantial rehabilitation of the defendant; or (3) deterioration of defendant's medical condition (providing an alternative compassionate release). Another member expressed support for the proposal, noting that this would provide another means for reducing the prison population.

Another member questioned how the proposal would operate in light of temporal statutory limits on collateral review under §§ 2241 and 2255. The member also questioned the Committee's ability to use a procedural rule to authorize sentence reductions below statutorily mandated minimums. At the same time, the member acknowledged that judges with experience

under the old Rule 35 (prior to the Sentencing Reform Act) thought that version of the Rule was beneficial.

Professor Beale reported that the American Law Institute is also considering including a “second look” provision in its draft model sentencing law.

Professor Coquillette stated that the Rules Enabling Act’s supersession clause does permit the adoption of rules that supersede existing statutes. But injudicious invocation of that clause may prompt Congress to reconsider it. Thus, the Rules Committees have often pursued a different approach, *i.e.*, sponsored legislation.

A member noted that the proposal intersects with many statutes and policies as well as current pending legislation. For example, a bill just approved by the Senate Judiciary Committee includes a “second look” provision that would apply earlier than the timing of the proposal.

F. New Subcommittees

The Committee adjourned for lunch, and when it reconvened Judge Raggi announced the membership of two new subcommittees:

Rule 35 Subcommittee

Judge Dever, Chair
Ms. Brook
Judge Feinerman
Judge Lawson
Mr. Siffert
Mr. Wroblewski

CM/ECF Subcommittee

Judge Lawson, Chair
Ms. Brook
Judge England
Prof. Kerr Judge
Judge Rice
Mr. Wroblewski

Judge Raggi also announced that Judge Dever would serve as the Committee’s liaison to the Evidence Committee, a position formerly held by Judge Keenan, whose term on the Committee expired.

G. Preparation for the Committee’s Public Hearing

Judge Raggi then asked the Reporters to provide the Committee with an overview of issues raised in public comments to Rule 41 in preparation for the next day’s hearing.

Professor Beale said the issues fell into three categories: (1) whether an alternate venue for remote access searches should be established by rule or by legislation; (2) Fourth Amendment issues as to particularity, the reasonableness of the proposed surreptitious entry into electronic devices, adequate notice, the types of information seized, the nature of the intervention and potential damage to targets and non-targets; and (3) concerns about the unintended effects of remote searches, including unintended damage to both the device to be searched and third parties.

Professor King added that some comments voiced concern that even if Rule 41 is amended only to expand venue, once such an amendment took effect, it would be difficult to litigate the identified constitutional issues.

Judge Raggi asked Professor Kerr to share his views. Professor Kerr stated that every remote access search raised numerous interesting questions beyond the venue issue addressed in the amendment. Some of these questions fall outside the Committee's authority. He noted that the proposed amendment does not affirmatively approve remote access searches, the constitutional status of which is presently unsettled. As for concerns about the adequacy of suppression motions to address all concerns, he observed that not all Title III issues could be raised in a motion to suppress. Some could be litigated only in collateral civil litigation. He thought the comments most helpful to the Committee's work were those that addressed (1) the adequacy of the proposed language about reasonable notice in cases in which a computer is affected by a botnet and the government has obtained a warrant to obtain the IP address, and (2) whether the "concealing" language could be applied more broadly to scenarios beyond those envisioned by the Committee. He also hoped that at the hearing commenters would expand on their concerns about applications of the Computer Fraud and Abuse Act. Professor Kerr observed that although the Justice Department's original proposal had been narrowed considerably by the Committee in the published rule, some of the comments appeared to address the original proposal, not the published rule, or were raising concerns to remote access searches generally. Commenters generally assume that the Committee has approved remote access searches, but the amendment does not do so.

Judge Raggi then asked the Department of Justice member for his views. She noted for the Committee that she had discouraged the Department of Justice from filing a written response to each critical public comment received, urging it to do so only after the November hearing.

Mr. Wroblewski stated that the government acknowledges commenters' legitimate concerns about particularity, nature of entry, ability to find vendors, nature of the procedure, and delayed notice. But those concerns are not implicated by the proposed rule, which only establishes venue. On the question of notice, he indicated that the government provides notice electronically, which when it has only an IP address, is all it can possibly do. He indicated that the government may still have to struggle with notice issues. He also acknowledged that some cases may raise Title III issues. But he noted that a well-established process exists for dealing with these issues if they arise. The government is not trying to avoid those issues, but they are

not part of this proposal. Most of the comments presented interesting questions about the use of various techniques; the use of these techniques is also not really raised by the proposed rule amendment.

A member asked about the Electronic Communications Privacy Act (ECPA), referenced by some commenters. Professor Kerr responded that the ECPA regulates access to remotely stored information, text messages, email, and cloud data. The original proposal presented a possible conflict with the statute because it might have allowed government to go around the provider and, instead, access email accounts directly. But the narrower published rule poses no such concern. If the government does not know where the data is located, the search would not involve data known to be controlled by the provider, so it could not use the ECPA process. And the second prong of the proposed amendment applies to damaged computers.

Professor Beale stated that some of the comments seemed not to understand that the proposed venue amendment did not relieve the government of its constitutional obligation to demonstrate probable cause for a warrant regardless of venue. Thus, the use of technology such as virtual private networks (VPNs) would not support a remote search under the proposed amendment absent probable cause.

Responding to some commenters' concerns that, when a company uses a VPN, the government could get remote access warrant without endeavoring to determine the location of the server, Professor Kerr suggested that the concern was not likely to be a significant issue in practice because it would be easier to find the server location than to do a remote search under the proposed amendment.

Professor Beale added that commenters had also raised concerns about the possible extraterritorial application of warrants issued under the published rule. Is it predictable that the computers to be searched will be outside the U.S.? If so, would this violate MLATs specifically or international law generally? If the foreign country in which the computer is located defines unauthorized access as a crime, could agents carrying out the remote search be charged with crimes by those countries?

Judge Raggi asked whether the government expected to advise United States judges of the possibility that a remote access search could reach beyond this country's borders.

Professor Beale noted that commenters' concern about collateral damage to non-targets, for example, in "watering hole" operations. Might the government exploit vulnerabilities in security protections, affecting computers networked to target computers?

A member observed that these and other concerns about do not seem to be generated by the proposed rule amendment itself, but from a concern that the amendment would increase the likelihood techniques having such effects would be used. In sum, the problems already exist, but the concern is that an amendment would exacerbate them.

Professor Beale also noted that although the proposed rule authorizes searches but not remediation, the government may want to do more than just search. The amendment may make it possible for government to do this in a greater number of cases.

Professor King noted that other rule amendments had established procedures for government conduct whose constitutionality had not yet been conclusively determined. For example, Rule 15 establishes procedures for depositions outside the U.S. where the defendant is not present, even though the admissibility of such a deposition at trial is not established under the Confrontation Clause. Rule 11 requires advice about appellate waivers that might not be deemed valid. Rule 41 established procedures for tracking devices, though at the time of the amendment it was unsettled whether such installations constituted searches subject to the Fourth Amendment. So there are some precedents for the Committee approving a rule of procedure for a process whose constitutionality is not yet settled.

A member noted that the examples just cited were distinguishable in that injury depended on later action (such as the admission of evidence). The injury of concern in the published rule would occur when the search and seizure authorized by the judge in the alternate venue occurs.

Another member noted that the details needed to address the myriad concerns identified by commenters may be more than a procedural rule can handle. But such detail is not needed if we are not attempting to legitimate remote access searches, but merely to provide a procedural framework addressing venue. This might even provoke legislative activity on the larger issues. Perhaps this could be made clearer by having the proposed rule say something such as “a magistrate can issue extraterritorial warrant according to law.”

A member suggested that the Committee Note might flag issues raised by commenters, and note that the Committee is not taking any position on them.

Professor Beale responded that the Standing Committee does not want elaborate Committee Notes and generally discourages the citation of cases therein. But she agreed the Committee should be as clear as possible in communicating that the amendment does not foreclose or prejudge any constitutional challenges to remote access searches.

Professor Coquillette added that the philosophy has always been to have each Advisory Committee draft the best rule possible and let the Standing Committee worry about reactions from Congress or the Supreme Court. The Standing Committee has adopted new procedures for previewing rules amendments for the Supreme Court in advance of formal approval by the Judicial Conference, thereby giving the Court more time to consider amendments. He noted two rules philosophies on the Court. One views the Court’s promulgation of a rule as a signal of its general constitutionality. The other views promulgation as simply sending the rule forth for application and review on a case-by-case basis. Professor Coquillette observed that the Court now seems to want unanimity on rules it approves. In short, one justice’s reservations can defeat a rule.

Draft Minutes
Criminal Rules Meeting
November 4-5, 2014
Page 17

Professor Beale agreed that although, in the past, some rules were adopted over a justice's dissent, the Supreme Court now generally approves proposed rules only by consensus.

Members agreed on the need for clarity in the Committee Notes. One emphasized the need to disavow any assessment of constitutional issues. Another noted that the Committee may be underestimating the concern about privacy, and public confusion about what the rule does and does not do. The Committee Note needs to make it clear what we are and are not doing.

At the conclusion of this discussion, the meeting adjourned for the day, with the Committee to reconvene on November 5 for public hearings, which were transcribed separately.

Judge Raggi announced that the next regular meeting of the Committee would take place on March 15-16, 2015 at the federal courthouse in Orlando, Florida.

TAB 1E

COMMITTEE ON RULES OF PRACTICE AND PROCEDURE

Meeting of January 8–9, 2015

Phoenix, Arizona

Draft Minutes

TABLE OF CONTENTS

Attendance	1
Introductory Remarks	2
Approval of the Minutes of the Last Meeting	3
Report of the Appellate Rules Advisory Committee	3
Report of the Bankruptcy Rules Advisory Committee	4
Report of the CM/ECF Subcommittee	6
Report of the Administrative Office	7
Report of the Criminal Rules Advisory Committee	8
Report of the Civil Rules Advisory Committee	10
Report of the Evidence Rules Advisory Committee	12
Concluding Remarks	13
Promoting Judicial Education Through Videos	13
Panel Discussion on the Creation of Pilot Projects	14
Next Committee Meeting	18

ATTENDANCE

The winter meeting of the Judicial Conference Committee on Rules of Practice and Procedure was held in Phoenix, Arizona, on January 8 and 9, 2015. The following members were present:

Judge Jeffrey S. Sutton, Chair
Dean C. Colson, Esquire
Associate Justice Brent E. Dickson
Roy T. Englert, Jr., Esquire
Gregory G. Garre, Esquire
Judge Neil M. Gorsuch
Judge Susan P. Graber
Dean David F. Levi
Judge Patrick J. Schiltz
Judge Amy J. St. Eve
Judge Richard C. Wesley
Judge Jack Zouhary

Elizabeth J. Shapiro, Esq., represented the Department of Justice in place of Deputy Attorney General James M. Cole. Larry D. Thompson, Esq., was unable to attend.

Also present were Professor Geoffrey C. Hazard, Jr., consultant to the committee; Professor R. Joseph Kimble, the committee's style consultant; and Judge Jeremy D. Fogel, director of the Federal Judicial Center. Judge Anthony J. Scirica, Judge Sidney A. Fitzwater, and Judge Eugene R. Wedoff participated in a panel discussion chaired by Judge Sutton. Associate Justice Sandra Day O'Connor attended as an observer.

The advisory committees were represented by:

Advisory Committee on Appellate Rules —
Judge Steven M. Colloton, Chair
Professor Catherine T. Struve, Reporter (tel)

Advisory Committee on Bankruptcy Rules —
Judge Sandra Segal Ikuta, Chair
Professor S. Elizabeth Gibson, Reporter
Professor Troy A. McKenzie, Associate Reporter

Advisory Committee on Civil Rules —
Judge David G. Campbell, Chair
Professor Edward H. Cooper, Reporter
Professor Richard L. Marcus, Associate Reporter

Advisory Committee on Appellate Rules —
Judge Reena Raggi, Chair
Professor Sara Sun Beale, Reporter (tel)

Advisory Committee on Evidence Rules —
Judge William K. Sessions III, Chair
Professor Daniel J. Capra, Reporter (tel)

Subcommittee on CM/ECF
Judge Michael A. Chagares, Chair

The committee's support staff consisted of:

Professor Daniel R. Coquillette	Reporter, Standing Committee
Jonathan C. Rose	Secretary, Standing Committee; Rules Committee Officer
Julie Wilson	Attorney, Rules Committee Support Staff (tel)
Scott Myers	Attorney, Rules Committee Support Staff (tel)
Bridget M. Healy	Attorney, Rules Committee Support Staff (tel)
Andrea L. Kuperman	Chief Counsel to the Rules Committee
Frances F. Skillman	Rules Office Paralegal Specialist
Toni Loftin	Rules Office Administrative Specialist
Michael Shih	Law Clerk to Judge Jeffrey S. Sutton

INTRODUCTORY REMARKS

Judge Sutton called the meeting to order by thanking the Rules Office staff and the marshals for their service. He introduced one new member of the Committee, Associate Justice Brent E. Dickson of the Indiana Supreme Court. He also introduced Judge Sandra Segal Ikuta of the Ninth Circuit, the new chair of the Bankruptcy Committee, and Judge William K. Sessions III of the District of Vermont, the new chair of the Evidence Committee. Finally, he introduced Judge Anthony Scirica of the Third Circuit, who helped coordinate the afternoon's panel discussion on pilot projects.

He then summarized the results of the September 2014 Judicial Conference, which unanimously approved both the Bankruptcy Committee's one proposal and the entire Duke Package. The proposed amendments are now before the Supreme Court of the United States.

Finally, Judge Sutton announced that, on December 1, 2014, many other proposals took effect, including Criminal Rule 12 and a multitude of changes to the Bankruptcy Rules and Forms. He thanked Judge Raggi and Judge Wedoff for their efforts in making those proposals law.

APPROVAL OF THE MINUTES OF THE LAST MEETING

The Committee, by voice vote and without objection, approved the minutes of its previous meeting, held on May 29–30, 2014, as well as a set of technical amendments to those minutes proposed by Professor Cooper.

REPORT OF THE ADVISORY COMMITTEE ON APPELLATE RULES

Judge Colloton presented the advisory committee's report, set out in his memorandum and attachments of December 15, 2014 (Agenda Item 3). He reported that the committee has published a package of rules changes for public comment. It plans to consider those comments after the February deadline expires, and to give a complete report at the upcoming spring meeting. He then highlighted three items currently on the committee's agenda.

Informational Items

FED. R. APP. P. 41

The advisory committee is considering how to relieve the tension between two provisions of Appellate Rule 41. Rule 41(d)(2) requires a court of appeals to issue its mandate immediately after the Supreme Court denies a petition for certiorari. However, Rule 41(b) allows courts of appeals to "extend the time" for issuing mandates under certain circumstances. These provisions present two questions. May a court of appeals stay its mandate after certiorari is denied? If so, must it do so in an order, or does mere inaction suffice?

The Supreme Court has twice considered these questions. As to the first issue, it has assumed without deciding that a court of appeals has authority to delay issuing a mandate, but

only if “extraordinary circumstances” exist. As to the second, it has concluded that Rule 41(b) does not clearly foreclose delay through inaction.

Judge Colloton reported that the committee is inclined to insert the words “by order” into Rule 41(b) to clarify that a court of appeals may not delay a mandate by letting the matter lie fallow. (Those words had actually been removed from a previous version of the Rule, most likely to reduce redundancy). However, it is still working through the more fundamental question of whether such authority exists. It has considered reaffirming what Rule 41(d)(2) already appears to say: A mandate must issue immediately after certiorari is denied. But if appellate courts retain authority to recall an already-issued mandate under extraordinary circumstances, any change to Rule 41(d)(2) would serve little purpose. It thus might make more sense to codify the “extraordinary circumstances” rule. In either case, the committee will make a formal proposal to the Standing Committee, perhaps as early as the spring meeting.

DISCLOSURE RULES

The advisory committee has been considering what disclosures parties must make in briefs for a long time. Its review revealed a bevy of local disclosure requirements that augment the Appellate Rules to different degrees. Concerned that the Rules are insufficiently thorough, the committee is considering expanding their scope: for example, by extending them to intervenors, partnerships, victims in criminal cases, and amici curiae. It is also consulting the Committee on Codes of Conduct for additional guidance. Judge Colloton reported that, because the project remains ongoing, the committee may or may not be able to present a concrete proposal at the spring meeting.

One member proposed that, instead of taking the lead, the Appellate Committee should coordinate with judges at all levels of the federal judiciary. Another suggested that the Appellate Committee coordinate with its sister advisory committees, all of which have an interest in the outcome. In response, Judge Colloton noted that the project was still in a nascent stage and expressed willingness to solicit input from other committees once it had crystallized its thinking.

CM/ECF PROPOSALS

The advisory committee has been working with Judge Chagares and the CM/ECF subcommittee to resolve issues related to electronic filing. Judge Colloton deferred consideration of those issues to Judge Chagares’s presentation.

REPORT OF THE ADVISORY COMMITTEE ON BANKRUPTCY RULES

Judge Ikuta presented the advisory committee’s report, set out in her memorandum and attachments of December 11, 2014 (Agenda Item 4).

Amendment for Final Approval

FED. R. BANKR. P. 1001

On behalf of the advisory committee, Judge Ikuta sought approval to amend Bankruptcy Rule 1001, the bankruptcy counterpart to Civil Rule 1. Rather than incorporate the Civil Rule by reference, the Bankruptcy Rule echoes its language. However, Rule 1001 does not reflect recent amendments—approved and pending—to Rule 1. The proposal brings Rule 1001 in line with those changes, stating that “These rules shall be construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every case and proceeding.”

The committee, without objection and by voice vote, approved the proposed amendment to Rule 1001 for publication.

Informational Items

PROPOSED CHAPTER 13 NATIONAL PLAN FORM

The advisory committee has been working on a national chapter 13 plan form since 2011. Currently, more than a hundred chapter 13 forms exist. Led by Judge Wedoff, the committee distilled those forms into one. It also developed amendments to the Bankruptcy Rules to bring them in line with that form. After publishing the first version of the form and amendments in 2013, the committee received many critical comments. So it went back to the drawing board and published a revised proposal in 2014. The comment period has not yet expired, but the reaction to the revisions has been mixed.

Judge Ikuta reported that, in her view, the committee can fix specific concerns about the form. The real question is whether the need for national uniformity should override local preferences. She recommends implementing the national form incrementally—for instance, by making the form optional and asking various bankruptcy districts to opt into the form.

A professor wondered whether it was possible to make the national form an alternative to local ones. Judge Ikuta confirmed that his question tracked the committee’s proposed incremental approach. By making the national form optional and soliciting compliance from individual districts, the committee hoped to build support for it over time.

An appellate judge asked why a national form was necessary. Professor McKenzie gave four reasons. First, the existing forms have generated a tremendous amount of confusion. Second, bankruptcy judges have an independent duty to scrutinize proposed plans, and a national form would reduce uncertainty about where such information may be found. Third, a national form could generate data more effectively. Finally, a national form would let entrepreneurs develop cheaper software for debtors’ use.

Judge Wedoff explained why the committee decided to devise a national form in the first place. One bankruptcy judge said that, in the form’s absence, bankruptcy courts could not easily

discharge their duty to independently scrutinize chapter 13 plans. And a bankruptcy lawyers' association said that its members had trouble processing chapter 13 forms from different jurisdictions—and lacked the resources to obtain local counsel. Professor McKenzie added that the committee surveyed the chief judge of every bankruptcy court in the country before getting the project started. The response was overwhelmingly positive.

A district judge asked about the reaction from bankruptcy practitioners. Their comments, Professor McKenzie said, were mixed. Some lawyers liked the idea so long as this word or that word could be changed. Others opposed it. A few lawyers candidly explained that they feared the competition an easily accessible national form would create.

FORMS MODERNIZATION PROJECT

The advisory committee's forms modernization project is almost complete. Unfortunately, the Administrative Office is having trouble integrating the new forms into its new CM/ECF system and may miss its December 2015 deadline—when the forms are scheduled to take effect. The question is whether to delay rolling out the forms until all technological kinks have been ironed out.

Judge Ikuta reported that the committee will discuss the issue at its April meeting, but she recommends releasing the forms on schedule. Doing so, she said, would not disrupt operations in the vast majority of courts. True, three bankruptcy districts give pro se debtors access to forms software on court-run computer terminals. But not enough debtors use that service to justify delaying the forms' national release.

A district judge said that the AO had told her that forms integration was mutually exclusive with the CM upgrade project. As it turns out, Judge Ikuta received that same answer too, but the AO changed its mind once it realized what the forms integration project entailed.

CM/ECF PROPOSALS

The advisory committee considered three of the CM/ECF subcommittee's proposals at its fall meeting. It will defer decision on two of them until the Civil Rules Committee acts. It is independently considering whether to redefine the word "information" to include electronic documents and the word "action" to include electronic action.

REPORT OF THE INTER-COMMITTEE CM/ECF SUBCOMMITTEE

Judge Chagares presented the subcommittee's report, set out in his memorandum and attachments of November 30, 2014 (Agenda Item 8). He announced that the subcommittee had successfully completed its work.

Informational Items

ABROGATION OF THE THREE-DAY RULE AS APPLIED TO ELECTRONIC SERVICE

The subcommittee previously proposed that parties should not receive three extra days to take action after electronic service. It worked with the relevant advisory committees to draft amendments to Appellate Rule 26(c), Bankruptcy Rule 9006, Civil Rule 6, and Criminal Rule 45. These amendments, Judge Chagares reported, thus far have been well received.

ELECTRONIC SIGNATURES

The subcommittee previously proposed that Bankruptcy Rule 5005 be changed to provide for more flexible electronic signatures, but the Bankruptcy Committee withdrew that proposed amendment after public comment. After that withdrawal, the subcommittee asked the Administrative Office to figure out how local rules treated electronic signatures. Judge Chagares thanked the AO for its diligence and hard work.

The AO's exhaustive survey revealed that nearly every local rule treats filing users' login and password as an electronic signature. The various districts are not nearly so uniform when it comes to nonfilers, but the most prevalent rule requires the user to obtain and retain the signatory's ink signature. In light of these findings, Judge Chagares concluded, the Bankruptcy Committee's decision was probably correct. The local rules appeared sufficient to meet present needs, and any formal rulemaking risked being overtaken by rapid technological developments.

CIVIL AND CRIMINAL RULES REQUIRING ELECTRONIC FILING

The subcommittee previously recommended that Civil Rule 5(d)(3) and Criminal Rule 49(e) be amended to mandate electronic filing as opposed to merely permitting it. Judge Chagares reported that the advisory committees are still considering those proposals.

UNIFORM AMENDMENTS TO ACCOMMODATE ELECTRONIC FILING AND INFORMATION

The current rules do not appear to accommodate electronic filing and information. Thus, the subcommittee proposed defining "information" to include electronic documents and "action" to include electronic action. The advisory committees considered these proposals but reached different conclusions. For example, the Appellate and Civil Rules Committees have decided not to adopt them, while the Bankruptcy and Criminal Rules Committees have submitted them to subcommittees for further study. Judge Chagares reported that the proposal to redefine "information" appears to be the more viable of the two.

Dissolution of the Subcommittee

Judge Sutton thanked Judge Chagares, Professor Capra, Julie Wilson, and Bridget Healy for their hard work, and praised the subcommittee for fulfilling its mandate quickly and efficiently. Professor Capra reiterated Judge Sutton's comments and thanked his fellow reporters.

Judge Sutton and Judge Chagares have agreed that, now that the subcommittee has run its course, there is no need to keep it in place.

REPORT OF THE ADMINISTRATIVE OFFICE

Mr. Rose presented the Administrative Office's report (Agenda Item 10).

Informational Items

The Administrative Office is preparing an updated version of its 2010 *Strategic Plan for the Federal Judiciary*. Because the Long-Range Planning Committee will be meeting in March, Mr. Rose noted, the time for input is now.

Mr. Rose asked anybody corresponding with the Office to copy both the head of the Rules Office and Frances Skillman. That, he said, is the best way to ensure the message gets where it needs to go. He also summarized recent personnel arrivals and departures at the AO.

Finally, Mr. Rose announced that this meeting would be his last as head of the Rules Office. He thanked the committee for the opportunity to work with and learn from such talented people. Judge Sutton thanked Mr. Rose for his leadership and lauded his commitment to public service over a long and distinguished career. He also introduced Rebecca Womeldorf, Mr. Rose's successor, and described her impressive background.

REPORT OF THE ADVISORY COMMITTEE ON CRIMINAL RULES

Judge Raggi presented the advisory committee's report, set out in her memorandum and attachments of December 11, 2014 (Agenda Item 6). She announced that the amendments to Criminal Rule 12 have now taken effect.

Informational Items

FED. R. CRIM. P. 4

The Standing Committee previously approved for comment a proposed amendment to Rule 4 that would govern service of process abroad. Judge Raggi reported that the advisory committee has received no critical feedback on that proposal.

FED. R. CRIM. P. 41

The Standing Committee previously approved for comment a proposed amendment to Rule 41 to govern venue for searches of electronic devices whose location is unknown. The advisory committee held a lengthy hearing and reviewed extensive public comments. Judge Raggi reported that the critical response has largely focused not on the amendment itself but on concerns about electronic searches more generally.

These thought-provoking comments led the committee to request a response from the U.S. Department of Justice. The Department endorsed the proposal and suggested ways for the government to satisfy the particularity requirement if the amendment takes effect. Judge Raggi noted that the Federal Judicial Center might consider educating judges about how to analyze such warrant applications down the road. But that, she concluded, is a question for later. For now, the committee is debating whether the amendment needs to be changed. Judge Raggi expects the committee to propose something at the spring meeting, although the current proposal may be tweaked.

SUGGESTED AMENDMENT TO RULE 52

A Second Circuit judge asked the advisory committee to consider amending Rule 52 to provide fresh review—as opposed to plain-error review—for defaulted sentencing errors. He reasoned that, unlike a new trial, a resentencing proceeding imposes an incidental burden on the judiciary. And it is unfortunate when a prisoner is forced to remain in jail longer than he deserves.

Judge Raggi reported that the committee decided not to proceed with this request. Professor Nancy King, the committee's associate reporter, surveyed cases in this area and discovered that the number of defaulted sentencing errors is not high—and were typically corrected on plain-error review. The committee was also concerned that the proposal would generate extensive frivolous litigation. Finally, drawing on its experience with the 2014 Rule 12 amendments, it expressed doubts that the Supreme Court would be willing to create an exception to the general rule that defaulted claims are reviewed for plain error.

One appellate judge proposed an alternative. He suggested that the rules might be amended to reflect what many circuits have already held: that a clear guidelines-calculation error presumptively satisfies the last two elements of plain-error review. The judge acknowledged, however, that his suggestion came close to the edge of the committee's rulemaking authority. Another appellate judge wondered whether a different approach might solve the problem. In his circuit, a defendant can never forfeit a substantive reasonableness challenge, so arguments that a sentence is unjustly long are always reviewed afresh. Judge Raggi responded that, in her view, no judge should ever rely on the guidelines unless that sentence also satisfies the § 3553 factors. Plain-error review is enough to fix the vast majority of problems, and loosening Rule 52's standards would open the floodgates to a host of defaulted sentencing claims. She suggested instead that circuits interested in these alternative proposals adopt them as a local rule or as circuit-specific precedent.

FED. R. CRIM. P. 11

The judges of the Northern District of California asked the advisory committee to let judges refer criminal cases to their colleagues to explore the possibility of a plea bargain. Judges in that district had routinely used this procedure until the Supreme Court held that the Criminal Rules barred it.

Judge Raggi reported that the committee decided not to proceed with this request either. 95% of criminal cases are already resolved by plea bargains nationally, and the Northern District is no exception to that norm. More, implementing this change would create a host of practical problems—and might raise separation-of-powers concerns to boot.

Judge Raggi also reported that, at around the same time, a judge from the Southern District of New York published an article advocating judicial involvement in plea bargaining to reduce the risk that someone would plead guilty to a crime he didn't commit. The committee was not persuaded by this argument either. If a district judge is not convinced that a defendant is guilty of the crime to which he pleaded guilty, the judge should reject that plea under Criminal Rule 11.

HABEAS RULE 5

A judge from the Eastern District of Pennsylvania asked the advisory committee to amend Habeas Rule 5. Currently, that Rule requires a State to give a habeas petitioner copies of all exhibits attached to its response. The judge proposed relieving the State of that obligation in the absence of a judicial order to the contrary.

Judge Raggi reported that the advisory committee unanimously rejected this proposal. Every court expects these documents to be provided, and the States themselves have not complained about the problem.

FED. R. CRIM. P. 35

The New York Council of Defense Attorneys asked the committee to grant judges authority to reduce a sentence if (1) the defendant can identify new evidence casting doubt on his conviction, (2) the defendant can show he has been fully rehabilitated, or (3) the defendant can point to medical problems justifying his release.

Judge Raggi reported that a subcommittee is still examining this proposal, but she thinks it will not ultimately succeed. Proposal 1 effectively repeals AEDPA's statutory time limits on presenting such evidence in a habeas petition. Proposal 2 would subject the courts to a flood of rehabilitation claims. And Proposal 3 is redundant, since prisoners can already be released on humanitarian grounds when appropriate.

REPORT OF THE ADVISORY COMMITTEE ON CIVIL RULES

Judge Campbell presented the advisory committee's report, set out in his memorandum and attachments of December 2, 2014 (Agenda Item 5).

Informational Items

CM/ECF PROPOSALS

Judge Campbell reported that the advisory committee has finished considering the CM/ECF Subcommittee's proposals. It recommended that the Civil Rules mandate electronic filing and service with appropriate exceptions for good cause. It recommended against changing the Rules' approach to electronic signatures, having observed the Bankruptcy Rules Committee's experience. It also recommended against defining "information" or "action" to include "electrons" (e.g., electronic filing), although it remains open to making that change if the existing regime becomes unworkable.

FED. R. CIV. P. 68

The advisory committee considered several proposals to amend Civil Rule 68, which governs offers of judgment. The committee has studied the Rule twice in the last two decades, and it provoked a storm of controversy both times. Nevertheless, Judge Campbell reported that the committee is once again looking at the question—this time by surveying how the States implement their own offer-of-judgment procedures. The committee will consider next steps at its April meeting.

FED. R. CIV. P. 26

The advisory committee considered a proposal to add the presence of third-party litigation financing to the list of Civil Rule 26(a) disclosures. The committee agreed that the issue is important but determined that rulemaking is not yet appropriate. Litigation finance is a relatively new field. Besides, judges already have tools to obtain this information when relevant. And the absence of a mandatory-disclosure rule does not appear to hinder the resolution of cases involving litigation financiers.

FED. R. CIV. P. 23 SUBCOMMITTEE ACTIVITY

The advisory committee appointed a subcommittee to consider issues related to Civil Rule 23. Currently, it is charged with gathering facts to identify questions worth further study. So far, Judge Campbell reported, the subcommittee has spotted six primary issues. It plans to present a set of conceptual proposals to the full committee at its April meeting that may generate more concrete proposals for the fall. It is also considering convening a mini-conference in 2016 to evaluate any suggestions that might emerge.

One member asked the subcommittee to examine the procedures governing multidistrict litigation. He said that mass-tort MDLs make up half the federal courts' civil docket, and the rules regulating them may be worth reexamining. He also observed that the MDL bar is a small and tightly knit group of lawyers with links to the MDL Panel. None of this is to say that MDLs are being mishandled. But because MDLs occupy such a large part of the civil system, the subcommittee ought to ensure that the process is working.

Two members responded that, judging from their past experience with the subject, they doubted whether Rule 23—and for that matter the Rule 23 subcommittee—was the best place to address any problems MDLs might pose. Two judges who have presided over MDL cases also expressed their doubts. One reported that, in his experience, the MDL process *was* working. The other reported hearing complaints about the system, but those focused more on the process of MDL certification and counsel selection than on the process of trying MDL cases once certified. Both questioned whether a one-size-fits-all approach was possible or desirable. Finally, a practitioner pointed out that a small bar is an efficient bar. MDL trial firms get along with MDL defense firms, so MDL cases tend to run smoothly. And from most firms' perspective, the cost of entering the MDL arena is prohibitively high, making MDL cases poor investments.

REPORT OF THE ADVISORY COMMITTEE ON EVIDENCE RULES

Judge Sessions presented the advisory committee's report, set out in his memorandum and attachments of November 15, 2014 (Agenda Item 7). The committee considered proposals developed from its April 2014 Symposium on the Challenges of Electronic Evidence. The *Fordham Law Review* has published the proceedings from that Symposium.

Informational Items

FED. R. EVID. 803(16)

Evidence Rule 803(16) provides a hearsay exception for authenticated documents over twenty years old. Judge Sessions reported that this Rule has almost never been used, but it may become more significant in an era of electronic evidence. The advisory committee thinks this Rule is inappropriate but is still deciding what to do about it. One option is to leave it be. Another is to abrogate it or narrow it to exclude electronically stored information. Still another is to amend it to require a showing of necessity or reliability.

RECENT PERCEPTIONS

The advisory committee considered whether to add a new hearsay exception for electronically reported recent perceptions to Evidence Rules 801(d)(1) and 804(b). This change would arguably prevent reliable statements made in texts, tweets, and Facebook posts from being excluded.

Judge Sessions reported that the committee is continuing to study whether these changes are necessary. With respect to Rule 801(d)(1), the committee has decided not to change that provision without first asking whether prior statements of testifying witnesses should even be defined as hearsay. It will begin that study at its next meeting. With respect to Rule 804(b), the committee is continuing to monitor the caselaw to see if courts have actually been excluding reliable evidence of this sort. A district judge asked the committee to study whether a witness's prior statement should be treated as hearsay when that witness is available to testify. Professor Capra responded that such a rule might open the door to all prior consistent statements.

STANDARDS FOR AUTHENTICATING ELECTRONIC EVIDENCE

The advisory committee considered whether to amend Evidence Rules 901 and 902 to provide specific grounds for authenticating electronic evidence. Judge Sessions reported that, in the committee's view, devising authentication standards against a rapidly changing technological backdrop would create more problems than they would solve. However, it unanimously decided to develop a best-practices manual to guide courts and litigants.

FED. R. EVID. 902

The advisory committee considered two proposals to make it easier for litigants to authenticate certain kinds of electronic evidence. They mirror the self-authentication procedure for business records in Evidence Rule 902(11) by shifting the burden for proving inadmissibility to the opposing party. Judge Sessions reported that the committee unanimously supports these proposals and will consider introducing them as formal amendments at its next meeting.

CONCLUDING REMARKS

Judge Sutton concluded this portion of the meeting by recognizing four departing individuals for their service: Jonathan Rose, Andrea Kuperman, Judge Sidney Fitzwater, and Judge Eugene Wedoff. He summarized their remarkable achievements and thanked them all for their tremendous work on the committee's behalf.

PROMOTING JUDICIAL EDUCATION THROUGH VIDEOS

The committee considered the Federal Judicial Center's proposal to produce videos that would educate judges and lawyers about changes to the Federal Rules. Judge Sutton explained how the proposal came to be. Education has always been a key component of the Duke Package, which was designed in part to change the culture of civil litigation. Judge Fogel came up with the idea of disseminating information through video presentations. Initially, the FJC planned to create test videos for all of the rules that took effect in December 2014. However, the committee expressed concern that such videos—if released to the public—would constitute a form of post-enactment legislative history. So it postponed a final decision on the FJC's proposal until it could review a sample video.

Judge Fogel showed a sample film featuring Judge Sessions and Professor Capra, who discussed recent amendments to Evidence Rules 801 and 803. He acknowledged concerns about post-enactment legislative history but argued that the video format was a much more dynamic way to communicate information. He also explained that the videos would reach a wide audience even if restricted to judges and judicial employees. For example, a thousand viewers watched a recent webinar on § 1983 litigation.

Many members supported the FJC proposal. The Duke Package depends on education for its success, and videos might help reach previously inaccessible constituencies. Several judges recommended presenting the videos to their law clerks and at judicial meetings both private and

public. As for the legislative-history concern, that issue can be solved with a disclaimer—or a rule that no such video could be used in court.

One appellate judge expressed reservations. He argued that the written word is superior to video in conveying this sort of information. In response, a member proposed releasing the transcript of the video with the video itself. Another member suggested that the videos might be more useful if they provided practice tips. This triggered concerns that expanding the videos beyond the text of the committee notes would stretch the bounds of proper rulemaking.

Judge Sutton recommended that the FJC proceed slowly. He asked it to work with any committee chairs and reporters willing to produce videos describing significant rule changes that took effect in December 2014. Those videos would be then placed on the private judicial intranet. The committee could then use that experience to determine whether to continue the program and whether to make the videos public. He thanked Judge Fogel, Judge Sessions, and Professor Capra for putting together the demonstration video.

PANEL DISCUSSION ON THE CREATION OF PILOT PROJECTS

Introduction

Judge Sutton presided over a panel discussion on the creation of pilot projects to facilitate civil discovery reform. When coupled with the Duke Package reforms, pilot projects offer a powerful way to change litigation norms for the better and to gather data for future reforms in the process. By convening the panel, he hoped to give the Civil Rules Committee some potential projects to consider. Judge Sutton introduced the panelists: Judge Eugene Wedoff of the Bankruptcy Court for the Northern District of Illinois, Judge Anthony Scirica of the Third Circuit, and Judge Sidney Fitzwater of the Northern District of Texas. Finally, he welcomed a special guest: Associate Justice Sandra Day O'Connor, who joined the Standing Committee for this panel discussion and for the dinner that followed.

Judge Wedoff: Improving the Speed of Case Administration

PRESENTATION

Judge Wedoff spoke about the impact of “rocket dockets” on case administration. The term was first applied to the Eastern District of Virginia, which implemented a series of procedural reforms in the 1970s. It has since been applied to several other jurisdictions that have adopted similar procedures, including the Western District of Wisconsin and the Eastern District of Texas. But their reputations sometimes do not match the data. The Eastern District of Virginia is truly one of the fastest courts in the country—but the Eastern District of Texas operates *above* the nation’s median case disposition time, and the Western District of Wisconsin has fallen off substantially. Meanwhile the Southern District of Florida works with remarkable speed despite not being labeled a rocket-docket court.

Based on this study, Judge Wedoff concluded that judges affect case-disposition time more powerfully than rules. Judges who impose credible deadlines, for example, resolve cases

faster than judges who don't. At the same time, efficient districts have certain procedural rules in common. For example, the Eastern District of Virginia sets short deadlines for discovery and trial that cannot be altered without a substantial showing to the court. For its part, the Southern District of Florida places every case into one of three tranches: expedited, standard, and complex. None of these tranches allows discovery to exceed one year.

DISCUSSION

The first question is whether to encourage district courts to adopt rocket-docket procedures district-wide. Many members said yes. Competition for litigants among courts can help everyone, said one professor, pointing to the creation of an omnibus hearing as an example of a useful procedural innovation that arose from one bankruptcy district's attempt to entice debtors to file there. Other committee members observed that, even if rocket-docket procedures make things harder for lawyers and judges, such procedures are *always* good for clients. And pilot projects implementing them may well change attorneys' hearts and minds in the process.

Attendees made several suggestions about what such pilot projects might look like. One recommended setting hard and credible trial deadlines. Another recommended capping not only a party's total deposition hours but also the number of hours he has available to conduct each deposition. He also recommended creating a tranches system for document production. And everybody who spoke emphasized the importance of making the pilot project mandatory.

The committee then moved to the question of implementation. Certain rocket-docket procedures—like the Eastern District of Virginia's weekly argument day—might conflict with local rules mandating one judge per case. More fundamentally, creating a rocket docket from scratch would be much harder than studying the ones that already exist, since district courts are unlikely to change in the absence of a strong leader backing the project.

One member counseled against implementing pilot projects too quickly. He recommended letting the FJC study the existing projects first, and moving only when the committee was sure that the projects' contents would work. Judge Sutton responded that he saw no reason why pilot-project advocacy should stop—especially since such advocacy isn't designed to mandate effective procedures but to suggest potentially useful ones. Another member agreed, and pointed out that studies and pilot projects could always take place simultaneously.

Finally, members sounded a note of caution about research methodology. One stressed the importance of getting independent opinions from participants, recalling an instance where rocket-docket practitioners were asked about their views on the process in full view of rocket-docket judges. Two district judges reiterated that numbers do not tell the whole story. Sometimes a case gets delayed for wholly appropriate reasons. And sometimes statistics are skewed by background factors not immediately apparent.

Judge Scirica: Requiring Initial Disclosure of Unfavorable Material

PRESENTATION

Judge Scirica explored the feasibility of requiring parties to disclose material unfavorable to their side by rule. In the 1990s, he said, the committee tried to do just that, but the proposal triggered a firestorm. Opponents argued that most cases did not require adverse disclosures, and that aggressive discovery techniques would ferret out such information in the cases that did. They also invoked the adversarial nature of the American justice system, arguing that a “civil *Brady* regime” would disrupt the attorney-client relationship. Eventually, the committee settled on a compromise position—explored through pilot projects in the Central District of California and the Northern District of Alabama—that retained initial disclosures but eliminated the requirement to disclose unfavorable material.

Today, Judge Scirica continued, an expanded initial disclosure regime might find a warmer reception. To test the waters, he envisioned two separate types of pilot projects. One would apply a robust but general initial disclosure regime to all civil cases. Another would apply a tailored initial disclosure requirement to certain categories of cases—say, employment discrimination or civil rights. The former is best left to the Standing and Civil Rules Committee, he advised; the latter, to a committee of experienced lawyers from both sides of the podium.

DISCUSSION

Every member who spoke expressed support for an expanded initial disclosure regime. One provided an especially powerful example from Arizona. In 1991, the Arizona Supreme Court adopted a robust mandatory disclosure rule that covered favorable and unfavorable material. The same debate took place. Now, however, Arizona’s local rules have overwhelming support. In fact, seventy percent of lawyers who practice in both federal and Arizona state court prefer the state disclosure system to the federal one.

Another speaker, who served on the committee during its first attempt to mandate adverse disclosures, argued that the committee should not be traumatized by that experience. The committee, he said, had been right all along. And this time, it knows what pitfalls to avoid. For example, it will not keep the bar in the dark until the very end of the process.

The committee also endorsed category-specific disclosures. Many district judges have already embraced the Federal Initial Discovery Protocols for Employment Cases. One member reported that, although the Protocols encountered initial resistance, the employment bar now loves them because they generate information that would otherwise require a six- to seven-month discovery battle to get. Another member explained that the Southern District of New York had successfully implemented similar protocols for § 1983 cases that helped clear out its cluttered docket. One district judge advised the committee to make sure it doesn’t define categories too narrowly. She has used the Employment Protocols for two years, in which time only three cases have qualified under its definition of “employment.” Finally, one member reiterated his belief that the committee should not endorse new pilot projects without studying the existing ones more thoroughly.

Judge Sutton concluded that the committee appears to support studying an expanded initial disclosure system. This, he said, might be the time to try again.

Judge Fitzwater: Streamlined Procedure

PRESENTATION

Judge Fitzwater surveyed the many existing pilot projects that offer litigants streamlined procedures. According to the Institute for the Advancement of the American Legal System (IAALS), successful projects have five key features:

- a short trial that limits time to present evidence,
- a credible trial date,
- an expedited and focused pretrial process,
- relaxed evidentiary standards that encourage parties to agree to admission, and
- voluntary participation.

Judge Fitzwater then summarized two examples of what such a pilot project might look like. He could not find data about how often summary procedures had been used, but the procedures themselves are well-known. He started with the short-trial regime established by the District of Nevada in 2013. Litigants who opt into that system lose their right to discovery. In return, they receive a trial within 150 days of initial assignment, with a 60-day continuance available in limited circumstances. Evidence may be admitted without authentication or foundation by a live witness, and parties are encouraged to submit expert testimony through reports and not live testimony. At the trial itself, each party receives 9 hours to allocate among all trial phases as it chooses. The litigants present their arguments before a condensed jury—and once the trial is over, their ability to file post-trial motions is limited.

He then contrasted Nevada's system with the short-trial process in the Western District of Pennsylvania. That district does not eliminate a party's right to discovery but instead puts numerical limits upon it. Each party only has three hours to present evidence to the jury, with additional time for jury selection allocated at the judge's discretion. Finally, and most critically, the system bars parties from filing motions for summary judgment or motions in limine. Other pretrial motions may be filed only with leave of court.

Judge Fitzwater placed particular emphasis on this last provision. In the mine-run civil case, dispositive motions—not discovery disputes—were the main source of delay. Ironically, the Criminal Justice Reform Act's reporting procedures reinforce the incentive to work on motions, not cases: Judges must report a motion as pending after six months, but need not report a case as pending until three years elapse.

DISCUSSION

Many committee members expressed skepticism that a voluntary program would succeed. One pointed out that the Northern District of California abandoned a similar short-trial

procedure after litigants declined to use it. Several district judges on the committee who have given litigants an expedited-trial option encountered the same problem. In light of that experience, they recommended that any pilot project in this area be mandatory, not voluntary.

Judge Sutton asked Professor Cooper why his proposal in the 1990s to apply simplified procedural rules to small-stakes cases failed to gain traction. Professor Cooper explained that the proposal failed after a district judge pronounced it “elegant on paper but of no practical use.” He also pointed out two potential implementation issues: First, different lawyers define a “small-stakes case” differently; and second, how should a simplified system treat a small-stakes case with a demand for injunctive relief?

One appellate judge recommended against defining “small stakes” using a dollar amount. She cited her experience with the Class Action Fairness Act, which contains a similar dollar-amount requirement, and collateral litigation over manipulation of that requirement. Another appellate judge warned that mandating streamlined procedures for certain categories of cases, but not others, will be tricky.

* * *

Judge Sutton summed up the conversation. At a minimum, he said, everybody agrees that the committee should study the many pilot projects in existence. And nobody thinks the committee should refrain from considering the possibility of civil litigation reform; the only worry is that specific reforms might be more complicated than anticipated. As such, he asked the Civil Rules Committee to study this topic and give its thoughts at the upcoming May meeting. He also advised it to consult Judge Fogel to see what FJC resources are available, and to coordinate with IAALS and the legal academy as well.

NEXT COMMITTEE MEETING

Judge Sutton concluded the meeting by announcing that the committee will next convene on May 28–29, 2015, in Washington, D.C.

Respectfully submitted,

Judge Jeffrey S. Sutton
Chair

TAB 2A

MEMO TO: Members, Criminal Rules Advisory Committee

FROM: Professors Sara Sun Beale and Nancy King, Reporters

RE: Rule 4

DATE: February 24, 2015

Proposed amendments to Rule 4, Tab B, were published for public comment in August 2014. A public hearing was held November 4, 2014, and one speaker (from the Federal Bar Council) testified about Rule 4, in support of the amendment. A total of six written comments were received before the close of the comment period; they are summarized at Tab C. Two comments – from the National Association of Criminal Defense Lawyers (NACDL) (CR-2014-0004-0031) and the Federal Magistrate Judges Association (FMJA) (CR-2014-0004-0019) – recommended revisions to the proposed amendments. One commenter, the Quinn Emanuel law firm (CR-2014-0004-0028), urged the proposal be withdrawn. The Department of Justice also provided a written response to the comments, defending the proposed amendment. The Department’s February 20, 2015 memorandum is at Tab D and its August 23, 2013 memorandum is at Tab E.

The Rule 4 Subcommittee met by telephone conference on February 23, 2015, to consider the comments on the published rule and the Department’s response. After carefully discussing the concerns raised by the comments, the Subcommittee decided unanimously to recommend that the Committee approve and transmit to the Standing Committee the proposed amendment and accompanying note as published, without changes.

The remainder of this memorandum summarizes the issues raised by the comments and the Subcommittee’s consideration and resolution of those concerns.

A. Judicial review of notice.

The lawyers at Quinn Emanuel asked the Committee to withdraw the proposed amendment, arguing that it 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 Subcommittee 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 the Subcommittee agreed with the Department of Justice that this 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.

Quinn Emanuel also argued that in suggesting notice was the sole criterion for service, the Rule would “eliminate a historical function of service.” It quoted the Supreme Court’s statement in *Omni Capital Int’l v. Wolf & Co.*, 484 U.S. 97, 104 (1987):

Thus, before a court may exercise personal jurisdiction over a defendant, there must be more than notice to the defendant and a constitutionally sufficient relationship between the defendant and the forum. There also must be a basis for the defendant's amenability to service of summons.

The Subcommittee 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).

B. Consequences of not appearing; proceedings in absentia.

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. The Subcommittee noted in its discussion of this concern that the Rule does not limit a defendant from contesting notice at any stage of the proceeding, and that Rule 43, not Rule 4, regulates a court’s ability to conduct proceedings without the presence of the defendant.

Raising a similar objection, 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 Subcommittee considered and rejected this suggestion. 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 rules are not applicable.

C. Required procedures for service.

Quinn Emanuel’s letter argued further that “any other means that gives notice” renders superfluous the other sections of the proposed amendment. Both points were debated at length in formulating the proposal. 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.

In a related comment, NACDL argued that the proposed amendment should be modified to allow service under proposed (3)(D)(ii) only if (3)(D)(i) does not apply. In its earlier deliberations the 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 Subcommittee 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 in the Department of Justice response, Tab F, litigation in a recent case on whether a subsidiary of a foreign corporation could be served took eight months. It would be contrary to the goals of the proposed amendment to add a procedural hurdle that might invite such extended litigation.

Finally, the FMJA, which supported the proposed amendment as a needed change to fill a gap in the rules, suggested that the Committee Note be revised to state expressly that the means of service must satisfy constitutional due process. The Subcommittee declined to act on this suggestion, reasoning (as with the suggested reference to Rule 43 above) that such cross references are not necessary and should ordinarily not be included in Committee Notes.

D. Reciprocal measures by foreign states; international relations concerns.

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, the Quinn Emanuel letter noted that 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 they 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 in a memorandum, Tab G, that it had consulted with appropriate authorities in the Executive Branch about the potential international relations ramifications of the proposed amendment. The Subcommittee agreed that in light of this assurance, concerns about any impact on diplomatic relations were not a basis for rejecting the proposed amendment.

E. Judicial discretion over the summons/arrest decision.

Finally, NACDL urged the Committee to revise the Rule to confer discretion on Magistrate Judges to decide whether a summons rather than a warrant should be issued, and to express a preference for issuance of a summons absent a showing of good cause to issue a warrant. This suggestion falls outside the scope of the proposed amendment, which was designed only to fill a specific gap in the existing rule regarding service on an organizational defendant not within a judicial district of the United States.

TAB 2B

**PROPOSED AMENDMENTS TO THE
FEDERAL RULES OF CRIMINAL PROCEDURE***

1 **Rule 4. Arrest Warrant or Summons on a Complaint**

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

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

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

17 * * * * *

18 (c) **Execution or Service, and Return.**

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

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

30 **(3) Manner.**

31 (A) A warrant is executed by arresting the
32 defendant. Upon arrest, an officer
33 possessing the original or a duplicate
34 original warrant must show it to the
35 defendant. If the officer does not possess
36 the warrant, the officer must inform the
37 defendant of the warrant's existence and of
38 the offense charged and, at the defendant's
39 request, must show the original or a
40 duplicate original warrant to the defendant
41 as soon as possible.

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

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

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

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

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

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

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

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

75 (a) stipulated by the parties;

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

79 submitted under an applicable
80 international agreement; or
81 (c) permitted by an applicable
82 international agreement.
83 * * * * *

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.

delivery” under subparagraph (F).

TAB 2C

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).

TAB 2D



U.S. Department of Justice

Criminal Division

Office of Policy and Legislation

Washington, D.C. 20530

MEMORANDUM

TO: Judge David M. Lawson
Chair, Subcommittee on Rule 4

FROM: Jonathan J. Wroblewski, Director
Office of Policy and Legislation *JW*

SUBJECT: Proposed Amendments to Rule 4

DATE: February 20, 2015

This memorandum responds to comments received from the law firm Quinn Emanuel and the National Association of Criminal Defense Lawyers regarding the pending proposed amendment to Rule 4 of the Federal Rules of Criminal Procedure. The authors from Quinn Emanuel note that they represent, among others, the Pangang Group Company (“Pangang”), a state-owned Chinese corporation.

A. In short, the Quinn Emanuel comments urge the Committee “to decline to approve the proposed amendments to Federal Rule of Criminal Procedure 4.” As we noted in our original request to the Committee to consider this amendment, the proposal would facilitate the service of process on Pangang – something the United States has been unable to do under the current Rule 4.¹ The amendment is intended to address the fact that under current law, foreign corporations

¹ 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.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage. 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,

can not only commit serious crimes in the United States without having any physical presence here, but also avoid criminal accountability due to the requirements of the current version of Rule 4. The amendment is necessary 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.

Although the Quinn Emanuel comments oppose the amendment, they do not argue that the United States government should be precluded from prosecuting foreign organizations, nor do they present any alternative solution to the problem identified by our proposal. Instead, the comments raise a series of hypothetical situations which they assert could be problematic, and thus urge the Committee to scrap the amendment entirely. We do not believe any of the concerns raised warrant scrapping or modifying the amendment.

First, the comments argue that the “fundamental problem” with the “notice only” approach of the amendment is that a foreign corporation with notice of a U.S. criminal summons could not challenge service because “the very act of challenging service might be said to conclusively establish the notice that would make service complete.” But this is not a flaw in the proposed amendment, it is the point of the amendment. If the defendant corporation has notice of a summons, it ought to be considered served, and there ought not be an avenue to present a factual claim that is, by definition, without merit. By contrast, if a corporate defendant seeks to raise some other claim regarding a defect in service, we do not believe anything in the proposed amendment would alter existing rules governing the availability of a “special appearance” to contest service.

For example, nothing in the proposed rule would alter current law regarding whether a corporate defendant could specially appear to contest the constitutionality of the amended Rule 4, whether the rule applied retroactively, or whether the rule applied to a particular defendant. Similarly, counsel for a defendant might seek to enter a special appearance to argue that a particular foreign corporation was dissolved prior to indictment and had no post-dissolution existence or obligations.

The purpose of a “special appearance” is to avoid automatically waiving threshold issues by operation of law – not to prevent fact finding. 5B Fed. Prac. & Proc. Civ. § 1344 (3d ed.) (“Prior to the federal rules, the practice was for counsel to appear specially for the purpose of objecting by motion to the jurisdiction of the court over the defendant or its property, venue of the action, or insufficient process or service of process; a failure to follow the correct procedure for doing so often resulted in a waiver of the defense.”); *Harkness v. Hyde*, 98 U.S. 476, 479 (1878) (“It is only where [a defendant] pleads to the merits in the first instance, without insisting upon the [failure of the plaintiff to meet a threshold procedural requirement], that the objection is deemed to be waived.”); *Ins. Co. of N. Am. v. Svendsen*, 74 F. 346, 347 (D.S.C. 1896) (“The purpose of a special appearance is to prevent a waiver of any objection which would be cured by a general appearance.”). When a party makes a special appearance, any *facts* that a court learns

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).

as a result of that appearance, including that a party has received actual notice of the prosecution, may be considered by the court.

The Quinn Emanuel commenters argue that the amendment might cause “a responsible foreign organization that wishes to contest service” to face “a Hobson’s choice” because if it appears to contest service it may be deemed to have notice. But feigning ignorance of a criminal summons of which the foreign organization does have notice (either by declining to appear, or by appearing and denying knowledge) is not a legitimate interest the criminal rules should protect. A foreign organization acting lawfully in this situation has two reasonable choices: it can either appear in a U.S. court to raise any legitimate defense or it can choose not to appear and face any attendant risks.

Nor would the amendment “foreclose judicial review” as the commenters state. If the foreign organization appears, either initially or belatedly, the court will have the opportunity to consider any appropriate argument that the organization presents. If the foreign organization does not appear, the court will have to satisfy itself that the United States sufficiently provided notice. Either way, service will be subject to proper judicial review.

Finally, the Committee has already considered and rejected the concern expressed by the Quinn Emanuel commenters that service under the proposed amendment might violate foreign law or an international agreement.

B. The National Association of Criminal Defense Lawyers suggests that the proposed provisions permitting service of process on a foreign organization abroad should only apply “if 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.” Perhaps if the suggested amendment unambiguously permitted service on a U.S. affiliate or subsidiary, if one exists, regardless of whether it is an alter ego, the amendment might be acceptable. However, this is not what NACDL suggests, perhaps because such a suggestion in and of itself would raise other serious concerns. Nonetheless, we think adding an ambiguous requirement, along the lines suggested by NACDL, would be problematic as it would only result in unnecessary delays and collateral litigation and not serve any legitimate public policy purpose. If a valid U.S. representative were available, it would be in the government’s interest to serve that representative rather than seek foreign service. But requiring to government to seek U.S. service first in the manner suggested by NACDL would likely result in collateral litigation regarding, for instance, whether a U.S. subsidiary was an appropriate alter-ego to serve. We have experienced lengthy litigation of such issues in prior cases.

Indeed, in the case involving Pangang, our prosecutors served a summons on Pangang's wholly owned subsidiary in New Jersey. Pangang’s lawyers contested service, and after eight months of litigation, Judge White held that that the subsidiary was not the alter ego of the parent company and that service was therefore not completed. *Pangang*, 879 F. Supp. 2d at 1068 (“The Court finds that the Government has not shown the requisite unity of interest to establish an alter-ego relationship between Pan America and PIETC.”).

A rule that requires the government to attempt to serve a U.S. subsidiary first and then spend months or years litigating whether that service constituted service on the foreign parent would be contrary to the goals underlying Rule 4 and the proposed amendment, which are to ensure adequate notice and encourage litigation of the merits of a case.

It is important to keep front and center that the “core objective” of Rule 4 is to provide “notice of a criminal proceeding.” See Draft Amendments at 335; see also *Henderson v. United States*, 517 U.S. 654, 672 (1996) (“the core function of service is to supply notice of the pendency of a legal action, in a manner and at a time that affords the defendant a fair opportunity to answer the complaint and present defenses and objections.”).² Service is not intended to be a significant barrier to initiating a prosecution, nor is it an invitation to collateral litigation. Indeed, in both civil litigation and criminal prosecution (with the possible exception of the subject of this amendment), service has generally been a routine matter, not prone to significant disputes. We believe the Advisory Committee, in carefully drafting this amendment, has made an effort to eliminate “unnecessary burdens and delays” when serving foreign organizations. Draft Amendments at 323 n.4. This Subcommittee and the full Advisory Committee should resist any attempt to derail this important effort.

cc: Professor Sara Sun Beale, Reporter
Professor Nancy J. King, Reporter

² The Quinn Emanuel commenters cite to a civil case, *Omni Capital Int'l v. Wolf & Co.*, 484 U.S. 97 (1987), for the proposition that “[m]aking notice the sole criterion for service, as the proposed rule could be argued to do, would eliminate a historical function of service.” But *Omni Capital* simply held that establishing that the defendant has actual notice is insufficient where “the procedural requirement” of the service rule requires that some specific procedure be followed. *Id.* at 104. *Omni Capital* does not suggest that a service rule *must* require the following of a particular procedure. Indeed, Rule 4 of the Federal Rules of Civil Procedure also permits service “by other means not prohibited by international agreement, as the court orders.” Fed. R. Civ. P. 4(f)(3).

TAB 2E



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

August 23, 2013

MEMORANDUM

TO: Judge David M. Lawson
Chair, Subcommittee on Rule 4

FROM: Jonathan J. Wroblewski, Director
Office of Policy and Legislation

Kathleen A. Felton
Deputy Chief, Appellate Section

SUBJECT: Proposed Amendments to Rule 4

I. Introduction

This memorandum responds to the discussion on our August 19th conference call and also to your specific request to address four issues raised by the Subcommittee on the call. You asked us to:

1. Provide a description of what the Department of Justice's approval process would be for the alternate means of service pursuant to Rule 4(c)(3)(D)(ii)(d);
2. Provide a statement for the record that the Departments of Justice and State have considered reciprocity concerns should Rule 4 be amended to permit service of a U.S. summons in a manner that could contravene foreign law;
3. Describe the practical consequences of service pursuant to Rule 4(c)(3)(D)(ii)(d); and
4. Lay out the options that are available to a court when a summons is served on a foreign entity that ignores the order to appear.

After the August 19th conference call, we consulted extensively with our colleagues within the Department of Justice and at the Department of State. We considered further the Subcommittee's latest draft amendment, the proposed addition to Rule 4(c)(3)(D)(ii)(d) to

authorize other means of service *not prohibited by international agreement*, and the other concerns raised on the call.

We would very much like to develop consensus in the Subcommittee for the proposed amendment. In that spirit, we now are prepared to accept the additional language – “not prohibited by international agreement.” We believe the language can work to effectuate service, notwithstanding the concerns we expressed on the call, and will also address the concerns raised by other members of the Subcommittee. However, we think two modifications are needed: first, that the language be amended to read “not prohibited by an applicable international agreement,” consistent with the language used in Rule 4(c)(3)(D)(ii)(b) and (c); and second, we think it is important to add Committee Note language to address some of the scenarios we discussed on our call. The note language we suggest, modeled on similar note language accompanying Civil Rule 4(f), spells out in greater detail when alternate means of service might be appropriate.

Paragraph (d) authorizes the court to approve other means of service not prohibited by an applicable international agreement. Some international agreements authorize other unspecified means of service in cases of urgency, when conventional methods will not permit service within the time required by the circumstances. Other means of service may also be justified by the failure of the foreign country's Central Authority to effect service pursuant to a bilateral or multilateral agreement, when there is no international agreement applicable, or when an agreement does not specify the type of legal assistance that can be sought or does not specify the means for serving a judicial document, such as a criminal summons. In such cases, the court, at the request of the attorney for the government, may direct a special means of service not explicitly authorized by international agreement if such means is not prohibited by any valid agreement ratified and in force.

We also believe one additional change to the draft is warranted to effectuate the Subcommittee's intent. Rule 4(c)(3)(D) should be amended to eliminate the phrase “at a place”. The provision would then read: “A summons is served on an organization ~~at a place~~ not within a judicial district of the United States by any of the following means that is reasonably calculated to give notice:”. In our prior discussions, the Subcommittee has contemplated that the alternate means of service under Rule 4(c)(3)(D)(ii) could take place within the United States, even though the organization is not within the United States. If the phrase “at a place” remains, the possibility of alternative service within the U.S. would arguably be eliminated.

We hope the Subcommittee will find this language acceptable. We look forward to discussing this further with you on our September 3rd conference call.

II. DOJ's Approval Process for the Alternate Means of Service Pursuant to Rule 4(c)(3)(D)(ii)(d)

As we have previously discussed, within the Department of Justice, the Criminal Division's Office of International Affairs (OIA) serves as the Central Authority and clearinghouse for all international criminal matters. Regardless of whether there is a treaty

relationship between the United States and the relevant foreign state, OIA ensures that the necessary steps are taken to effectuate service of a criminal summons on an appropriate representative or agent of that organization in accordance with U.S. and international law and consistent with U.S. foreign policy. OIA is staffed with specialists whose experience and training enable them to assess what process both complies with domestic and international law and will best effectuate service, and they will confer as needed with the State Department.

The U.S. Attorney's Manual and Departmental policy guidance instruct prosecutors on when and how to make a request for approval and assistance from OIA. *See* U.S. Attorneys' Manual, 9-13.500, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/13mcrm.htm#9-13.500 (last visited August 20, 2013). Department policy requires prosecutors to seek approval from OIA when seeking any assistance abroad or taking "any act outside the United States relating to a criminal investigation or prosecution." *Id.*

OIA works with the Executive Office of United States Attorneys to ensure that the U.S. Attorney's Manual captures the Department's expectations about a prosecutor's need to work with and through OIA for all forms of assistance sought and in cases implicating foreign policy, including serving a criminal summons on a foreign organization. The Department is prepared to further amend the U.S. Attorney's Manual to make absolutely clear the need to obtain the approval of OIA before seeking any means of service outside the U.S. or otherwise involving a foreign organization under Rule 4.

III. Reciprocity Concerns if the Rule were Amended to Permit U.S. Service in a Manner that Could Contravene Foreign Law

When serving a criminal summons on a foreign organization at a place not within a judicial district of the United States pursuant to subsection (c)(3)(D) of the proposal, the United States will generally seek to ascertain and comply with the law of the place where service is to be made. The proposed inclusion of subsection (c)(3)(D)(ii)(d) would permit service by a means that "the court orders on request by an attorney for the government," as a last resort when other means are unavailable, which in some cases could result in a manner of service that could be deemed inconsistent with foreign law. However, such service would only proceed after consultations between the Criminal Division's Office of International Affairs and the Department of State. In light of this, Criminal Division Deputy Assistant Attorney General for International Affairs Bruce Swartz, the Criminal Division's Office of International Affairs and representatives of the Department of the State consider this proposal to provide an appropriate opportunity for potential reciprocity or foreign policy implications to be taken into account in the context of particular cases and believe the amendment proposal should proceed.

IV. The Practical Steps that a Court and the Executive Branch Can Take When an Organization Fails to Appear in Response to a Validly Served Summons

As we have discussed with the Subcommittee, we have found little case law addressing the consequences of an organization failing to appear in response to a validly served summons. We believe this is because in most cases, when a summons is properly served, organizations do

appear and have a very strong financial incentive to appear. Interestingly, in recent criminal cases involving foreign corporations contesting service of process under Rule 4, those corporations paid U.S. counsel to “specially appear” and make the argument that service was invalid. *See, e.g. United States v. Kolon Industries, Inc.*--- F.Supp.2d ----, 2013 WL 682896 (E.D.Va., February 22, 2013), *United States v. Dotcom*, 2012 WL 4788433 (E.D. Va., Oct. 5, 2012); *United States v. Pangang Group, Ltd.*, 879 F. Supp. 2d 1052 (N.D. Ca. 2012). These corporations could have simply ignored the criminal case and not paid anyone to appear. Whether it was a concern for the company’s international reputation, management’s fear of being arrested when attending an overseas business meeting, the desire not to be perceived as a fugitive, or a desire to maintain a sense of honor, these companies all decided it was better to contest service than have the corporation labeled a fugitive.

Anytime an organization has assets in the U.S. or intends to continue doing business in the U.S., there will be a very strong incentive for the organization to appear and address the criminal allegations, for the pending criminal charges could result in actions that would impact the assets or continuing operations. If the organization does not appear, though, there are a number of practical steps that a court and the Executive Branch could take. They include:

Contempt Orders: In response to a foreign organization’s decision not to appear following properly initiated criminal charges, a court could enter a contempt order (*e.g.*, under 18 U.S.C. § 401(3)), possibly resulting in significant fines, forfeitures, and/or other penalties. These penalties may be enforced through the imposition of daily fines. *See, e.g., United States v. Darwin Const. Co., Inc.*, 873 F.2d 750 (4th. Cir. 1989) (in civil contempt action, corporation found in contempt for failure to comply with IRS summons was subject to a daily fine of \$5,000); *Perfect Fit Indus., Inc. v. Acme Quilting Co., Inc.*, 673 F.2d 53 (2d Cir. 1982) (civil contempt).

The ability to obtain a contempt order is further enhanced by the Committee Note to proposed subsection (a), which states that “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.”

Injunctive Relief: A foreign organization’s decision not to appear in response to properly initiated criminal charges would be a factor weighing in favor of granting the United States injunctive relief against the foreign organization. Such relief is permitted under various criminal statutes, including the Economic Espionage Act, 18 U.S.C. § 1836, which authorizes the government to file a civil action to “obtain appropriate injunctive relief against any violation of this chapter.” Prosecutors commonly seek injunctive relief to prevent further disclosure of a trade secret by the defendant or third parties during a criminal investigation, or as part of the judgment at the end of the case. Depending upon its terms, such an injunction could also limit a foreign corporation’s ability to do business in the United States and be used by victims or third-parties to obtain relief abroad.

Appointment of Counsel: There is some authority for the proposition that, in certain circumstances, a court may appoint counsel for a corporation that fails to appear after being properly served, and may proceed with a criminal trial. *See United States v. Rivera*, 912 F. Supp.

634, 638-39 (D. Puerto Rico 1996) (appointing counsel to a corporate defendant that failed to appear at two initial hearings and holding that “[i]nasmuch as a defendant’s right to retain counsel of his choice may not interfere with the efficient administration of justice, when confronted with a recalcitrant defendant who refuses to . . . submit to the jurisdiction of the Court, the Court in its discretion may appoint counsel”; fees and expenses to be paid from corporate assets and properties); *United States v. Crosby*, 24 F.R.D. 15, 16 (S.D.N.Y. 1959) (observing that “a corporation may not appear except by counsel” and holding that “[i]t would be idle to provide for summoning a corporation if the court, after so doing, could not render a judgment against it. The court must, therefore, have power to appoint one of its attorneys and officers to appear for the corporation.”).

Parallel Proceedings: There is also some authority for the proposition that, in certain circumstances, a court may sanction a party that fails to comply with orders in a criminal action through penalties in a parallel civil action. *See, e.g., United States v. Crawford Enterprises Inc.*, 643 F. Supp. 370, 380 (S.D. Tex. 1986) (court finds a foreign oil company in criminal and civil contempt and holds that the oil company’s civil action against a corporation that was a defendant in a separate criminal case should be dismissed for the oil company’s failure to comply with the corporation’s *subpoena duces tecum* in the criminal case).

Seizure/Forfeiture: A foreign organization’s decision not to appear in response to properly initiated criminal charges can result in seizure and forfeiture of the organization’s assets, including assets in foreign countries that honor U.S. forfeiture orders, and any assets located in the United States. Under the Civil Asset Forfeiture Reform Act, Congress reinstated what is commonly known as the “fugitive disentitlement doctrine.” *See* 28 U.S.C. § 2466. Under the doctrine, a court where a civil forfeiture action is pending may disallow any challenge to the forfeiture if the Government establishes that a related criminal case was initiated against the claimant; that the claimant was notified and has knowledge of the criminal case; and that the claimant deliberately avoided prosecution by leaving or declining to “enter or reenter” the U.S. or was otherwise evading the jurisdiction of the court where the criminal case is pending. Congress has included within the scope of the statute not only claims filed by fugitive individuals, but also claims filed by corporations. *See, United States v. \$6,976,934.65 Plus Interest*, 478 F. Supp. 2d 30, 43 (D.D.C. 2007) (section 2466(b) creates a presumption that the disentitlement doctrine applies if a fugitive is the corporate claimant’s majority shareholder, but even without the presumption, the fugitive’s disentitlement may be imputed to the corporation if the court pierces the corporate veil and finds that the corporation is the fugitive’s alter ego), *rev’d on other grounds*, 554 F.3d 123 (D.C. Cir. 2009).

Office of Foreign Asset Control: The President has the ability to issue executive orders directing the Treasury Department to administer and enforce economic and trade sanctions based on U.S. foreign policy and national security goals. These sanctions may prevent a foreign corporation from doing business in the United States or through a U.S. bank. The Department of Justice can seek such OFAC sanctions against foreign corporations where certain criteria are met. One factor favoring OFAC sanctions would be a foreign corporation’s decision not to appear in response to a properly initiated criminal lawsuit.

Listing and Diplomatic Consequences: Executive Branch agencies such as the Department of Commerce maintain public lists of foreign corporate entities that are being sanctioned because of misconduct. In addition, the fact that a particular country or countries have engaged in a pattern of harboring fugitive corporations may also be an important factor forming or modifying diplomatic, trade or other relationships. For example, a number of recent cases in which Rule 4 process was challenged involve intellectual property issues. A country's pattern of harboring fugitive corporations in that context could be one factor in determining whether to include a country in United States Trade Representative's "Special 301" Report, an annual review of the state of intellectual property rights protection and enforcement in trading partners around world, which the Office of the United States Trade Representative conducts pursuant to section 182 of the Trade Act of 1974 (as amended by the Omnibus Trade and Competitiveness Act of 1988 and the Uruguay Round Agreements Act). The May 2013 report can be found at:
<http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf>.

Debarment: The Government may impose other non-penal sanctions that may accompany a criminal charge, such as suspension or debarment from eligibility for government contracts or federally funded programs. Determining whether or not such sanctions are appropriate or required in a particular case is the responsibility of the relevant agency, and is a decision that is made based on the applicable statutes, regulations, and policies. The Federal Acquisition Regulations System codifies these policies as well as applicable procedures for imposing suspension and debarment. The Federal Acquisition Regulation (FAR), *Subpart 9.4—Debarment, Suspension, and Ineligibility*, permits a contracting official to suspend or debar a contractor once charged with a criminal offense. However, there are procedural protections that go along with suspension and debarment, including notice. Such notice would be evidenced in part by service of process in the criminal case.

V. Conclusion

We hope this memorandum and our suggested revisions to the draft amendment and Committee Note are helpful. As we stated earlier, our ultimate objective is to facilitate the efforts of the U.S. Government to hold organizations accountable for criminal conduct, obtain restitution, and otherwise vindicate the interests of the people of the United States. Our specific objective underlying our rule proposal is to amend Rule 4 to authorize the service of process in manners that provide notice to the defendant organization while not placing unnecessary obstacles to the initiation of criminal proceedings.

We look forward to discussing all of this with the Subcommittee soon. Please let us know if there is any further information we can provide to you.

TAB 3A

MEMO TO: Members, Criminal Rules Advisory Committee

FROM: Professors Sara Sun Beale and Nancy King, Reporters

RE: Rule 41

DATE: February 25, 2015

A proposed amendment to Rule 41 was published for public comment in August 2014, and was the subject of public hearings held November 4, 2014. The Rule 41 Subcommittee held three teleconference calls after the hearings to discuss the written and oral testimony of the witnesses, as well as other written comments on the proposed amendment.

This memorandum first provides general introduction to the proposed amendment, and then describes the issues raised during the public comment period and the Subcommittee's recommendations. As discussed below, the Subcommittee recommends that the Committee make three clarifying changes in the text of the proposed rule and add clarifying language to the Committee Note. With those changes, the Subcommittee unanimously recommends that the proposed amendment be approved for transmittal to the Standing Committee.

The recommended changes are discussed first as they relate to specific public comments, and then presented as action items at the end of this memorandum. The proposed amendments, as modified, is Tab B. Tab C is the amendments as published. Tab D is a summary of each public comment on Rule 41. Three memoranda from the Department of Justice, which respond to public comments, are Tabs E, F, and G.

I. INTRODUCTION

The proposed amendment 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,¹ but permits out-of-district searches in specified circumstances.² The amendment would add specified remote access searches for electronic information to the list of other extraterritorial searches permitted under Rule 41(b). Language in a new subsection 41(b)(6) would authorize a court to issue a warrant to use remote access to search electronic storage media and seize electronically stored information inside *or outside* of the district in two specific circumstances.

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

A. Reasons for the proposal

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

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

¹ 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”).

² 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.

such a search. Although some judges have reportedly approved such searches, one judge recently concluded that the territorial requirement in Rule 41(b) precluded a warrant for a remote search when the location of the computer was not known, and he suggested that the Committee should consider updating the territorial limitation to accommodate advancements in technology. *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (noting that "there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology").

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

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

B. The proposed amendment

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

standards to ongoing case law development.

II. The Public Comments and the Subcommittee's Recommendations

During the public comment period the Committee received 18 written comments from individuals and organizations, as well as testimony from one witness who did not provide a written statement.³

The Federal Bar Council, the Federal Magistrate Judges' Association CR-2014-0004-0019, the National Association of Assistant United States Attorneys CR-2014-0004-0027, and a former advocate for missing and exploited children, Carolyn Atwell-Davis, CR-2014-0004-0007, all supported the amendment without change.

The amendment was opposed by the American Civil Liberties Union (ACLU), CR-2014-0004-0013; Google, CR-2014-0004-0029; the National Association of Criminal Defense Attorneys (NACDL), CR-2014-0004-0031; the Pennsylvania Bar Association, CR-2014-0004-0030; the Reporters Committee on the Freedom of the Press, and several foundations and centers that focus on privacy and/or technology. A number of individuals also opposed the amendment.

This memorandum is organized according to the principal concerns raised in the public comments opposing the amendment. In addition, we provide a brief description of each comment at Tab D. Memoranda from the Department of Justice responding to concerns raised during the public comment period are Tabs E, F, and G.

A. Concerns about privacy and the Fourth Amendment

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 concerns focus 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. Comments raising these concerns generally urged that the proposed amendment be withdrawn.

The Subcommittee recognizes that remote electronic searches are likely to raise novel difficult issues under the Fourth Amendment, but it concluded unanimously that these concerns

³In addition, the record includes a comment from the American Civil Liberties Union, recorded as CR-2014-0004-16, which was commented on an earlier proposed draft that was substantially modified before publication. In light of the substantial differences between the original publication and that proposed for public comment, and the ACLU's extensive comments on the current draft, this memorandum does not discuss the ACLU's earlier letter.

do not justify withdrawing the amendment. Nothing in the current Federal Rules of Criminal Procedure precludes the issuance of warrants for remote electronic searches. Courts now issue warrants for remote electronic searches and resolve any constitutional questions on a case-by-case basis. At present, Rule 41(b)'s rigid venue requirement serves as a serious stumbling block into investigations of serious criminal conduct. The current venue requirements allow a person who has committed a crime to use anonymizing technology to prevent the issuance of a remote warrant even when all of the other requirements of the constitutional have been met. Indeed the government could not now obtain a warrant even by going to every one of the 94 judicial districts, since it would not be able to establish that the property to be searched was located in any of these districts. The Subcommittee concluded that the proper course of action is to amend the rule and allow the courts to rule on Fourth Amendment issues as they arise on a case by case basis. The Subcommittee's specific response to each concern is noted below in bold.

1. Particularity

Concerns about the Fourth Amendment particularity requirement were discussed in detail in several comments. The Center for Democracy and Technology (CDT), CR-2014-0004-0009, argued, at 2-3, that a warrant that cannot specify the district in which the target storage medium or information is located cannot meet the particularity requirement. The ACLU, CR-2014-0004-0013, at 21-22, argued that a "watering hole" attack would likely result in the search of many innocent computers for which the government has no probable cause. Innocent computers might also be searched if the government used more targeted remote search techniques, such as an email to the target device with a link that the recipient will click, because the recipient would likely forward the link and recipients might do the same.

Google, CR-2014-0004-0029, expressed a related concern, at 7-8, that the proposed amendment "fails to specify or limit how searches may be conducted" as well as "what, precisely, may be searched once the media or information is accessed." Bellotin et al. also noted that the nature of the technology is such that it is inherently difficult to describe the location of information, which may be stored in many forms on a computer or other device. Jeffrey Adzima, CR-2014-0004-0037, expressed a general view that the proposed amendment was at odds with the Fourth Amendment particularity requirement.

Steven Bellotin et al., CR-2014-0004-0012, also noted concerns, at 6-7, about the particularity requirement under proposed (b)(6)(B), because it would allow for a search of a large number of computers victimized by a botnet. Similarly, Google, CR-2014-0004-0029, stated, at 13-14, that millions of computers could be searched under proposed (b)(6), noting that the breadth of the definition of "damaged computer" under the Computer Fraud and Abuse Act.

In its December 22 letter, Tab F at 3-7, the Department of Justice described how particularity may be demonstrated in the case of remote searches when anonymizing technology has been employed, providing several examples.

The Subcommittee's response. The amendment responds to a significant

problem created by the venue provisions of the current rule, which do not address where the government may apply for a search warrant when anonymizing technology is used to conceal the location of the device or information to be searched. The amendment provides for venue in a limited class of such cases, but it does not resolve any of the constitutional issues (such as particularity concerns) that may be raised in individual cases. As stated in the Committee Note, “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.”

The Department of Justice letter provides examples of how warrant applications may specify a particular account or computer, even when the location has been concealed by technology. If the proposed amendment is adopted and the government seeks a warrant on the basis of such information, the courts can at that time rule on the question whether the application meets the Fourth Amendment particularity requirement.

2. Surreptitious entry, invasive or destructive searches

Electronic Privacy Information Center (EPIC), CR-2014-0004-0010, argues at 3-7, that searches conducted under the authority of remote access warrants operate as surreptitious entry searches with delayed notice. Like other delayed notice and covert entry searches, remote access searches must be severely limited to comply with the Fourth Amendment, and the proposed amendment does not impose the required limitations.

The ACLU, CR-2014-0004-0013, also argued, at 17-18, that remote searches may violate the reasonableness requirement of the Fourth Amendment because they are, by their nature, exceptionally intrusive, destructive, and dangerous. They are analogous to the use of a battering ram to gain entrance to a residence. Similarly, Google, CR-2014-0004-0029, at 9, expressed concern that the use of network investigative techniques to conduct remote access searches “may constitute an unreasonable search because of their destructive and unpredictable nature.(Other arguments concerning the potential collateral damage that may be caused by remote searches are discussed below.)

***The Subcommittee’s response.* As noted in connection with concerns focusing on the particularity requirement, the proposed amendment does not foreclose or prejudice these constitutional issues. Rather, it leaves them to be resolved on a case-by-case basis.**

3. Notice

Many of the comments argue that the notice provisions in the proposed amendment do not satisfy the requirements of the Fourth Amendment, or weaken desirable existing notice requirements.

The ACLU, CR-2014-0004-0013, at 23-24, argued that the proposed amendment “weakens” the current notice requirements. In comparison to current Rule 41(f)(1)(C), which requires that the officer “must” provide a copy of the warrant, the proposal requires only “reasonable efforts” that are “reasonably calculated to reach” the parties in question. This contemplates cases in which notice (or effective notice) may not be given, and casts doubt on whether such searches would meet the requirements of the Fourth Amendment. The ACLU stated that surreptitious searches strike at the heart of the interests protected by the Fourth Amendment. The ACLU detected two specific problems with the notice provision, *id.* at 24-25. First, if both the owner of a computer and others who use the computer are affected by a search, the proposed amendment requires that only one “or” the other be given notice. The ACLU argued that both the owner of a computer and others who use the computer should given notice if the users files are affected by a search. Second, notice may often be delayed.

Similarly, EPIC, CR-2014-0004-0010, at 3-7, argued the requirement of “reasonable efforts” to give notice is insufficient, allowing excessive delay in providing notice that would not be permitted in other contexts.

Bellotin et al., CR-2014-0004-0012, at 7-8, explained that all possible means of giving notice of a remote electronic search (a file left on the searched device, a pop-up window, an email, or a letter) will be problematic.

The Subcommittee’s response. The proposed notice requirements are intended to be parallel, to the degree possible, with the requirement for physical searches.

Actual notice, reasonable efforts to give notice

In the case of physical searches, it is not always possible to provide actual notice to the owner of property. Rule 41(f)(1)(C) presently requires that the officer executing a warrant must give a copy of the warrant and a receipt for 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.” If the owner is not present when the warrant is executed, leaving a copy is a reasonable means of giving notice, but it does not guarantee actual notice. The proposed amendment imposes a parallel requirement stated in general terms because of the variety of situations that may be presented.

Who will receive notice

In the case of a physical search of a computer that has been used by persons other than the owner, Rule 41(f)(1)(C) now requires that the government give notice “to the person from whom, or from whose premises, the property was taken.” (emphasis added.) If the government executes a warrant for a business and seizes business records containing information about individual customers, giving notice not only to the business but also to

each customer would be burdensome, and is not presently required. If the government does a physical search of a computer whose owner has permitted others to use it, the rule requires the government to give notice to the owner of the computer, not to both the owner and others who may have stored files or other information there.

The amendment is intended to impose a parallel requirement for remote electronic searches. As published, it provided:

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.*

The Subcommittee concluded that the italicized phrase was unclear, and it might not have the desired effect of making the notice requirements for electronic parallel to those now applicable to physical searches. Accordingly, the Subcommittee unanimously proposes that the phrasing be altered slightly to require that notice to be given “to the person whose property was searched *or who possessed the information that was seized or copied.*”

Providing a receipt for information seized or copied

In comparing the notice provisions for remote electronic searches with those currently required for physical searches, the Subcommittee noted that as published the proposal did not provide that the officer executing the warrant for a remote electronic search must not only make a reasonable effort to give notice, but also to provide a receipt for information seized or copied. The Subcommittee recommends that line 40 be amended to require that the officer make reasonable efforts to serve not only the warrant but also a receipt.

4. Delayed notice

Several commentators opposed the amendment, at least in part, because the requirement that the government make “reasonable efforts” to give notice was not accompanied by any requirement that notice be given promptly. For example, EPIC, CR-2014-0004-0010, at 7-8, argues that merely requiring reasonable efforts to provide notice would allow excessive delays not permitted in other contexts. The ACLU, CR-2014-0004-0013, at 24-25, also expressed concern that notice would often be significantly delayed.

The Subcommittee’s response. The proposed notice provisions would be subject to the requirements of Rule 41(f)(3), which provides that at the government’s request the judge issuing a warrant “may delay any notice required by this rule if the delay is authorized by statute.” Thus any delay in giving the proposed notice would be subject to precisely the same statutory limitations as those currently applicable to all other searches. In order to draw attention to this point, the Subcommittee unanimously recommends the following addition to the Committee Note:

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).

5. General concerns about privacy and the Fourth Amendment

Several other commentators – Mr. Anonymity, CR-2014-0004-0004; Former Federal Agent, CR-2014-0004-0005; Anonymous, CR-2014-0004-0020; Dan Teshima, CR-2014-0004-0021; George Orwell, CR-2014-0004-0022; Kati Anonymous, CR-2014-0004-0033; Jeff Cantwell, CR-2014-0004-0034; and Benoit Clement, CR-2014-0004-0035 – oppose the proposed amendment on the basis of broadly stated concerns that it will “weaken the Fourth Amendment” and allow the government to spy on its citizens or invade their privacy.

***The Subcommittee’s response.* As noted in connection with concerns focusing on the particularity requirement, the proposed amendment does not foreclose or prejudge these constitutional issues. Rather, it leaves them to be resolved on a case-by-case basis. Additionally, as noted below the Subcommittee concluded that commentators’ opposition might to some degree be premised on misconceptions about the effect of the amendment.**

6. Impediments to judicial review

Several commentators expressed concern that the serious constitutional issues raised by remote electronic searches would be insulated from judicial review. The ACLU, CR-2014-0004-0013, at 25-28, argues that the critical Fourth Amendment issues are unlikely to be resolved by the courts “for years, if ever.” Warrant applications are considered *ex parte*, without adversarial argument, and magistrate judges are “likely to be ill-equipped to provide robust review of applications ... particularly when the search warrant applications do not make clear that agents are seeking permission to hack into the computers of surveillance targets.” Judges’ limited technical knowledge will hamper their evaluation of particularity and other aspects of reasonableness. Orders granting or denying orders are rarely published and are often sealed, and notice may be delayed for a significant period of time, forestalling constitutional challenges. Other doctrines, such as qualified immunity, will also truncate judicial review of the constitutional issues. These problems, the ACLU states at 27, are “exacerbated by the government’s lack of candor about the nature of its remote application searches.” Similarly, EPIC, CR-2014-0004-0010, at 8, expressed concern that the Fourth Amendment’s good faith doctrine would prevent the courts from excluding evidence that had been illegally seized pursuant to a remote warrant.

Similarly, Google, CR-2014-0004-0029, at 8-13, argues that there are many impediments to judicial review that will slow the development of the law dealing with many significant constitutional statutory issues, and casting doubt on reliance on case-by-case resolution of these issues. It identifies the following as impediments: (1) the *ex parte* nature of the review of warrant applications, (2) the good faith exception to the exclusionary rule; (3) the inability of law abiding non-targets of a search to learn of a search and challenge it; and (4) qualified

immunity, which can shield government officials from civil liability for damages.

***The Subcommittee’s response.* Nothing in the current Federal Rules of Criminal Procedure precludes the issuance of warrants for remote electronic searches. Courts now issue warrants for remote electronic searches and resolve any constitutional questions on a case-by-case basis.**

The amendment addresses problems arising from language in Rule 41 that was drafted before the technology existed for remote searches. It removes a venue stumbling block that currently precludes the issuance of warrants that meet all constitutional and statutory requirements. And it clarifies how notice is to be given for remote electronic searches, creating parallel requirements for notice of remote electronic and physical searches.

The Rules Enabling Act authorizes the promulgation of “rules of practice and procedure” that do “not abridge, enlarge or modify any substantive right.” 28 U.S.C. § 2072. It is not the Committee’s role to address the constitutional issues that may arise when the government seeks warrants for remote electronic searches. The language of the draft Committee Note was modeled on the 2009 Committee Note accompanying Rule 41(e)(2)(B), which governs warrants seeking electronically stored information. In both cases, the amendments appropriately leave the constitutional standards to ongoing case law development.

B. The Effect of the Amendment on the Use of Virtual Private Networks and other Anonymizing Technology

More than a dozen commentators opposed the amendment because of an apparent misunderstanding of its effect on persons who use anonymizing technology such as Virtual Private Networks (VPNs).⁴ They noted that the use of VPNs and other technology is common and entirely legitimate. They expressed strong opposition to treating the use of a VPN as evidence of criminal activity or otherwise as a basis for allowing the government to conduct a remote electronic search. They appeared to think that whenever the government satisfied

⁴Mr. Anonymity, CR-2014-0004-0004; Former Federal Agent CR-2014-0004-0005; Bellotin et al., CR-2014-0004-0012; Anonymous, CR-2014-0004-0018; Ladar Levison, CR-2014-0004-0024; Edward Mulcahy, CR-2014-0004-0032; Tadeas Liska; CR-2014-0004-0039; Timothy Doughty, CR-2014-0004-0042; Stephen Argen, CR-2014-0004-0043; Ryan Hodin, CR-2014-0004-0046; Cormac Mannion, CR-2014-0004-0048; Michael Boucher, CR-2014-0004-0050; Andrew Gordon, CR-2014-0004-0052. Similar concerns also appear to underlie other comments. See Staff, Clandestine Reporters Working Group, LLC, CR-2014-0004-0051 (amendment improperly treats “secret” or “hidden” activity as ipso facto “illicit” activity); Anonymous Anonymous, CR-2014-0004-0045 (arguing that protecting one’s privacy does not create probable cause for a search).

proposed Rule 41(b)(6)(A) it could conduct a remote search. The Subcommittee concluded that the misunderstanding arose, at least in part, from the current caption of Rule 41(b): “Authority to Issue a Warrant.” To one concerned with privacy but not familiar with Rule 41 as a whole, or the relationship between Rule 41 and the Fourth Amendment, it could appear that a court may issue a warrant for a remote search once the government meets the criteria of proposed Rule 41(b)(6)(A).

The Subcommittee’s response. The Subcommittee proposes a revision to the caption to Rule 41(b) to clarify the limited effect of that provision: “Venue for a Warrant Application.” The Committee Note accompanying this revision would state:

Adding the word “venue” to the caption responds to some confusion about the effect of new subdivision (b)(6), making it clear that Rule 41(b) identifies which court may consider a warrant application; it does not address the constitutional requirements for the issuance of a warrant, which must also be met. The revised caption is not intended to have a substantive effect.

The Subcommittee hopes the reference to venue and the explicit statement that the constitutional requirements “must also be met” will allay the concerns of those who misunderstood the effect of the amendment.

Our style consultant, Professor Joe Kimble, does not think a revision is necessary, and if a revision in the caption is made he advocates retaining the reference to “Authority to Issue a Warrant,” while adding a reference to “Venue.” He reasoned that Rule 41 as a whole makes it clear that the requirements in (b)(6) cannot be read in isolation, and doubted that anyone has ever argued that meeting the criteria of (b)(1)-(5) would be sufficient to obtain a warrant. Moreover, he noted that references to the authority to issue a warrant recur throughout the rule and provide a desirable parallelism with (d), (e), and (f).

Although the Subcommittee agrees that anyone familiar with all of Rule 41 would not be misled by the current caption, the proposed amendment has generated substantial public opposition based, at least in part, on this misunderstanding. Given the public concern about the possibility that the government will employ technology to erode personal privacy, the Subcommittee concluded that a revision of the caption to clarify the limited function of Rule 41(b) would make an important contribution to the public’s understanding of the proposed amendment. In the Subcommittee’s view, the value of this enhanced clarity far outweighs the loss of parallelism that would otherwise be desirable.

Following the Subcommittee’s third teleconference call, Professor Kimble suggested that as a matter of style it would be preferable to substitute “District from Which a Warrant May Issue” for the Subcommittee’s proposed caption. Unless the Committee believes there is a substantive difference between “Venue for a Warrant Application” and “District from Which a

Warrant May Issue,” we would ordinarily adopt the language proposed by the Style Consultant.

C. Forum Shopping

The Center for Democracy & Technology (CDT), CR-2014-0004-0009, argued at 5-6, that the proposal would allow for a new form of forum shopping, resulting in the issuance of warrants in courts remote from the individual whose electronic media was searched or seized. The National Association of Criminal Defense Lawyers (NACDL), CR-2014-0004-0038, also argued that a restriction to the “district where activities related to a crime may have occurred” is too broad and promotes forum shopping.

Another commentator, Keith Uhl, CR-2014-0004-0003, raised the question whether the defense must travel to the first district to challenge the warrant.

The Subcommittee’s response. Rule 41(g) provides that a person aggrieved by an unlawful search may move for the property’s return in the district in which the property was seized. Alternatively, if an individual is indicted, he or she may move for the exclusion of the evidence in that proceeding.

D. Interaction with Title III

The ACLU, CR-2014-0004-0013, at 18-21, argued that the proposed amendment would authorize searches that can be carried out only pursuant to a warrant issued under the Wiretap Act, 18 U.S.C. § 2518 (Title III), or a surveillance warrant containing equivalent protections. Title III, the ACLU notes, provides special safeguards, requiring a preliminary showing that other investigative procedures have failed as well as minimization of non-pertinent communications. Remote access warrants, it argues, raise the same or analogous concerns (if, for example, the government seeks to activate a computer’s built-in camera), as well as additional concerns about “the unpredictable and irreversible damage to a target’s computer or data.” The ACLU argues, at 20, that “[a]ny malware, spyware, or other government software that remains on a target computer and collects information on an ongoing basis” implicates the concerns that require the safeguards of Title III. Further, hybrid orders cannot substitute for Title III. *Id.* The ACLU concludes, at 21, that adopting the amendment “risks facilitating violations of Title III and deciding by administrative rulemaking a question better left to Congress—how to regulate and circumscribe the controversial and invasive search techniques at issue here.”

Similarly, Google, CR-2014-0004-0029, expressed concern, at 9-10, that the network investigative techniques authorized by the proposed amendment could have “wide-ranging capabilities for accessing and engaging various features of the device, including the device’s camera and microphone, but the process under Rule 41 “may circumvent the ‘super warrant’ requirements of Title III.”

Michael Boucher, CR-2014-0004-0050, opposes the amendment, at 16-17, because it lacks the safeguards applicable to wiretaps under Title III. He asserts that it allows it does not . 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. He asserts that it allows “a gross intrusion into privacy” with only “a showing ‘that activities related to a crime may have occurred’ and that the target computer may have ‘evidence of a crime.’” (footnotes omitted). Further, he emphasizes, at 17, that unlike Title III the amendment is not limited to serious crimes.

NACDL similarly criticizes the proposed amendment, at 5, as being “unlike more measured and carefully considered legislative solutions like Title III, applying across the entire range of federal crimes and thus allowing federal agents to “hack into any number of computers, servers, storage accounts, laptops, and flash drives once an anonymous address had been exposed, whether the offense under investigation is commercial production and distribution of child pornography or a hit-and-run collision in the Veterans Administration hospital parking lot.”

***The Subcommittee’s response.* The Department of Justice has acknowledged, Tab F at 9, that “[a] Rule 41 search warrant does not permit law enforcement to intercept the communications covered by Title III, and “if investigators sought an order to intercept wire, oral or electronic communications, they would have to proceed by Title III rather than Rule 41 (or in addition to Rule 41, if stored information is sought as well).**

Further, under the proposed amendment “a showing ‘that activities related to a crime may have occurred’ and that the target computer may have ‘evidence of a crime’” is not sufficient to obtain a warrant. It establishes only venue for a warrant application. The government must also meet all other constitutional and statutory requirements to obtain a search warrant.¹

E. Extraterritorial Searches

Several commentators based their opposition in whole or part on the potential for remote searches authorized under proposed Rule 41(b)(6)(A) to reach devices or information outside of the United States. The Center for Democracy & Technology (CDT), CR-2014-0004-0009, argued at 3-4, that given global nature of the Internet and anonymizing technology, it is highly

¹Comment CR-2014-0004-0050 also stressed that Title II, unlike the proposed amendment, allows wiretaps only in investigations of serious offenses, such as sabotage of nuclear facilities, threats regarding weapons of mass destruction, sex trafficking of children, and other offenses “of comparable gravity.” *Id.* at 17, citing 18 U.S.C. §§ 2518(3)(a) and 2516. 18 U.S.C. § 2516 includes a large number of federal felonies that encompass a wide range of conduct, including mail and wire fraud, embezzlement, interstate transportation of stolen property, false statements on passport applications.

likely that warrants would be authorized for searches outside of the United States, in violation of international law and the sovereignty of other nations, as well as any applicable Mutual Legal Assistance Treaties (MLATs). CDT questioned whether a judge has the authority to issue a warrant for an extraterritorial search, noting ongoing litigation on a related issue. This concern was also raised by Bellotin et al., CR-2014-0004-0012, at 3.

Similarly, Google, CR-2014-0004-0029, asserted at 2-3 that “the nature of today’s technology is such that warrants issued under the proposed amendment will in many cases end up authorizing the government to conduct searches outside the United States.” In light of the traditional rule that the jurisdiction of law enforcement agents does not extend beyond a nation’s borders, it urges that “[s]uch a change is for Congress to effect, not the Committee.” *See also* Martin MacKerel, CR-2014-0004-0041 (opposing amendment because it dramatically expands law enforcement powers and “should be subject to robust public debate in the appropriate legislative forum,” rather than the subject of an administrative rule change).

Ahmed Ghappour, CR-2014-0004-0053, asserted at 1-4 that issuance of remote warrants when location is disguised by technological means “will necessarily result in extraterritorial cyber operations,” noting that more than 85% of the computers connected to the Tor network are *outside* the United States.” (Emphasis in original.) He characterized the amendment as “a radical shift” that “constitutes an enlargement of law enforcement’s substantive authority to conduct investigative activities overseas.” *Id.* at 1. Under the amendment, he urged, unilateral action will be the rule, rather than the exception, whenever an anonymous target happens to be outside the U.S.; “overseas cyber-operations will be unilateral and invasive; they will not be limited to matters of national security, nor will they be executed with the consent of the host country or with meaningful coordination with internal agencies.” *Id.* at 4. He argued that for this reason the amendment exceeds the powers granted by the Rules Enabling Act. *Id.* at 6-7. However, if the rule, is to be amended, he proposed “measures to minimize the encroachment on other states’ sovereignty, leaving open the possibility for diplomatic overtures,” requiring Network Investigative Techniques to return only country information first, prompting the executing FBI agent to utilize the appropriate protocols and institutional devices.” *Id.* at 7. Additionally, the rule (1) should require a preliminary showing that less intrusive investigative methods have failed or are unlikely to succeed, and (2) limit the range of techniques that are permitted to law enforcement trickery and deception that result in target-initiated access, and (3) limit search capabilities to monitoring and duplication of data on the target.

***The Subcommittee’s response.* To the extent a search warrant is required for a remote search, the proposed amendment provides the government an opportunity to apply for that warrant, an opportunity not available under the current Rule. It is the responsibility of the executive branch, not the judiciary, to execute the warrants, and to consider any requirements that may be imposed by treaties and mutual legal assistance agreements. The same is true, as Judge Raggi noted at the hearing, *id.* at 131-32, when the federal courts authorize arrest warrants for individuals whose locations may not be known. And, as Mr. Bitkower noted at the hearing, *id.* at 129, nothing in the proposed rule interferes with the government’s interest in inter-executive branch coordination on issues**

that may have foreign policy implications.

F. The Rules Enabling Act and the Limited Role of Rulemaking

Multiple commentators argued that the proposed amendment is a substantive expansion of the government's search capabilities that falls outside the rule-making authority conferred by the Rules Enabling Act. Google, CR-2014-0004-0029, asserted at 4-5, that the proposed amendment "invariably expands the scope of law enforcement searches, weakens the Fourth Amendment particularity and notice requirements, opens the door to potentially unreasonable searches and seizures, and expands the practice of covert entry warrants." It argues, *id.* at 5, that these are substantive changes that must be the work of Congress. It notes that the other provisions of Rule 41(b) that allow the issuance of out-of-district warrants were both authorized by Congress. *Id.* Similarly, it was Congress that authorized Title III wiretaps as well as legislation authorizing access to foreign intelligence information, electronically stored information, and real time telephony data. *Id.* Congress can debate and weigh various interests.

Other commentators made similar points. The Pennsylvania Bar Association, CR-2014-0004-0030, urged that the amendment "substantively expand the government's investigative powers," conferring authority for "a category of searches that the government is currently barred from conducting." These matters, it concludes, should be addressed by Congress. Ahmed Ghappour, CR-2014-0004-0053, asserted at 5-7 that by expanding the authority for power to conduct extraterritorial searches the amendment enlarges or modifies substantive rights. The National Association of Criminal Defense Lawyers (NACDL), CR-2014-0004-0038, argued at 2 that the amendment "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." NACDL states, at 3, that "[o]nly a Title III-like statutory regime, not a Rule amendment, can provide what is needed to render such searches reasonable in the context of the often unfamiliar and always transforming digital domain."

The Subcommittee's Response. Many of the comments argue that the proposal somehow expands the search and seizure authority of the government beyond what currently exists, thereby making a substantive change in the law that exceeds the Committee's authority under the Rules Enabling Act. But the proposal addresses only *which court* may consider a warrant application. The legality of every search remains a matter for courts to determine. Only warrants that meet the requirements of existing constitutional and statutory law can be issued lawfully, and designating the court that may consider whether those requirements are met is not a substantive change in the law. The proposed subsection operates just as the other subsections of Rule 41(b) in specifying venue for different types of warrants. The change removes a procedural impediment created by the language of the Rule itself, precisely the type of action delegated by Congress to the Courts under the Rules Enabling Act. It does no more.

G. The Potential For Collateral Damage

Several commentators stressed the danger that remote electronic searches could cause unpredictable, widespread and serious damage. Damage might be caused to the devices to be searched, as well as information and systems those devices. But many other devices, information, and systems may also be affected.

Bellotin et al., CR-2014-0004-0012, who are computer scientists, explain at 3-4 that software often fails and causes unanticipated problems; this occurred, for example, in the case of the Stuxnet attack on the Iranian nuclear centerfuge. Accordingly, they urge that it is imperative that warrant applications give the judge considering a remote warrant application the fullest possible information about the technology to be employed. The comment from Bellotin et. al. emphasizes the legal and technical danger of allowing the government to “to use a ‘common scheme to infect the victim computer with malware,’” at 1, citing the Committee Draft at 325. Bellotin et. al. have taken the quotation out of context. It is the Committee Note’s description of a botnet; it is not a description of the authority provided by the proposed amendment.

The Center for Democracy and Technology (CDT), CR-2014-0004-0009, stressed, at 7-9, that the consequences of executing a remote electronic warrant would be difficult to predict and may be very serious. Acts of intrusion may damage the device, data, or dependent systems. Network investigative techniques employ flaws or bugs in software, such as web browsers, to gain access, and may employ simple technology or much more intrusive methods. This may cause not only immediate damage, but also further damage resulting from increased vulnerabilities in the system. Similarly, the ACLU, CR-2014-0004-0013, at 9-12, expressed concern that the techniques used for the remote search can weaken devices, exposing them to compromise by third parties, and it emphasized that the government does not have a strong record of technological excellence. It also stressed that the availability of remote electronic search warrants would create an undesirable incentive for the government to acquire and use zero-day exploits that exploit vulnerabilities in common software and hardware, rather than notifying manufacturers to make changes to correct these vulnerabilities.

In its December 22, 2014 letter, Tab G, at 10-11, the Department of Justice noted that to date it has “balanced risks involved in technical measures against the importance of the objectives of an investigation in stopping crime and protecting public safety, and we have considered the availability and risks of potential alternative investigative avenues.” Accordingly, remote searches have been relatively uncommon, and “ave not resulted in the types of collateral damage that the commentators hypothesize.” The Department pointed to its ant-botnet initiatives as examples that brought substantial benefits while avoiding collateral damage to victims.

The Subcommittee’s Response. The amendment addresses only a narrow technical question: the venue for warrant applications. It removes a technical stumbling block that presently prevents the issuance of warrants that meet all other constitutional and statutory requirements.

H. Concerns about searches of victim computers

Access and the Electronic Frontier Foundation (Access and EFF), CR-2014-0004-0008, strongly oppose proposed (b)(6)(B), which would authorize a single warrant application in an investigation of a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5), when the media to be searched are protected computers that have been damaged in five or more judicial districts. This authority allows greater efficiency in the investigation of botnets. Access and EFF oppose the amendment on the ground that it expands the authority for searches and seizures beyond those who create and use unlawful botnets to those who are their victims. Access and EFF note that the victims of botnets are often journalists, dissidents, whistleblowers, lawmakers, world leaders and others in the U.S. and elsewhere, at 4. The amendment, they argue would subject the personal data of thousands of innocent users, as well as others who share a common server, to government surveillance. *Id.* at 5. These problems, they argue, are exacerbated by the government's overbroad application of the Computer Fraud and Abuse Act. *Id.* at 6-7. See also NACDL, CR-2014-0004-0038, at 8 (noting that (b)(6)(B) allows the privacy of "putative victims" to be invaded "with tools of unknown, but predictably harmful, effect").

The Subcommittee's response. The proposed amendment focuses only on venue. It does not relax the other constitutional requirements for searches and seizures. It does not subject all victim computers to remote electronic searches. The Subcommittee's proposed revision in the caption for Rule 41(b), which would clearly label these as provisions governing the "Venue for a Warrant Application" (or Professor Kimble's proposed alternative, "District from Which a Warrant May Issue") may help allay the concerns raised by Access and EPP. Their concerns regarding the scope of the Computer Fraud and Abuse Act fall beyond the Committee's authority under the Rules Enabling Act.

H. Concerns about Intrusions into the Constitutional and Statutory Rights of the Media

The Reporters Committee for Freedom of the Press, CR-2014-0004-0047, urges the rejection of the amendment on the grounds that would implicate the constitutional and statutory rights of journalists in multiple ways that should be addressed by Congress if they are to be altered. Citing 42 U.S.C. § 2000a, it also argues, at 2-3, that "any search of a journalist's computer or other electronic devices implicates the Privacy Protection Act of 1980 ("PPA"), which [with narrowly enumerated exceptions] prohibits searches and seizures of work product and documentary materials held by a person with 'a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication.'" It notes that the First and Fourth Amendment also protect journalists against searches of their communications and work product. It states, *id.* at 6-8, that journalists commonly use anonymizing technologies, such as TOR, to safeguard the confidentiality of their work product, communications, and sources, and it expresses concern that if journalists use these technologies, their work product, communications, and contacts will be subject to search "without probable cause to suspect them of a crime." The Committee also expressed concern, *id.* at 8-9, that remote access searches may

involve the impersonation of news media in a “watering hole attack,” when custom malicious code is installed on a website that is popular with the target group, and infects all who visit the site. Deception of this nature, it argues, compromises the credibility of the news media and is “unacceptable.”

The Subcommittee’s response. The proposed amendment, which governs only venue for warrant applications, is fully consistent with the limitations imposed by the PPA, which apply to all searches pursuant to Rule 41. Indeed, the PPA applies “[n]otwithstanding any other law.” The PPA does not, however, prohibit searches of persons not believed to be journalists at the time the search is executed. Rather, it is applicable imposes limitations on the search of “any work product materials *possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce*).

The Committee’s concerns about the impact of the amendment on journalists who use TOR and other anonymizing technologies appear to be based on the misunderstanding, noted above, that the proposed amendment would make use of anonymizing a sufficient basis for conducting a search or seizure. As noted above, however, the amendment affects only venue, leaving all other constitutional and statutory requirements unchanged.

The Committee’s concern about the propriety of employing deceptive techniques that may undermine the credibility of the news media falls beyond the scope of the procedural matters that fall within the Advisory Committee’s responsibilities.

III. RECOMMENDED CHANGES IN AMENDMENT AS PUBLISHED AND TRANSMITTAL TO THE STANDING COMMITTEE

The Rule 41 Subcommittee unanimously recommends that the Committee make the following changes in the proposed amendment and committee note as published, and that it forward the amended proposal to the Standing Committee:

A. New Caption for subdivision (b)

The Subcommittee’s new caption, “Venue for a Warrant Application,” lines 3-4, makes it clear that subdivision (b) identifies to the courts in which warrant applications may be considered. It does not, however, state the standards for the issuance of such warrants or relax the applicable constitutional requirements.

Following the Subcommittee’s third teleconference call, Professor Kimble suggested that as a matter of style it would be preferable to substitute “District from Which a Warrant May

Issue.” Unless the Committee believes there is a substantive difference between “Venue for a Warrant Application” and “District from Which a Warrant May Issue,” we would ordinarily adopt the language proposed by the Style Consultant.

B. Committee Note accompanying the new caption for subdivision (b)

The proposed Committee Note explains the reason for the amendment:

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.

C. Revision in Notice provision

The proposed revision on lines 39-42, are intended to implement the Committee’s decision to require notice of remote searches that would parallel the requirements for physical searches. As amended, the notice provision would provide:

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.

The amendment adds a requirement that the officer conducting a search must provide a receipt for property seized or copied, paralleling the requirement for physical searches on lines 32-34. The second change, lines 41-42, makes it clear that the required notice must be given to persons whose possessory interests were affected by the search, not persons who might claim other interests.

D. Committee Note Accompanying the notice provisions

The proposed Committee Note parallels the change in language on lines 39-42, and it also adds a cross reference to the existing provision restricting delayed notice. It provides:

Subdivision (f)(C)(1). 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).

TAB 3B

14 information located within or outside that district
15 if:
16 (A) the district where the media or information
17 is located has been concealed through
18 technological means; or
19 (B) in an investigation of a violation of
20 18 U.S.C. § 1030(a)(5), the media are
21 protected computers that have been
22 damaged without authorization and are
23 located in five or more districts.

24 * * * * *

25 **(f) Executing and Returning the Warrant.**

26 **(1) *Warrant to Search for and Seize a Person or***
27 ***Property.***

28 * * * * *

29 **(C) *Receipt.*** The officer executing the warrant
30 must give a copy of the warrant and a

31 receipt for the property taken to the person
32 from whom, or from whose premises, the
33 property was taken or leave a copy of the
34 warrant and receipt at the place where the
35 officer took the property. For a warrant to
36 use remote access to search electronic
37 storage media and seize or copy
38 electronically stored information, the
39 officer must make reasonable efforts to
40 serve a copy of the warrant and receipt on
41 the person whose property was searched or
42 who possessed the information that was
43 seized or copied. Service may be
44 accomplished by any means, including
45 electronic means, reasonably calculated to
46 reach that person.

47 * * * * *

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 also 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).

TAB 3C

**PROPOSED AMENDMENTS TO THE
FEDERAL RULES OF CRIMINAL PROCEDURE***

1 **Rule 4. Arrest Warrant or Summons on a Complaint**

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

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

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

17 * * * * *

18 (c) **Execution or Service, and Return.**

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

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

30 **(3) Manner.**

31 (A) A warrant is executed by arresting the
32 defendant. Upon arrest, an officer
33 possessing the original or a duplicate
34 original warrant must show it to the
35 defendant. If the officer does not possess
36 the warrant, the officer must inform the
37 defendant of the warrant's existence and of
38 the offense charged and, at the defendant's
39 request, must show the original or a
40 duplicate original warrant to the defendant
41 as soon as possible.

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

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

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

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

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

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

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

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

75 (a) stipulated by the parties;

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

79 submitted under an applicable
80 international agreement; or
81 (c) permitted by an applicable
82 international agreement.
83 * * * * *

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.

delivery” under subparagraph (F).

TAB 3D

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. 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. 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 than 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.

TAB 3E



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

October 20, 2014

MEMORANDUM

TO: The Honorable Reena Raggi
Chair, Advisory Committee on Criminal Rules

FROM: David Bitkower^{DB}
Deputy Assistant Attorney General

SUBJECT: Response to Post on Proposed Amendment to Rule 41

The Committee has asked the Department to respond to a September 16, 2014 post by Professor Ahmed Ghappour on the *Just Security* blog arguing that the Department's proposed amendment to Rule 41 would expand the extraterritorial surveillance authorities of the FBI.¹ We thank the Committee for this opportunity, and offer the following response.

The post's central premise is that the proposal expands the FBI's authority to access computers outside the United States. That premise is incorrect. The proposed amendment has no effect on the FBI's authorities outside the United States. As the Department explained in its September 18, 2013 letter to the Committee, the proposed amendment "does not purport to authorize courts to issue warrants that authorize the search of electronic storage media that is located in a foreign country or countries." Indeed, the amendment 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. Rather, with respect to anonymizing technology, it would only ensure that a judge is available to hear a search warrant application in a narrow category of cases where, under Rule 41's current venue provisions, that might not otherwise be the case because the nature of modern Internet crimes has frustrated the existing warrant process.

Overseas Authorities and Rule 41

In fact, with limited exceptions, the FBI's overseas authorities have nothing to do with Rule 41. In cases where the Fourth Amendment's warrant requirement applies, the procedures

¹ See <http://justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/>.

for obtaining a warrant in Rule 41 effectively limit the FBI's ability to conduct searches and seizures. But the Fourth Amendment's warrant requirement does not apply to searches outside of the United States, even searches of United States persons. Instead, such searches are evaluated under the Fourth Amendment's reasonableness requirement. *See United States v. Stokes*, 726 F.3d 880, 890-93 (7th Cir. 2013); *In re Terrorist Bombings*, 552 F.3d 157, 170-71 (2d Cir. 2008); *see also United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990) (describing a warrant issued by United States magistrate as "a dead letter outside the United States"). Because Rule 41 warrants are not required in the first place, the current venue limitations in Rule 41 do not limit the FBI's authority to conduct extraterritorial searches. A modification of those venue limitations, therefore, would not expand that authority.

As discussed in the Department's proposal, it is possible that a defendant may move to suppress evidence obtained from the search of computer media that proves to be outside the United States. In such a case, the government could point to the magistrate's determination of probable cause as part of its argument that the extraterritorial search was reasonable under the Fourth Amendment. But the issuance of the warrant in such a case would not have authorized any action the FBI was not already permitted to take under its current extraterritorial authorities.

Practical Considerations

Beyond its argument about expanded legal authorities, the post also makes the practical claim that the proposal will result in "overseas cyber operations [that are] unilateral and invasive." This argument is also incorrect. Nothing in the proposal changes the government's foreign policy considerations, which are also not governed by Rule 41, one way or the other. In fact, the Department of Justice (including the FBI) has long maintained internal protocols for handling investigations with potential overseas effects. But these practices are not mandated by Rule 41 – rather, the Department employs them because they are good policy. There is thus no basis to argue that the Department's practices in this regard would change if the proposed amendment to Rule 41 is adopted.

There may be cases in which it is impossible, without undertaking a remote search, to determine whether a computer that is involved in criminal conduct is located in the United States or abroad. This may be the case even though the conduct is in flagrant violation of American law. For example, pedophiles involved in the ongoing sexual exploitation of children, including American children, often use "hidden," or anonymized, websites to sell or exchange the child pornography that they have produced. In such cases, law enforcement authorities may be confronted with the choice of undertaking a remote search to locate the server that is hosting the website, potentially in another country – or permitting harmful criminal conduct to continue unabated. These are, unfortunately, precisely the cases in which international cooperation is least likely to be available, because there are no identifiable "local authorities" to ask for help. This problem predates our proposal and will continue to exist even if our proposal is adopted: as noted above, Rule 41 does not currently limit the FBI's authority to remotely access a computer outside the United States. What our proposal would accomplish is untying the hands of law enforcement when it is not yet known whether the Fourth Amendment requires a warrant because it is unknown whether the media is in the United States – and it accomplishes that by ensuring that a judge is available to hear the warrant application.

Additional Restrictions Are Unnecessary and Would Be Counterproductive

The Committee should reject the post's suggestions to impose unnecessary and unworkable restrictions on remote search authority in Rule 41, such as a requirement to search only for "country information." Restrictions on seizing evidence for which the government establishes probable cause are inconsistent with the role of a magistrate judge considering a warrant application. To the extent the computer media is in the United States, the scope of what can be seized should be governed by the same probable cause and particularity standards whether the data is taken from the computer by walking up to it or by connecting to it remotely. And to the extent there is a possibility that the computer media is not in the United States, and hence there is a theoretical foreign policy concern, the Federal Rules of Criminal Procedure are not the right mechanism to balance the foreign policy implications (if any) of proceeding with a search against the risk of conducting multiple searches of the same media, or of not searching at all. For example, in a given case it may be advisable to search only for location information; but in another case, there may be only one opportunity to employ a remote search, and a "location information-only" rule could thwart the investigation.

Second, the Committee should reject the recommendation that Rule 41 include a "necessity" requirement like that of the Wiretap Act for remote search warrants. Under this requirement, to obtain a warrant for a remote search, the government would first be required to demonstrate that other investigative methods have failed or are unlikely to succeed. But it would not be wise to use Rule 41 to enact a policy preference favoring, for example, physical intrusions into residences over remote searches of computers. Nor, as discussed above, do we think it would be consistent with the institutional advantages of the different branches of government to embed into the Federal Rules a foreign policy decision that requires magistrate judges to study and consider the international relations effects of various potential investigative steps – or investigative inaction, for that matter. *Cf. Zurcher v. Stanford Daily*, 436 U.S. 547, 552, 559 (1978) (reversing a district court ruling that had essentially adopted a necessity requirement for warrants, noting that "[t]he Fourth Amendment has itself struck the balance between privacy and public need" and rejecting the district court's attempt to "strike a new balance by denying the search warrant . . . on the theory that [a subpoena] is a less intrusive alternative"). Rather, courts should be authorized to issue warrants when the government satisfies the Fourth Amendment's probable cause and particularity requirements.

Finally, prohibiting the use of certain types of software to conduct remote searches would be out of place in a federal rule of procedure. As the Supreme Court has explained, "the details of how best to proceed with the performance of a search authorized by warrant" are "generally left to the discretion of the executing officers." *Dalia v. United States*, 441 U.S. 238, 257 (1979). There is no compelling reason for the Committee to limit such discretion, which must be employed on a case-by-case basis, and which of course remains subject to judicial review for reasonableness. *Id.* at 258; *see also United States v. Schesso*, 730 F.3d 1040, 1050 (9th Cir. 2013) (holding that magistrate judges may impose protocols on warrant execution and recognizing that the protocols "must be determined on a case-by-case basis").

Conclusion

The Department looks forward to further engagement on this issue during the public comment period. Please let us know if there is any further information we can provide to you.

TAB 3F



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

December 22, 2014

MEMORANDUM

TO: The Honorable Reena Raggi
Chair, Advisory Committee on Criminal Rules

FROM: David Bitkower *DB*
Deputy Assistant Attorney General

SUBJECT: Response to Comments Concerning Proposed Amendment to Rule 41

The Committee has asked the Department to address certain issues raised by commenters who presented testimony at a public hearing on November 5, 2014, regarding the Department's proposed amendment to Rule 41. We thank the Committee for the opportunity to address these issues.

As we have stated previously, the proposed amendment would ensure that a court has jurisdiction to issue a search warrant in two categories of investigations involving modern Internet crime: cases involving botnets and cases involving Internet anonymizing techniques. The proposal would do so by clarifying Rule 41's current venue provisions in these two circumstances. The proposal would not authorize the government to undertake any search or seizure or use any remote search technique not already permitted under current law. Certain of the comments received by the Committee have contested this assertion, but as discussed below, many of those comments appear to be misreading the text of the proposal or misunderstanding current law. We welcome the opportunity to clarify how the proposal would operate as a matter of law and practice.

First, we address concerns that warrants authorizing remote searches would violate the Fourth Amendment's particularity requirement. As with all search warrant applications, such concerns must ultimately be resolved through judicial determination on a case-by-case basis. We nevertheless explain here why we believe that remote search warrants can satisfy the Particularity Clause. To illustrate, we describe three investigative scenarios in which warrants for remote searches might be used, and we provide specific language that might be used for the "place to be searched" and "things to be seized" components of remote search warrants in these scenarios.

Second, we address concerns about the notice requirement of the proposed rule. Like the Rule 41 requirement for physical searches, the proposed amendment 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.

Third, we explain that the proposed amendment has no effect on the requirements of Title III. 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.

Fourth, we discuss the “concealed through technological means” requirement for obtaining a warrant pursuant to the proposed venue provision for remote searches. This requirement provides an appropriate and workable standard for obtaining a warrant for a remote search in cases involving Internet anonymizing technology. The 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.

Fifth, we note that the 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, just as it is careful to avoid injury to persons or damage to property in the far more common scenario of executing physical warrants. Although there is currently no Department regulation that specifically applies to the remote searches that would be conducted under the proposed amendment, such searches are scrutinized carefully, and they may be subject to other internal Department regulations depending on the circumstances.¹

Before addressing the substance of the comments in detail, we note that the commenters’ objections regarding issues such as particularity and notice do not relate to venue. Rather, they are general objections to obtaining and executing search warrants using certain remote search techniques. These objections are misplaced here because the proposed amendment is solely about the appropriate venue for applying for such warrants. The existing rules already allow the government to obtain and execute such warrants when the district of the targeted computer is known. Thus, the issue before the Committee is not whether to allow warrants to be executed by remote search; it is whether such warrants should as a practical matter be precluded in cases involving anonymizing technology due to lack of a clearly authorized venue to consider warrant applications. Finally, we note that none of the commenters who expressed opposition to the proposal offered any substantive alternative solution to provide venue for a search warrant application when the district in which the targeted computer is located is unknown.

Particularity requirement for remote search warrants

We believe that search warrants authorizing remote searches can satisfy the Fourth Amendment’s particularity requirement. A number of magistrate judges have issued warrants for remote searches, and those judges have been satisfied that the warrants fulfilled the

¹ This letter does not address potential international issues associated with the proposed amendment, as those concerns were previously addressed by the Department in a letter dated October 20, 2014.

requirements of the Fourth Amendment.² As an initial matter, however, we note that the law regarding the particularity requirement for remote searches cannot be resolved by the Rules Committee; it must develop, as it does for all search warrants, through judicial resolution of specific, concrete cases. As the Committee Note to the proposed amendment states, “[t]he 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.”

Nevertheless, because several commenters raised concerns about the particularity of remote search warrants, we discuss how remote search warrants can satisfy the Fourth Amendment’s particularity requirement.³ In addition to discussing relevant doctrine regarding the Fourth Amendment’s particularity requirement, we will describe three investigative scenarios and explain how warrants can be drafted in those scenarios to satisfy the Fourth Amendment.

The particularity requirement of the Fourth Amendment demands that “warrants must particularly describe the things to be seized, as well as the place to be searched.” *Dalia v. United States*, 441 U.S. 238, 255 (1979) (internal quotation marks omitted); see also *United States v. Grubbs*, 547 U.S. 90, 97 (2006).⁴ The particularity requirement “makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another.” *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (quoting *Stanford v. Texas*, 379 U.S. 476 (1965)). “As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927).

Describing the information to be seized pursuant to a remote search warrant need not be complicated. The warrant specifies evidence of crime that can be obtained through access to the targeted computer. For warrants in investigations of crime involving use of Internet anonymizing technology, this evidence will usually be information that helps to identify the suspect. For example, the MAC address and IP address of a computer help identify the computer and its owner.

² For example, in one recent investigation, the government sought a search warrant to help identify computers used to access a child pornography hidden service on Tor. The magistrate judge issued a warrant for the search; in the subsequent criminal prosecution, the district court denied a motion to suppress challenging the warrant. See *United States v. Cottom*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #155) (denying suppression motion), (Doc #122, Attachment 1) (search warrant).

³ Commenters including the Center for Democracy and Technology (“CDT”) and the ACLU recommend that Congress address whether to authorize warrants for remote searches. See CDT Memorandum at 11; ACLU Memorandum at 28. This recommendation suggests that these commenters agree that such searches can, in principle, comply with the Fourth Amendment; otherwise any Congressional action would be futile.

⁴ The scope of the particularity requirement does not extend to describing how a warrant will be executed. The Supreme Court has explained that “[n]othing in the language of the Constitution or in this Court’s decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed.” *Grubbs*, 547 U.S. at 98 (quoting *Dalia*, 441 U.S. at 255).

Because the physical location of the place to be searched by remote access is typically unknown, remote search warrants usually describe the place to be searched through some other means designed to specify the particular account or computer that officers have probable cause to search. For example, when investigators have the ability to send an email to the suspect, the place to be searched could be described as the computer used to access and open the email sent to the suspect.

Some commenters argue that a search warrant can satisfy the Fourth Amendment's particularity requirement only if it specifies the physical location of the computer to be searched. This argument is mistaken: the Supreme Court has made clear that the particularity requirement does not preclude use of warrants where the purpose of the search is to discover the location of the place to be searched. In *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court held that a warrant for a tracking device could satisfy the Fourth Amendment despite the fact that the purpose of the warrant was to determine the place to be searched:

The Government contends that it would be impossible to describe the "place" to be searched, because the location of the place is precisely what is sought to be discovered through the search. . . . However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance.

Id. at 718. These same principles apply to warrants for remote searches. The government may satisfy the Fourth Amendment with respect to a remote search warrant by describing the computer or web server to be searched (for example, the computer that is used to access and open a particular email message, or the web server hosting a particular hidden web site), the circumstances that justify the search, the information that will be obtained through the search, and the time period during which the search may be conducted. None of these things require knowledge of the physical location of the object of the search.

The ACLU also objects that the "proposed amendment would allow police to remotely search many people's computers using a single warrant," *see* ACLU Memorandum at 21, but the law it cites regarding multi-location search warrants makes clear that such warrants may in fact comply with the Fourth Amendment. "A search warrant designating more than one person or place to be searched must contain sufficient probable cause to justify its issuance as to each person or place named therein." *Greenstreet v. County of San Bernardino*, 41 F.3d 1306, 1309 (9th Cir. 1994) (quoting *People v. Easley*, 671 P.2d 813, 820 (Cal. 1983)). Courts can address the extent to which this rule applies to remote search warrants in the usual manner, just as they would in the case of warrants for physical searches: through judicial resolution when the issue arises in specific cases. In any event, even if there were a rule requiring the use of a separate warrant for every location to be searched, the proposed amendment would not modify that rule. Rather, it merely provides a venue for a court to decide whether a warrant application satisfies the Fourth Amendment.

Particularity requirement: sample warrant language

To illustrate how remote search warrants can satisfy the Fourth Amendment, it is helpful to describe their use in several investigative scenarios. Here, we will discuss three scenarios: a drug trafficker using an email account offered through a Tor hidden service, a fraud scheme facilitated by email, and a child pornography group. For each, we will explain how two key elements of the warrant – the place to be searched and the items to be seized – can be drafted in compliance with the Fourth Amendment.

Warrant scenario 1: obtaining stored email content from a hidden email provider by using a username and password

It is worth noting at the outset that the proposal does not relate only to remote searches conducted through the use of special software or computer exploits. A warrant for a remote search under the proposed amendment could closely resemble a search warrant of the sort that is routinely issued by magistrate judges across the country. Suppose that in executing a Rule 41 warrant on the home of a drug trafficker, agents discover the user name and password for an email account hosted on a Tor hidden service that the target uses to advertise and sell drugs. Investigators would like to search the account for evidence, but they likely will not know the location of the server hosting the account, and they cannot serve the email provider with a standard email search warrant under 18 U.S.C. § 2703 as they would with a commercial service provider. Instead, investigators would like to access the email account themselves using the user name and password that they have discovered. Doing so will not require use of any special or otherwise sensitive software.

A warrant authorizing a search of the drug trafficker's email account will comply with the Fourth Amendment. First, the affidavit in support of the warrant can present facts sufficient to establish probable cause that the target has used the account in connection with his crimes and that there is reason to believe that the account will contain information related to that activity. Second, the search warrant will specify the place to be searched. For example, the warrant can state that the place to be searched is the "target account on the target computer," defined as "the account associated with [username] that is stored on the server hosting [the specified Tor email service]." The affidavit can also explain that investigators intend to log on to the account directly in order to execute the warrant. Third, the warrant will specify the information to be obtained from the account, such as particularly-described information that constitutes evidence of drug trafficking within a specified date range. Such a warrant will comply with the Fourth Amendment and would not present any novel particularity issues.

Warrant scenario 2: identifying a criminal using a web-based email account

Criminals frequently use web-based email accounts, such as Gmail, Yahoo, or Hotmail accounts, to send and receive communications related to their criminal activity. For example, a fraudster will want to use a seemingly "normal" email address to communicate with a potential victim. Investigators can typically determine the IP address that was used to access a web-based email account at a particular time by serving a subpoena on the email provider. But criminals can hide their true IP address from their service providers and the government through

anonymizing techniques such as use of a proxy server.⁵ In such circumstances, investigators may be able to use a Network Investigative Technique (“NIT”) to identify the criminal’s true IP address.

Suppose, for example, that investigators become aware that a fraudster is communicating with a victim through a web-based email account, and that the fraudster is trying to persuade the victim to wire him a large sum of money. In addition, investigators determine that the fraudster accesses his email account only using proxy servers. With the assistance of the victim, investigators can send an email containing a NIT from the victim’s email account to the fraudster’s email account. If the fraudster accesses the email, the NIT will cause the fraudster’s computer to send identifying information, such as the computer’s true IP address, to investigators.⁶

A warrant authorizing use of a NIT in such a manner can satisfy the Fourth Amendment. First, the affidavit in support of the warrant can present facts sufficient to establish probable cause that the fraudster is committing a crime, that he is using a computer to do so, and that the identity and location of the fraudster and the computer will constitute evidence. Second, the search warrant will specify what computer will be searched. For example, the warrant can state that the place to be searched is the “target computer,” defined as “the computer that accesses [the fraudster’s email account] and retrieves an email that will be sent to that account from [the victim’s email account] in furtherance of this warrant.” Third, the warrant will specify the information to be obtained from the computer. For example, the warrant could state that the information to be obtained is: “the target computer’s actual IP address, and the date and time that the NIT determines that IP address; and the target computer’s MAC address and host name.” This information would assist investigators in identifying the physical location and owner of the computer. Such a warrant will comply with the Fourth Amendment.

Warrant scenario 3: investigating members of a child pornography group

Many producers and traffickers of child pornography rely on Internet anonymizing techniques, in particular the Tor network, to hide from law enforcement. As an example, suppose that law enforcement becomes aware of a password-protected Tor website dedicated to the production, receipt, and distribution of child pornography. As explained on the publically-accessible part of the website and corroborated by an undercover agent’s attempt to access the site, an individual can only obtain a user account and password necessary to access the website by providing the site administrator with samples of newly created images of child pornography. Because of the strict rules governing access to the website, there is probable cause to believe that anyone who uses a password to access the site is engaged in the ongoing abuse of children and the production, distribution, and possession of child pornography. Investigators thus seek to

⁵ Frequently, criminals route their communications through proxy servers that openly advertise the fact that they do not maintain records.

⁶ This type of warrant is analogous to an anticipatory warrant to search the residence of a person who accepts a package containing contraband, even if the precise residence is not known at the time the warrant is obtained. *See, e.g., United States v. Dennis*, 115 F.3d 524, 528 (7th Cir. 1997) (anticipatory warrant to search whichever of two apartments belongs to the individual who accepts delivery or opens a particular package containing drugs).

identify the location of the individuals accessing the site. They intend to do so by sending a NIT to each computer used to log on to the website using a password during a specified time period. Each NIT will then send identifying information from each computer back to the investigators.

A warrant authorizing such searches can be written to comply with the Fourth Amendment. First, the affidavit in support of the warrant would set forth the facts described above, establishing probable cause that each computer used to access the website (or portion of the website) in question will contain evidence of a crime. Second, the search warrant authorizing the use of the NIT will specify the places to be searched. The warrant can state that the places to be searched are the “target computers,” which are “the computers used to log on to [the child pornography website] with a valid password during [specified time period] and to which a NIT will be sent pursuant to this warrant.” Third, the warrant will specify the information to be obtained. For example, the warrant can state that the information to be obtained is: “for each target computer, the actual IP address, and the date and time that the NIT determines that IP address; and the target computer’s MAC address and host name.”

The ACLU calls this technique a “watering hole attack” and suggests that it may violate the Fourth Amendment. *See* ACLU Memorandum at 22. The Department disagrees both with that label and with the legal conclusion.⁷ As discussed above, when investigators can establish probable cause to search multiple locations, the Fourth Amendment allows investigators to obtain a warrant to search them. *See, e.g., United States v. Johnson*, 26 F.3d 669, 692 (7th Cir. 1994); *Greenstreet*, 41 F.3d at 1309. And by the same token, if investigators cannot establish probable cause to search a particular location, then they will not be able to obtain a warrant to authorize the search of that location. Nothing in the proposed amendment would hold otherwise.

As these three hypothetical scenarios demonstrate, warrants executed by remote search can satisfy the Fourth Amendment. We do not doubt that one could also conjure up hypothetical instances in which a remote warrant would *not* satisfy the Fourth Amendment. But that is beside the point because the proposed amendment would not authorize such searches. What the proposed amendment would do is ensure that a court is available to determine whether a specific warrant application satisfies the Fourth Amendment or not.

Notice requirement for remote search warrants

The proposed amendment’s notice requirement mandates that when executing a warrant for a remote search, “the officer must make reasonable efforts to serve a copy of the warrant on the person whose property was searched or whose information was seized or copied,” and that

⁷ The term “watering hole” attack is generally used to describe a technique whereby criminal hackers implant a virus on a widely-used website and cause it to infect large numbers of users who may not be of interest to the hackers, in hopes that the virus will also infect a smaller number of users who are of specific interest to the hackers. *See, e.g.,* <http://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-hole-sites>. By contrast, the search described in this scenario is – and by definition must be – targeted based on probable cause. The ACLU also asserts in its comment that the FBI performed such a “watering hole attack” on a particular Tor-based server known as Freedom Hosting that “forc[ed] all of the Freedom Hosting sites to deliver malware to visitors, not just those sites that were engaged in the distribution of illegal content.” ACLU Memorandum at 15. This assertion appears to be based on Internet rumor.

“[s]ervice may be accomplished by any means, including electronic means, reasonably calculated to reach that person.” Commenter EPIC asserts that this amendment authorizes surreptitious searches without a showing of need for the delay, *see* EPIC Memorandum at 7, but EPIC is misreading the proposed rule. The proposed amendment, as a default matter, requires officers to make reasonable efforts to give notice of the warrant at the time the warrant is executed.

The proposed amendment does not modify the delayed-notice statute. If investigators seek to delay notice of a warrant executed by remote search, they will be required to follow the existing delayed-notice procedures and meet the existing delayed-notice standard of 18 U.S.C. § 3103a. Under that statute, in order to authorize delayed notice, the issuing court must find “reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial).” 18 U.S.C. § 3103a(b)(1). This standard will be the same for remote searches as it is for physical searches. In addition, a court cannot authorize the seizure of either physical evidence or electronic information pursuant to a delayed-notice warrant without a judicial finding of reasonable necessity. *See* 18 U.S.C. § 3103a(b)(2) (requiring that a delayed-notice warrant must prohibit “the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure”). Again, this provision treats “stored wire or electronic information” that will be obtained by a remote search in precisely the same manner as “any tangible property.” The Department has interpreted “seizure . . . of any stored wire or electronic information” in Section 3103a(b)(2) broadly to include the copying of information stored on a computer. Finally, unless a longer period of delay is justified by the facts of the case, Section 3103a will allow for an initial 30-day period of delayed notice for a remote search warrant, with possible extensions of up to 90 days each. *See* 18 U.S.C. § 3103a(b), (c).⁸

The Department anticipates that it will seek judicial approval to delay notice in many of the cases in which it seeks a warrant for a remote search. This is so because, as described above, such warrants will often be sought when investigators are trying to identify or locate an online criminal who is taking steps to avoid identification. Such circumstances will typically provide reasonable cause for delaying notice of the search, but notice will be delayed only where appropriate under existing rules. For example, in *United States v. Cottom*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #155) (denying motion to suppress), investigators invoked Section 3103a to delay notice of a remote search warrant through which they identified users of a Tor-based hidden service child pornography website. The court held that “the 30-day delayed notice, under the facts of this case, did not create any violation of Rule 41.” *Id.* at 8.

⁸ Under the proposed amendment, the rules for delaying notice for warrants for remote searches will be more demanding than the existing rules for delaying notice for tracking device warrants. For a tracking warrant, the government need not provide notice of the warrant for up to ten days after the tracking has ended, and no showing of need is required for that initial period of delay. *See* Fed. R. Crim. P. 41(f)(2)(C). Because tracking warrants can last for 45 days, *see* Fed. R. Crim. P. 41(e)(2)(C), notice of a tracking warrant can therefore be given 55 days after the initial search without any showing of need for the delay.

The proposed amendment requires officers to make “reasonable efforts” to provide notice of a warrant. This standard recognizes that in some cases – particularly cases in which the location of the computer has been concealed – the officer may be unable to provide notice of the warrant. For example, even after officers conduct a remote search, they may still lack sufficient information to identify or contact the owner of the searched computer. The “reasonable efforts” language recognizes that there may be unusual difficulty in providing appropriate notice in cases where the district in which the computer is located is unknown; by contrast, if the government can provide notice using reasonable efforts, the rule will require it to do so. As the Supreme Court stated in *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995), “[t]he Fourth Amendment’s flexible requirement of reasonableness should not be read to mandate a rigid rule of announcement that ignores countervailing law enforcement interests.” As with other notice issues under the Fourth Amendment, the reasonableness of the government’s efforts to provide notice must be evaluated on a case-by-case basis.

Finally, the proposed amendment requires that a copy of the warrant be served on “the person whose property was searched or whose information was seized or copied” (emphasis added). This approach is consistent with Rule 41’s existing requirements for both standard search warrants and for tracking device warrants. See Fed. R. Crim. P. 41(f)(1)(C), (f)(2)(C); *United States v. Zacher*, 465 F.3d 336, 339 (8th Cir. 2006) (warrant for FedEx package). When the government executes a Rule 41 warrant in the physical world, it is not obliged to provide notice to everyone with a potential privacy interest in the place searched. For example, if the search of a house includes the search of a locked trunk stored at the house by a friend of the house’s owner, law enforcement has never been required to seek out and give notice of the warrant to the owner of the trunk. Similarly, if investigators execute a remote search warrant on a computer used to access a specified email account, and the computer turns out to belong to the suspect’s friend, the government should be able to satisfy its notice obligation – as it would in the physical world – by providing notice to the friend.

Interaction between the proposed amendment and Title III

The proposed amendment to Rule 41 would not affect law enforcement’s obligations to comply with the Wiretap Act, 18 U.S.C. §§ 2510-2522 (“Title III”). Title III generally requires a wiretap order to intercept⁹ wire, oral, or electronic communications, unless one of several statutory exceptions apply. See 18 U.S.C. § 2511. A Rule 41 search warrant does not permit law enforcement to intercept such communications, and nothing in the proposed amendment suggests otherwise. Thus, the ACLU is mistaken to assert that the proposed amendment “authorizes searches that can only be carried out pursuant to a Title III wiretap order.” ACLU Memorandum at 18. For example, if investigators sought an order to intercept wire, oral or electronic communications, they would have to proceed by Title III rather than Rule 41 (or in addition to Rule 41, if stored information was sought as well).

⁹ The Wiretap Act defines “intercept” to mean the “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). Communications are intercepted within the meaning of Title III when they are acquired contemporaneously with transmission. See, e.g., *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 460-63 (5th Cir. 1994).

Concealed through technological means

Under the proposed amendment, a magistrate judge in a district where activities related to a crime may have occurred will have authority to issue a warrant for a remote search if the location of the computer to be searched “has been concealed through technological means.” This “concealed through technological means” requirement provides an appropriate standard for obtaining warrants for remote searches. An officer seeking a warrant for a remote search can satisfy this component of the court’s jurisdiction to issue the warrant through an affirmative factual showing regarding the criminal’s conduct – for example, the criminal’s use of Tor to distribute child pornography. Alternative formulations of the proposed amendment, such as a requirement that the location of the computer to be searched be unknown, would likely lead to excessive *Franks* hearings on whether agents had disclosed every fact that might have suggested a possible location of the criminal’s computer; such formulations could also draw courts into determinations of whether investigators had taken appropriate steps to determine the location of the computer to be searched. In its current form, the proposed amendment provides a workable and reasonable standard for obtaining warrants for remote searches that is less likely to result in excessive litigation.

Commenter Center for Democracy and Technology (“CDT”) argues that the “concealed through technological means” standard is overly broad, *see* CDT Memorandum at 6, but its argument is based on a misunderstanding of the requirements for obtaining a criminal search warrant. CDT states that “[I]legitimate uses of technology that have the effect of ‘concealing through technological means’ a user’s location . . . should not trigger the ability for a judge to issue a Rule 41 warrant.” *Id.* at 7. Under the proposed amendment, however, investigators could not obtain a search warrant merely because a user’s location is concealed through technological means. Rather, the warrant application must also demonstrate probable cause that the search will uncover evidence, fruits, or instrumentalities of crime. *See* Fed. R. Crim. P. 41(c). The proposed amendment does not alter that rule, but instead provides an alternative means of satisfying Rule 41’s venue provisions. Standing alone, the use of Internet anonymizing techniques to conceal location does not provide a basis for obtaining a search warrant.¹⁰

Avoiding collateral damage and internal Department of Justice policies

Some commenters raised concerns about the possibility that the Department’s use of remote searches could damage a targeted computer or other computer systems. The Department is mindful of the impact that remote search software has on computers, and we are careful in our use of remote searches, just as we are careful to avoid injury to persons or damage to property in the far more common scenario of executing physical search warrants. In our efforts to date, we have balanced risks involved in technical measures against the importance of the objectives of an investigation in stopping crime and protecting public safety, and we have considered the

¹⁰ CDT is also concerned that a warrant could be issued when a user conceals location through a means that is “not technically technical,” such as misreporting of the city of residence in a Facebook profile. CDT Memorandum at 7. The language of the proposed amendment, however, requires that the location of the relevant “media or information” be concealed through “technological means.” It is unclear to us how misrepresenting one’s city of residence on Facebook would conceal the location of media or information subject to search in the first place, much less through technological means.

availability and risks of potential alternative investigative avenues. As a result of this caution, although remote searches are relatively uncommon, the searches we have undertaken have not resulted in the types of collateral damage that the commenters hypothesize. Such careful consideration of any future technical measures will continue.

Similarly, the successes of the Department's anti-botnet initiatives demonstrate that our efforts in the cyber realm can bring substantial benefits while avoiding collateral damage to victims. The Department, often in collaboration with public and private sector partners, has conducted technical operations pursuant to court authorization to disrupt and dismantle several botnets infecting computers of innocent users, including the Coreflood¹¹ and Gameover Zeus¹² botnets. The results of these operations demonstrate that our technical efforts have resulted in substantial benefits for computer users victimized by online crime, rather than any undue collateral damage.

Currently, the remote searches that would be applied for under the amended rule are not subject to mandatory internal regulation at the Department. However, remote searches may implicate other existing Departmental guidelines and regulations depending on the circumstances. Additionally, the FBI is required to adhere to the Attorney General's Guidelines for Domestic FBI Operations ("AGG-DOM") and the FBI's Domestic Investigations and Operations Guide ("DIOG") in conducting remote searches, and those guidelines require that the FBI use the least intrusive method available in conducting a search.¹³ Section I(C)(2)(a) of the AGG-DOM provides:

The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of different investigative methods that are each operationally sound and effective, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and potential damage to reputation. The least intrusive method feasible is to be used in such situations. It is recognized,

¹¹ In Operation Coreflood, the FBI worked with private sector and law enforcement partners to disable a botnet that had infected an estimated two million computers with malicious software. The malware on the Coreflood botnet allowed infected computers to be controlled remotely by criminals to steal private personal and financial information from unsuspecting users. The FBI obtained a court order to seize domain names, re-route the botnet to FBI-controlled servers, and stop the Coreflood software from running.

¹² Gameover Zeus, believed to have infected approximately 500,000 to one million computers worldwide and to have caused losses of over \$100 million, is an extremely sophisticated type of malware designed to steal banking and other credentials from the computers it infects. Those credentials are then used to initiate or redirect wire transfers to accounts overseas. The government obtained civil and criminal court orders in federal court in Pittsburgh authorizing measures to sever communications between the infected computers and criminal servers, and redirect them from the criminal servers to substitute servers under the government's control.

¹³ Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM), Sec. I(C)(2)(a); Domestic Investigations and Operations Guide (DIOG), Sec. 18.2.

however, that the choice of methods is a matter of judgment. The FBI shall not hesitate to use any lawful method consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of foreign intelligence sought to the United States' interests. This point is to be particularly observed in investigations relating to terrorism.

Likewise, Section 18.2 of the DIOG provides, "The AGG-DOM requires that the 'least intrusive' means or method be considered and—if reasonable based upon the circumstances of the investigation—used to obtain intelligence or evidence in lieu of more intrusive methods." The DIOG also contains a section providing extensive and detailed guidance on making least intrusive method determinations.¹⁴ Although the least intrusive methods requirement is primarily designed to address privacy and civil liberties concerns, its principles apply to avoiding collateral damage in remote searches as well and inform, among other things, the way in which a NIT is designed (so as to minimize the likelihood of damage), its capabilities, and the manner in which it is used.

Most remote searches are unlikely to have any significant lasting effect on the integrity of a targeted computer. In any case, as the Supreme Court has recognized, "the details of how best to proceed with the performance of a search authorized by warrant" are "generally left to the discretion of the executing officers." *Dalia*, 441 U.S. at 257. Subsequently, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Id.* at 258. This same standard would apply to any damage caused by officers executing a warrant by remote search. In addition, as with all investigative techniques, the Department will scrutinize the use of NITs, and the Department may in the future choose to impose additional regulations on their use.

- - -

We appreciate the opportunity to respond to issues raised by commenters on the proposed amendment to Rule 41. We look forward to further discussions with the Committee. Please let us know if there are other issues or concerns which you would like the Department to address.

¹⁴ DIOG § 4.4. The section includes subsections entitled, "General Approach to Least Intrusive Method Concept," Section 4.4.2; "Determining Intrusiveness," Section 4.4.3; and "Standard for Balancing Intrusion and Investigative Requirements," Section 4.4.4.

TAB 3G



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

February 20, 2015

MEMORANDUM

TO: The Honorable Reena Raggi
Chair, Advisory Committee on Criminal Rules

FROM: David Bitkower *DB*
Deputy Assistant Attorney General

SUBJECT: Additional Response to Comments Concerning Proposed Amendment to Rule 41

The Committee has asked the Department to address recent comments received in opposition to the Department's proposed amendment to Rule 41. We thank the Committee for the opportunity to address these comments. Because many of the comments reiterate concerns raised by other commenters and previously addressed by the Department, we will not fully repeat our discussion of those issues here.¹

The Rules Committee is an appropriate forum to address venue for warrant applications.

Several comments, including comments from Google and the Pennsylvania Bar Association ("PBA"), argue that the proposal expands the government's investigative authority and therefore should only be addressed by Congress. The Department believes that these arguments are mistaken for multiple reasons.

First, the criticisms appear to misunderstand what is at stake in the proposal. As the Department has repeatedly emphasized, the proposal would not authorize the government to undertake any search or seizure or use any remote search technique not already permitted under current law. Rather, the proposed amendment would merely ensure that some court is available to *consider* whether a particular warrant application comports with the Fourth Amendment. Google characterizes the proposal as impacting substantial rights, Google Memo at 4, but

¹ For example, Google's memo at pages 1-4 addresses international issues. The Department addressed these issues in its letter to the Committee dated October 20, 2014, which explained that a warrant is not required to conduct searches outside the United States. Google's memo at pages 8-10 addresses particularity, collateral damage, Title III, and notice; the Department addressed each of these issues in its letter to the Committee dated December 22, 2014.

provides no support for this claim; there is no substantive right to be free from a search warrant that complies with the Fourth Amendment. Because only warrants that meet the relevant substantive legal requirements can be lawfully issued by a court, a rule concerning which court can consider applications cannot accurately be said to be substantive.²

Second, it is entirely proper for the Rules Committee to address the appropriate venue for issuing a search warrant. Indeed, the Committee did so in 1990 (creating what is now Rule 41(b)(2) governing property that may move out of the issuing district after the warrant is issued), and it did so more recently in 2006 (creating Rule 41(b)(4) to provide venue to issue tracking warrants) and 2008 (creating Rule 41(b)(5) to provide venue to issue warrants for, among other places, diplomatic and consular missions). Accordingly, Google's assertion that the proposed amendment would violate the Rules Enabling Act is also incorrect.³

Third, certain commenters suggest that law enforcement generally should not be permitted to use new investigative techniques absent congressional approval. This suggestion is incorrect on two counts. Initially, the premise underlying the suggestion is incorrect because the use of remote searches is not new (as other commenters have pointed out), and warrants for remote searches are currently issued under the Federal Rules. Moreover, there is not and has never been a practice of forswearing the use of "new" techniques absent congressional approval. As one example, Congress has never specifically authorized video surveillance warrants, but courts have appropriately approved such warrants under Rule 41. *See, e.g., United States v. Falls*, 34 F.3d 674, 678-83 (8th Cir. 1994); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987). The Supreme Court also approved warrants to collect dialing information from telephones long before Congress enacted the Pen Register and Trap and Trace statute. *See United States v. New York Tel. Co.*, 434 U.S. 159 (1977). Nor has Congress passed statutes governing other investigative techniques that may be judicially authorized via search warrant, ranging from thermal imaging to the compulsory taking of a DNA sample. A rule that law enforcement cannot use a new investigative technique absent specific congressional authorization would thus be both inconsistent with historical practice and unwise.

Finally, the Rules Committees and the Judicial Conference, which exercise authority delegated by Congress over federal court procedures, have repeatedly counseled the Department to raise procedural issues with the appropriate Rules Committee first, rather than directly with Congress. Congress delegated to the courts "the power to prescribe general rules of practice and

² Google also argues that that Rule would impact substantial rights because it would weaken Fourth Amendment protections. Google Memo at 4-5. But an amendment to the rules cannot limit the application of the Fourth Amendment, and courts will address constitutional issues associated with remote search warrants on a case-by-case basis, just as they do with physical warrants.

³ Google appears to argue that the 2008 amendment was attributable to Congress and not the Committee because seven years prior to that amendment Congress authorized the prosecution of certain criminal offenses taking place in a subset of the locations in which the amendment later authorized searches. This logic does not follow. In any event, the 2008 amendment clarified venue to issue warrants in investigations of crimes defined by Congress, which is exactly what the proposed amendment would do here.

procedure.” 28 U.S.C. § 2072. Of course, Congress continues to exercise oversight over the rules, and no new rule goes into effect until Congress is given the opportunity to review it. And should Congress determine that additional regulation of remote searches is desirable, it can enact legislation to provide such regulation. But the Department shares the Judiciary’s view that congressional consideration of this important issue, which will follow passage of any amendment, will benefit greatly from this Committee’s work. We therefore believe that following this standard practice to amend the Federal Rules of Criminal Procedure with respect to venue for search warrant applications is entirely appropriate in this circumstance.

The language of the proposed rule is not vague.

The National Association of Criminal Defense Lawyers (“NACDL”), Google, and commenter Michael Boucher argue that certain language in the proposed amendment is either vague or too broad, including the phrases “in any district where activities related to a crime may have occurred,” “remote access,” and “concealed through technological means.” The Department believes that each of these phrases is appropriately clear and limited.

The Department addressed the scope of the phrase “concealed through technological means” in its December 22, 2014 memorandum, and we will not fully repeat that discussion here. However, because many commenters appear to have misunderstood this point, we again take the opportunity to note that under the proposed amendment, investigators could not obtain a search warrant merely because a user’s location is concealed through technological means. Rather, the warrant application must also demonstrate probable cause that the search will uncover evidence, fruits, or instrumentalities of crime. *See* Fed. R. Crim. P. 41(c). Nothing in the proposed amendment would affect the existing probable cause requirement or any other substantive requirement to issue a warrant. By the same token, satisfaction of the “concealed through technological means” requirement would not by itself result in issuance of a warrant, but rather merely identify which subpart of the rule would govern which court was empowered to consider the warrant application in the first instance.

The NACDL objects that the phrase “in any district where activities related to a crime may have occurred” is vague. This language, however, was copied verbatim from the existing Rule 41(b)(3) and (b)(5). The Department believes that using existing language where possible minimizes confusion and uncertainty in the interpretation of the Rules. To the extent that there is any ambiguity in this phrase – and we doubt there is much – courts can give appropriate meaning to this language in the context of specific facts.⁴

Google asserts that the proposed amendment is vague because it does not limit or specify how “remote access” searches are conducted. But the Supreme Court has repeatedly specified that “[n]othing in the language of the Constitution or in this Court’s decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed.” *United States v. Grubbs*, 547 U.S. 90, 98 (2006) (quoting *Dalia v. United States*, 441 U.S. 238, 255 (1979)). The Department believes that the meaning of “remote access” is clear. The dictionary defines “remote” as “far away; distant.”

⁴ Google similarly objects to use of the word “media,” but that word is also adopted from the language of the current rule.

New Oxford American English Dictionary 1433 (2nd ed. 2005). The term “remote access” means that the search will not be conducted by agents physically accessing the media, but rather by agents connecting to the computer remotely – from far away – such as through a network.

The botnet amendment is appropriate.

We continue to believe that the portion of the proposal addressing botnets is important and appropriate despite objections raised by Google, NACDL, and Michael Boucher. Again, the botnet proposal does not authorize any searches that cannot already be conducted under current law; it merely concerns venue, specifying which judge (or how many judges) may consider an application for a warrant in investigations of violations of 18 U.S.C. § 1030(a)(5) affecting five or more districts.

Google objects to the scope of botnet warrants, noting that they could authorize remote searches of millions of computers. But the large scope of botnet warrants is not a function of Rule 41, it is a function of the scope of botnet crime. Botnets may affect millions of people. And importantly, Google offers no solution for obtaining a warrant in such cases. It would be odd to adopt a “too big to investigate” rule in response to vast criminal activity.

NACDL and Michael Boucher correctly note that the computers searched pursuant to a botnet warrant may belong to innocent victims. Again, this fact is not unique to the botnet context, or even the digital evidence context. In *Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978), the Supreme Court held that search warrants may be directed to evidence in the possession of innocent parties, and investigations involving crimes ranging from burglary to murder frequently involve searches of a victim’s premises or property for evidence left behind by the perpetrator. We anticipate that the items to be searched or seized from victim computers pursuant to a botnet warrant will typically be quite limited in order to remain within the scope of current law concerning reasonableness. However, we believe that it may be reasonable in a given botnet investigation to obtain information from a large number of victim computers – for example, to measure the scope of the botnet. The purpose of our proposed rule is not to mandate such searches in every case or to alter any of the substantive rules governing when such searches are reasonable under the law, but to ensure that if such searches are appropriate they are not effectively precluded because of the practical difficulty of obtaining simultaneous judicial authorization from 94 different magistrate judges.

The proposed amendment does not conflict with the Privacy Protection Act.

Finally, the Reporters Committee for Freedom of the Press (“RCFP”) is concerned that the proposed amendment contravenes the protections of the Privacy Protection Act, 42 U.S.C. § 2000aa (“PPA”). These concerns are misplaced, as the PPA would apply to warrants issued under the proposed amendment in the same manner as it currently applies to other search warrants. The RCFP also objects that the proposed amendment does not substantively preclude “law enforcement impersonation of the news media in an effort to execute a remote access search.” But again, the proposal neither authorizes nor precludes the use of any particular undercover activities with respect to remote search, just as the current Rule 41 does not authorize or preclude the impersonation of journalists (or anyone else) when executing physical search

warrants. Those matters are appropriately addressed, if at all, through substantive law rather than venue provisions.

- - -

Few of the recently received comments raise any issue not already addressed by the Department and the Committee. Several of the arguments are premised on incorrect understandings of what the proposal would actually authorize or of current law. We continue to believe that the proposed amendment would provide needed clarity concerning venue and thus ensure the availability of prior judicial consideration of these important investigative techniques. Of course, Congress will have the final say on the proposal, but Congress's review only benefits from the Judicial Conference's thorough consideration. We appreciate the opportunity to respond to issues raised by commenters and look forward to further discussions with the Committee.

TAB 4A

MEMO TO: Members, Criminal Rules Advisory Committee

FROM: Professors Sara Sun Beale and Nancy King, Reporters

RE: Rule 45

DATE: February 24, 2015

At its April meeting the Criminal Rules Committee approved a proposed amendment to Rule 45 that would eliminate the additional 3 days provided for actions after electronic service. Parallels change in the Civil, Bankruptcy, and Appellate Rules were published at the same time.

The public comments were reviewed by the CM/ECF Subcommittee, chaired by Judge David Lawson. The members of the Subcommittee are Ms. Brook, Judge England, Professor Kerr, Jude Rice, Mr. Wroblewski representing the Department of Justice, and Mr. Hatten, our clerk of court representative. The Subcommittee met by teleconference to consider the comments. This memorandum discusses the comments and the Subcommittee's recommendations. The amendment with revisions recommended by the Subcommittee is Tab B, and the amendment as published is Tab C. The public comments are discussed below.

A. Background

As published, the proposed amendment to Rule 45 provides:

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).

The amendment and committee note as published are Tab C. The proposed changes reflect the view that electronic transmission and filing are now commonplace, and no longer warrant additional time for action after service. Advances in technology and widespread skill in using electronic transmission have alleviated earlier concerns about delays in transmission or incompatible systems that might make it difficult or impossible to open attachments.

Additionally, 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. The parentheticals were added to make it unnecessary for readers to reference the Civil Rule to understand when 3 additional days are still provided. Parentheticals are also being added to the committee notes accompanying the parallel amendments to the Civil, Bankruptcy, and Appellate Rules.

The Committee received four comments on the proposed amendment, two opposing the amendment and two supporting the amendment but suggesting revisions.

1. Comments opposing the amendment

Both the **Pennsylvania Bar Association, CR-2014-0004-0030**, and the **National Association of Criminal Defense Lawyers (NACDL), CR-2014-0004-0031**, oppose the amendment. The Pennsylvania Bar states that “the additional 3 days serves a useful purpose in alleviating the burdens that can arise if a filing is electronically served at extremely inconvenient times.” NACDL argues that eliminating 3 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.” It emphasizes that many criminal defense counsel are solo practitioners or in very small firms, where they have little clerical help. Given these practice patterns, the 3 added days are particularly valuable because many criminal defense lawyers do not see their ECF notices the day they are received.

The Civil Rules Committee received similar comments from practitioners (many in solo practice or small firms) who argued that the added 3 days are valuable and should not be eliminated. Some of the comments stressed the potential for gamesmanship (such as seeking to disadvantage opposing parties by filing late in the evening on Friday night), while others argued that filing deadlines are already difficult to meet and should not be shortened. In general, the other reporters were not persuaded by these arguments. Accordingly, they are recommending that their respective committees move forward with their proposed amendments.

The Civil, Bankruptcy, and Appellate Committees will not meet until after our March meeting. It seems likely, though not certain, that all of the committees will approve the parallel amendments eliminating the additional 3 days after electronic service for transmission to the Standing Committee.

Assuming that the other rules will be amended to eliminate the 3 extra days, the Subcommittee recommends that the Criminal Rules follow suit. There may occasionally be gamesmanship or hardship when electronic filing occurs late in the evening before a weekend or holiday. The Subcommittee concluded, however, that those problems can be dealt with by other means without losing the benefits of simplifying time counting by eliminating the 3 extra days after electronic filing. The Subcommittee recommends that the Committee Note to Rule 45(c) be

revised to include language drafted by the Department of Justice as an amendment to the Committee Note accompanying Civil Rule 6(d) (and other parallel rules). The Department’s proposed addition, described more fully in its Memorandum at Tab E, states:

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.

The Subcommittee agreed with the Department’s suggestion that the addition to the Committee note would be a helpful middle position, preserving the benefits of the proposed amendment but providing some useful guidance on how to handle problem cases.

2. Comments suggesting changes in the amendment as published

A. The parentheticals

The **Federal Magistrate Judges Association (FMJA), CR-2014-0004-0019**, “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 notes that after amendment Rule 45(c) would still provide for an added 3 days for other means consented to. Unless and until Civil Rule 5(b)(2)(E) is amended, it requires consent to service by electronic means.¹ Although the purpose of striking the cross reference to Civil Rule 5(b)(2)(E) from Rule 45(c) is clearly to eliminate the 3 added days for service by electronic means, the FMJA fears that readers of the amended rule might nonetheless think that 3 days are still added after electronic service because of the cross reference to Civil Rule 5(b)(2)(F) “(other means consented to).” The FMJA suggests 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 FMJA made parallel comments in response to the proposed civil rule eliminating the 3 extra days.

¹Civil Rule 5(b)(2)(E) and (F) provide that service of a paper may be made by:

(E) sending it by electronic means *if the person consented in writing*—in which event service is complete upon transmission, but is not effective if the serving party learns that it did not reach the person to be served...; or
(F) *delivering it by any other means that the person consented to in writing*—in which event service is complete when the person making service delivers it to the agency designated to make delivery.

(emphasis added).

All of the reporters and the liaison members of the Civil Rules Committee discussed the FMJA's concerns and concluded, for several reasons, that they recommended no change in the published rules. First, the likelihood of confusion did not seem to be great. Second, the problem (if there is one) is likely to be short lived because efforts are underway to eliminate the requirement for consent to electronic service. Third, the reporters and liaison members were reluctant to adopt either of the FMJA's proposed solutions. They believe the parentheticals will be very helpful to practitioners. In any event, deletion of the parentheticals would not solve the problem. A reader who pursued the cross referenced rules might still feel the same confusion. The reporters and liaison members also resisted the idea of revising the parenthetical reference to "(other means consented to except electronic service)," because it would require a further amendment of the parenthetical in the near future (assuming that the rules are amended to eliminate the requirement of consent to electronic service).

The Subcommittee agreed that the parentheticals have great value, and that the likelihood of confusion is not sufficient to warrant deleting them or revising the language as suggested by the FMJA. The Committee Note directly addresses this issue. It states:

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).

B. The caption

NACDL, CR-2014-0004-0031, questioned change in the caption to Rule 45(c), suggesting it may lead to confusion. The inclusion of the phrase "Time for Motion Papers" was intended to parallel the current caption of Civil Rule 6, on which Rule 45 was patterned, as well as the caption to Bankruptcy Rule 9006. Rule 12 (which was recently amended) deals extensively with the time for motions, and upon reflection the Subcommittee agreed that there might be some possible confusion. It recommends that the phrase "Time for Motion Papers" be deleted from the proposed amendment.

C. "Within a specified time after service"

In **CR-2014-0004-0023, Cheryl Siler, of Aderant**, suggests 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 reporters believe a member of the Standing Committee also questioned why the Criminal Rule was phrased differently than the Civil and Bankruptcy Rules at the June 2014 meeting when the Standing Committee approved all of the parallel

amendments for publication.

The Subcommittee recommends that the language of Rule 45(c) be modified to parallel the language of the other rules, referring to action “within a specified time *after being served*” on line 6 if that can be done without republication. The Subcommittee is unaware of any substantive reason for the slightly different wording of Rule 45 as compared to the Civil and Bankruptcy Rules. The discrepancy may have arisen when the various sets of rules were restyled at different times. Although we know of no problems that have arisen from the current phrasing of Rule 45(c), it seems desirable to revise the language of Rule 45(c) to eliminate this discrepancy while other changes are being made in Rule 45(c). We do not believe that republication would be required.

3. Summary of the Subcommittee’s recommendations

The Subcommittee recommends that the proposed amendment to Rule 45(c) be approved and forwarded to the Standing Committee with the following changes after publication:

- The addition of the following language at the end of the Committee Note:

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).

- Deletion of the phrase “Within a specified time after service” from the caption.
- Revision of line 6 to refer to action that must be taken “within a specified time after being served.”

TAB 4B

**PROPOSED AMENDMENTS TO THE
FEDERAL RULES OF CRIMINAL PROCEDURE***

1 **Rule 45. Computing and Extending Time; Time for**
2 **Motion Papers**

3 * * * * *

4 (c) **Additional Time After Certain Kinds of Service.**

5 Whenever a party must or may act within a specified
6 time after service and service is made under Federal
7 Rule of Civil Procedure 5(b)(2)(C) (mailing), (D)
8 (leaving with the clerk), ~~(E)~~, or (F) (other means
9 consented to), 3 days are added after the period would
10 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

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

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).

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.

TAB 4C

**PROPOSED AMENDMENTS TO THE
FEDERAL RULES OF CRIMINAL PROCEDURE***

1 **Rule 45. Computing and Extending Time; Time for**
2 **Motion Papers**

3 * * * * *

4 (c) **Additional Time After Certain Kinds of Service.**

5 Whenever a party must or may act within a specified
6 time after service and service is made under Federal
7 Rule of Civil Procedure 5(b)(2)(C) (mailing), (D)
8 (leaving with the clerk), ~~(E)~~, or (F) (other means
9 consented to), 3 days are added after the period would
10 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

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

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).

TAB 4D

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.

TAB 4E



U. S. Department of Justice

Civil Division

Office of the Assistant Attorney General

Washington, D.C. 20530

February 13, 2015

The Honorable David G. Campbell
Chair, Advisory Committee on Civil Rules
United States District Court
623 Sandra Day O'Connor
United States Courthouse
401 West Washington Street
Phoenix, Arizona 85003

Dear Judge Campbell:

This letter provides the comments of the Department of Justice on proposed amendments to the Federal Rules of Civil Procedure that were published for public comment in August 2014. The Department appreciates the opportunity to provide its perspective on these proposed changes. The Department is the largest and most frequent litigant in federal court. At various times, we are plaintiffs, defendants, litigants in complex cases, and parties in small matters. As a result, the Department has a special interest in the continued effective operation of the federal court system, and has a broad perspective and many interests to weigh in considering rule changes.

The Committee has proposed amendments to Rule 4(m), Rule 6(d), and Rule 82. The Department supports the Rule 4(m) and Rule 82 proposals, but has specific reservations about the impact of the proposed amendment to Rule 6(d) in actual practice, as I describe below.

Rule 4(m)

The Committee proposes a clarifying amendment to Rule 4(m) with respect to service in a foreign country on a corporation, partnership or other unincorporated association under Rule 4(h)(2). Under the proposed amendment, the time limits specified in Rule 4(m) to serve a complaint would not apply to service on such entities. The Committee has concluded that additional time may be necessary to effect service on such entities.

The Department supports this proposal.

Rule 6(d)

The Committee proposes to amend Rule 6(d) to eliminate the three additional days that are provided under the current Rule to respond to papers that have been served electronically, *e.g.*, through a court's CM/ECF system or by consent of the parties. The Committee has concluded that, because of advances in technology and greater facility by attorneys in electronic transmissions, the three additional days are no longer needed. The Committee also has reasoned that, because many rules have been amended to ease the computation of time by adopting periods of seven, fourteen, twenty-one, or twenty-eight days for filing responses to motions or other papers, maintaining the three additional days results in complicated time computation.

While the Department understands the Committee's rationales for the proposed amendment, the Department is concerned about the consequences of the amendment in actual practice. Unlike personal service, electronic distribution does not assure actual receipt by a party. The Department can foresee frequent situations in which the elimination of the three additional days will result in prejudice or disadvantage to a responding party.

The Department believes that the elimination of the three additional days could exacerbate the challenges faced by an attorney in such situations, particularly when applicable local rules require a response within fourteen or fewer days. Because electronic filings may be made after normal business hours, and courts generally allow filings up to midnight of the due date, a filing in a different time zone could be made as late as 3:00 a.m. (or later) the following day for lawyers on the East Coast of the United States. In addition, a filing could be made late in the evening on a Friday, or on a day before a holiday. Where that happens before a holiday weekend, the result (absent the three-day rule) could be a reduction, in practice, from the ten calendar days to respond to as little as five business days, which may not suffice to respond to substantive or complicated jurisdictional motions. In those situations, the attorney will need to respond to a filing in a more compressed time frame, having lost valuable time because of the manner and timing of service. It is foreseeable that some attorneys will try to take advantage of the elimination of the three additional days to serve papers at those time periods and thereby shorten the time within which the other party must respond.

If the Committee decides to proceed with the proposal, the Department recommends that the Committee incorporate language in the Note that acknowledges these problems. Specifically, the Department recommends the following language:

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,

sometimes on short notice. The courts should accommodate those situations and provide additional response time to discourage tactical advantage or prevent prejudice to the responding party.

The Committee Notes accompanying the proposed amendments to Appellate Rule 26(c), Bankruptcy Rule 9006(f), and Criminal Rule 45(c) should be consistent with the Committee Note for Civil Rule 6(d). For that reason, comparable language should be included in all four Committee Notes.

Rule 82

The Committee proposes a clarifying amendment to Rule 82, which states that the Civil Rules “do not extend or limit” district court jurisdiction or the venue of actions in those courts. The Committee explains that the Rule should be clarified to reflect the 2011 enactment of a new venue statute for civil actions in admiralty.

The Department supports the proposal.

* * *

We appreciate the Committee’s continued work and thank the Committee for its consideration of the Department’s comments.

Sincerely,

A handwritten signature in blue ink, appearing to read "Joyce R. Branda". The signature is stylized with a large loop at the beginning and a horizontal flourish at the end.

Joyce R. Branda
Acting Assistant Attorney General

TAB 5

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8dvr-4htf
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0003](#)

Comment from Keith Uhl, NA

Submitter Information

Name: Keith Uhl

Organization: NA

General Comment

Thankyou for the opportunity to comment. Regarding Rule 41 and venue for warrant approval, what considerations have been given to appropriate venue to challenge the validity of a search warrant? For example if a New York federal judge approves a multidistrict warrant that results in a search of computer and eventual indictment in Iowa, will the Iowa forum have jurisdiction to review sufficiency of New York decision or will the defense lawyer have to proceed with that issue in New York?.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8e0q-v3mv
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0004](#)

Comment from Mr. Anonymity, NA

Submitter Information

Name: Mr. Anonymity

Organization: NA

General Comment

Dear Undoubtedly Comment-Weary USC and Regulations[dot]gov Staff,

Just for the record, I'm commenting here on a Proposed Rule which the United States Courts is considering, to wit, a 'Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure.'

Specifically, my comments will be focused here on that thing which is referred to in your documents as:

"RecommendationThe Advisory Committee recommends that the proposed amendment to Rule 4 be published for public comment. (...) ACTION ITEMRule 41 (venue for approval of warrant for certain remote electronic searches)."

In commenting, I'm providing a few Remarks here, followed by a Conclusion and Suggested Course of Action:

I. Remarks

a) :-(

b) The reasoning for the proposed amendment (as described generally on pages 324-325 of the Preliminary Draft) states in part that "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 proxys IP address, not the originators true IP address. Accordingly, agents are unable to identify the physical location and judicial district of the originating computer." Let us suppose, for the sake of argument, that the perfect anonymity technology exists, in which case anyone could communicate or transact anonymously. Examining such an environment, some considerations are worthy to include in this section of my Remarks:

b.1) Anonymity is protected, within the United States (including anonymity online), by longstanding court precedent(s). I suggest you read the Electronic Frontier Foundation's fabulous document on the subject, titled "On Newspapers, Public Discourse, and the Right to Remain Anonymous." But you

probably won't bother, so I'll quote a little bit from it here:

In *Talley v. California*, Justice Black wrote Anonymous pamphlets, leaflets, brochures, and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. And in 1995, the Court upheld online speakers First Amendment right to remain anonymous, emphasizing, protections for anonymous speech are vital to democratic discourse. The court went on to say anonymous speech exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation at the hand of an intolerant society.

b.2) Under an environment in which individuals would have access to a hypothetical 'perfect anonymity technology,' most anyone could use it, and routine communications and financial transactions would be facilitated by such technologies, and,

b.3) The vast number of users (who, because this 'perfect anonymity technology' is hypothetical) would be ordinary users, doing ordinary things, going about their ordinary business, and perhaps never doing anything that would be of any interest to any serious person in any law enforcement agency, and

b.4) The super-hyper-encrypted communications and transactions which would result from use of this 'perfect anonymity technology' would very likely involve the use of ephemeral keys and zero-knowledge proofs, and a bunch of maths which would make even interceptions via malware result in the capture of largely useless information which would include certain types of information that would take many years to decrypt (if it could be done at all), and so basically such communications and transactions would be a bunch of gobblety-gook to everybody and anybody interested in intercepting them, unless a user were to divulge a communication or transaction willingly to someone else. Indeed, with a 'perfect anonymizing technology,' even installed malware would be ineffective at unmasking the information.

b.4) Many states have a Castle Doctrine, and people will respond if they detect that you are attacking their computers with malware. Remember Kennedy? "It shall be the policy of this nation to regard any nuclear missile launched from Cuba against any nation in the Western Hemisphere as an attack on the United States, requiring a full retaliatory response upon the Soviet Union." My, oh my. I do hope that that malware that the US government may have already installed surreptitiously on computers across the United States and the world isn't somehow discovered! When it comes to people who install malware, well, let's just say every action has (at least) an equal and opposite reaction.

II. Conclusion and Suggested Course of Action:

Just say no to malware!

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8ej5-ghqp
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0005](#)

Comment from Former Fed A , NA

Submitter Information

Name: Former Fed A

Organization: NA

General Comment

Dear Sirs:

As I have no doubt others will describe the technical means and argue the virtues of anonymity, I wish to provide two quick comments at a more rhetorical level.

First, as a former FBI agent working such matters, I can assure you the people doing that job mean no harm and are good people at heart. They are also driven to perform and find new and innovative ways to find evidence and prove their worth. It's just the culture of the FBI and other agencies when it comes to new technologies and the people that work with them. I was one of these people. I put away many child predators, cyber criminals and hackers who put people in danger. All were legitimate criminals who just happened to use a computer instead of a gun. Many of them tried to remain anonymous through technologies, but that is not what made them criminals. My fellow agents and I were always trying to find that nugget of information, or that simple slip, where they revealed their true identity. That said, future Agents will undoubtedly come up with ways to pierce the veil of anonymity and get that one piece of identifying information. To do so, they'll need a blessing from an AUSA and FBIHQ (specifically OGC). Typically, they will try to say that ANYONE visiting a site or acting in such a suspicious way (such as trying to remain anonymous) is predicated as a person of interest and their data should be subject to search. This blessing of "predication" clears the way for Agents to forge ahead and still be covered if there's blow-back later. This invariably leads to more Virtual Academy trainings, multiple emails from OGC and maybe even some press on how management is making sure the information obtained is only used "lawfully". I can absolutely assure you, that ANY information obtained will be used. If not for criminal proceedings, then for "Lead Purposes Only". Oddly enough, most people assume the NSA and other Intelligence agencies wield this power now and that may be true, but I also know first hand that they will not share it except under the most explicit circumstances and only in matters of national security, not criminal. The FBI will happily share this data with the Intelligence agencies, however, so I'm sure they would be thrilled to have Law Enforcement as cover when any captured data was subsequently released in criminal complaints. Allowing Law Enforcement the ability to distribute malware, pierce anonymity and or circumvent encryption technologies sounds like a valiant effort to catch criminals, but that's assuming the persons acting that way ARE, in fact, criminals. I submit law abiding, peaceful citizens perform these same actions as part of being regular citizens on the Internet. Agencies should target individuals, not practices.

Secondly, do I not still have the right to wear a Groucho Marx moustache and glasses as I walk down a public street? Does a Muslim have the right to wear a veil? These things, done in public, may hide my identity. If I pass by a business known to be frequented by bad people am I now a predicated target because of my dress and proximity? The Internet is a very busy highway with a world of peoples passing by. In Topeka, Kansas my disguise might raise an eyebrow or two, but would anyone even notice me in San Francisco? I urge you to dismiss this proposal. For the same reasons the Supreme Court disallowed using technologies to look inside your home from outside, allowing technologies to look through your firewalls is just as intrusive and paves the way to negating the 4th amendment.

Thank you.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8f5w-8fzw
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0006](#)

Comment from Robert Anello, Federal Bar Council

Submitter Information

Name: Robert Anello

Organization: Federal Bar Council

General Comment

See attached file(s)

Attachments

FBC Letter on Rule 4 and Rule 41 Amendments



Serving the courts and legal community
of the Second Circuit since 1932

Federal Bar Council

ROBERT J. ANELLO
President, Federal Bar Council

DAVID B. ANDERS
Chair, Federal Criminal Practice Committee

October 27, 2014

Committee on Rules of Practice and Procedure
Administrative Office of the United States Courts
Thurgood Marshall Federal Judiciary Building
One Columbus Circle, N.E., Suite 7-240
Washington, D.C. 20544

Re: Proposed Amendments To Fed. R. Crim. P. 4 and 41

Dear Sir or Madam:

The Federal Bar Council and its various committees regularly comment on proposed changes to the various rules that affect the practices of our members in the federal courts of the Second Circuit. By letter dated August 27, 2014, the Judicial Conference of the United States Advisory Committee on Criminal Rules solicited the views of the Council and its Federal Criminal Practice Committee regarding proposed amendments to Fed. R. Crim. P. 4 and 41. The Chair of the Federal Criminal Practice Committee, David B. Anders, formed two separate subcommittees to review and report on the proposed amendments. As set forth below, upon the recommendation of the Federal Criminal Practice Committee, the Federal Bar Council supports the proposed amendments to both Rules and recommends that the Advisory Committee submit all of the proposed amendments to the Committee on Rules of Practice and Procedure.

Rule 4

Background.

Rule 4 deals generally with the issuance of an arrest warrant or summons, the form of the warrant or summons, the required manner of service and the relief available if an individual fails to appear in response to a summons. Regarding corporations, Rule 4(c)(3)(C) states that:

A summons is served on an organization by delivering a copy to an officer, managing or general agent, or to another agent appointed or legally authorized to receive service of process. A copy must also be mailed to the organization's last known address within the district or to its principal place of business elsewhere in the United States.

By letter dated October 25, 2012, the Department of Justice wrote to the Advisory Committee recommending that Rule 4 be amended because the DOJ believed that the Rule posed an obstacle to the prosecution of foreign corporations that may have committed offenses in the United States, but cannot be served because they have no last known address or principal place of business here. Accordingly, the DOJ recommended that Rule 4 be amended a) to remove the requirement that a copy of the summons be sent to the organization's last known mailing address within the district or to its principal place of business within the United States; and b) to designate the means to serve a summons upon an organization located outside the United States. The Advisory Committee then took up consideration of the DOJ's proposal through the formation of a Rule 4 Subcommittee.

The Advisory Committee's Proposed Amendments.

The proposed amendments are as follows:

A. Limiting The Mailing Requirement When Delivery Is Made In The United States

In its present form, Rule 4 requires that in every case involving an organizational defendant, service must be made in two ways: on an agent of the organization and by mailing a copy of the summons to the entity at its last known address within the district or its principal place of business elsewhere in the United States. As a result, even if the government is able to serve an agent, service cannot be completed if the corporate defendant does not have either an address within the district or principal place of business outside the district but within the United States. The Advisory Committee's proposed amendment states as follows:

"A summons is served on an organization in a judicial district of the United States¹ 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 ~~of~~ If the agent is one authorized by

¹ The Advisory Committee's proposed amendments also make explicit in Rule 4(c)(2) that a court may issue a warrant to an organizational defendant located outside of the United States. If the Advisory Committee's proposed changes are approved, that provision would state:

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.

~~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."~~

The proposed amendment limits the mailing requirement to cases in which service has been made on a statutorily appointed agent when the statute itself requires mailing as well as personal service. The proposed amendment does not specify the location to which the summons should be mailed, expressly deleting the requirement that it be mailed to the organization at its last known address within the district or to its principal place of business elsewhere in the United States.

B. Providing For Service Outside the United States

The next portion of the proposed amendment authorizes service on a foreign organization by any "means that gives notice" and it lists three permissible methods of service that presumptively do so.² It reads as follows:

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.

C. Sanctions For An Organizational Defendant's Failure To Appear

The final proposed amendment addresses the potential consequences for an organization that fails to appear in response to a summons. Indeed, although Rule 4 currently provides that both individual and corporate defendants may be served with a summons, and that an arrest warrant may be issued if an individual defendant fails to appear in response to a summons, the rule is silent on the procedure to be followed if

² The Advisory Committee has made clear in the comments to the proposed rule that the list of permissible means in Rule 4 is non-exhaustive.

an organizational defendant fails to appear. Accordingly, the Advisory Committee proposes that the following sentence be added to the end of paragraph (a):

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

Given the many incentives that foreign and domestic corporations have to appear and resolve criminal charges once service is made, cases in which an organizational defendant has defaulted appear to be rare. Thus, rather than try to specify the particular sanctions that could be imposed on the non-appearing defendant, the Advisory Committee's language provides a framework for the courts to evaluate the range of actions authorized by law if and when cases arise in which a corporate defendant – foreign or domestic – fails to appear after being served with a summons.³

The View of The Federal Bar Council.

In the view of the Federal Bar Council, the proposed amendments fairly address the gaps in the current version of the Rule that can prevent the government from being able to effectively prosecute foreign organizations that commit crimes in the United States but have no physical presence here.

First, with one notable exception, the amendments eliminate the requirement that, in addition to actual delivery of the summons to an agent of the organization, a summons be mailed to the organization's last known address or principal place of business in the United States. The exception requires the government to continue to mail a copy of a summons to an organization where there is a statutory requirement to do so. The Council agrees that, in light of the actual delivery required by the Rule, the mailing requirement in Rule 4 is largely redundant and unnecessary. It moreover prevents service on foreign organizations without a physical presence in the United States.

Second, the various methods of service for foreign organizations described in the amendments appear reasonably calculated to provide effective notice while ensuring

³ In its submission to the Advisory Committee, DOJ identified the following steps that a court might take if a corporate defendant fails to appear in response to a summons: a contempt order subjecting the defendant to fines, forfeitures or other penalties; injunctive relief (such as an order preventing further disclosure of a trade secret); appointment of counsel who would appear for the organization; and the imposition of penalties in a parallel civil action. Other, extra-judicial actions that might be taken include suspension or debarment from eligibility for government contracts and possible imposition of economic and trade sanctions.

that service complies with United States constitutional requirements, the law of the foreign jurisdiction and any applicable international agreements.

Third, the amendments give the courts discretion to fashion remedies for a corporation's failure to appear after service, but only to the extent "authorized by United States law." As noted in the DOJ's letter to the Advisory Committee, cases in which an organizational defendant has defaulted appear to be rare. However, to the same extent there are good reasons to permit a court to impose consequences on a defendant that fails to appear for a criminal summons, those reasons seem to apply to individual defendants and organizational defendants alike.

For those reasons, and for the reasons provided by the Advisory Committee, we recommend that the Advisory Committee submit the proposed amendments to Rule 4 to the Committee on Rules of Practice and Procedure.

Rule 41

Background.

Rule 41, titled "Search and Seizure," deals with the circumstances under which a court has authority to issue a warrant to search and seize a person or property. With few exceptions, the court's authority is limited to issuing warrants for search and seizure of person or property located within the district.⁴

According to the report of the Advisory Committee, the proposed amendment to Rule 41 originated with a letter from the Acting Assistant Attorney General, Mythili Raman, who raised concerns about the Rule's territorial venue restrictions in the context of efforts to search and seize electronic information. In particular, Raman noted the Rule may prevent or hamper the government's investigation when: (1) the location of electronic information sought is unknown, or (2) the electronic information sought spans multiple districts requiring law enforcement to coordinate efforts with local law enforcement, prosecutors, and courts in multiple jurisdictions. As stated in Raman's

⁴ Currently, Rule 41 authorizes courts to issue warrants related to persons or property outside the district in cases involving: (1) property that is within the district when the warrant is issued, but that may 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. Fed. R. Crim. P. 41(b)(2)-(5).

letter, at least one court has declined to issue a warrant under such circumstances precisely because of the Rule's express territorial limits.⁵

The Advisory Committee's Proposed Amendments.

The Advisory Committee's proposed amended version of Rule 41 is annexed hereto as Exhibit B. There are two parts to the proposed amendment. The first is the addition of Rule 41(b)(6), which, in two specific circumstances, authorizes a court in a district where the activities related to a crime may have occurred to issue a warrant to use remote access⁶ to search electronic storage media and to seize or copy that information even if it is or may be located outside of the district. The first circumstance is where the district where the media or information is located has been concealed through technological means. The second circumstance is an investigation of a violation of 18 U.S.C. § 1030(a)(5) (covering certain fraudulent activities in connection with computers), where the media are protected computers that have been damaged without authorization and are located in five or more districts. The second part of the proposal is a change to Rule 41(f)(1)(C), which regulates notice to be given that a search has been conducted. The proposal adds new language indicating the process for providing notice of a remote access search.

As outlined above, while traditional law enforcement efforts may be carried out within Rule 41's existing framework, the Rule's territorial limits present unique problems for investigations requiring access to electronic information or electronic storage devices. The current territorial venue limitations pose a problem for the government where (1) the alleged perpetrators mask the location of the computer or storage device to be searched and seized through the use of sophisticated anonymizing software, thereby preventing law enforcement from identifying the district in which the information or the device is located in an otherwise sufficiently detailed warrant; and (2) the investigation of a complex criminal scheme involves the use of multiple computers in multiple districts simultaneously, requiring the government to expend extraordinary

⁵ See *In re Warrant to Search a Target Computer at Premises Unknown*, 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013) (noting that "there may well be a good reason to update the territorial limits of [Rule 41] in light of advancing computer search technology").

⁶ A warrant for a remote access search would authorize investigators to send an email to the target of the warrant, remotely install software on the device receiving the email, and determine the true IP address or identifying information for that device. The ACLU has submitted comments to the Advisory Committee objecting to this type of remote access. See https://www.aclu.org/sites/default/files/assets/aclu_comments_on_rule_41.pdf at pp.9-15. The Federal Criminal Practice Committee has reviewed the ACLU's objections and concludes the use of remote access techniques is appropriate in the narrow circumstances outlined in the Rule.

resources and efforts to coordinate obtaining individual warrants from the various districts involved.

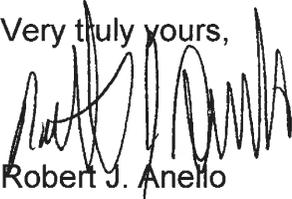
Both of these problems have become increasingly common as crimes involving the use of computers have increased in frequency and complexity. The Advisory Committee took action to propose the narrowly tailored amendments at issue, reasoning that the use of anonymizing software to mask a computer's location, or the use of malicious software to infect a large number of computers scattered in multiple districts should not prevent law enforcement from efficiently investigating serious federal crimes in the face of increasingly more sophisticated criminal activities.

The View of The Federal Bar Council.

On balance, we believe that these amendments to Rule 41 are necessary and will be effective in permitting law enforcement to properly investigate crimes involving computers and electronic information. Although we note that the proposed amendments leave unanswered a number of Constitutional questions, such as the level of specificity required in a warrant seeking authorization to conduct a remote access search or seizure, these questions can and will be addressed by the courts in due course. The Advisory Committee explicitly addresses this point in the Comments to the proposed Rule, which state that “[t]he amendment . . . leav[es] the application of this and other constitutional standards to ongoing case law development.”

* * *

In conclusion, the Federal Bar Council supports the proposed amendments to Fed. R. Crim. P. 4 and 41, and believes that they effectively and fairly address the issues presented by the current versions of the Rules as discussed above. We recommend that the Advisory Committee solicit the support approval of the proposed amendments from the Committee on Rules of Practice and Procedure.

Very truly yours,

Robert J. Anello

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8f78-zdhe
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0007](#)

Comment from Carolyn Atwell-Davis, NA

Submitter Information

Name: Carolyn Atwell-Davis

Organization: NA

General Comment

See attached file(s)

Attachments

Ltr 10_14 Judicial Conference Advisory Committee on Criminal Rules

Judicial Conference Advisory Committee on Criminal Rules
Administrative Office of the U.S. Courts
One Columbus Circle, N.E.
Washington, D.C. 20544

October 28, 2014

To the Members of the Advisory Committee on Criminal Rules:

I am writing to support the Proposed Amendment to the Federal Rules of Criminal Procedure authorizing warrants to permit law enforcement to use remote access to search electronic storage media and to seize or copy electronically stored information even when the media or information is located outside of the district where the warrant is issued.

Until recently, I worked for 13 years at the National Center for Missing & Exploited Children ("NCMEC"). NCMEC is authorized by Congress to serve as the U.S. clearinghouse on missing and exploited children issues, and to operate the CyberTipline, the mechanism for reports of suspected child sexual exploitation. *42 U.S.C. §5773(b)(1)(P)*.

The CyberTipline is operated in partnership with the FBI, Immigration and Customs Enforcement, U.S. Postal Inspection Service, U.S. Secret Service, military criminal investigative organizations, U.S. Department of Justice, Internet Crimes Against Children Task Force program, as well as other state and local law enforcement agencies. www.missingkids.com. When the CyberTipline receives a report, its analysts determine the geographic location related to the report, and refers reports to the law enforcement agency with jurisdiction to investigate. Electronic Communication Service Providers ("ESP") are required by federal statute to report apparent child pornography to the CyberTipline. *18 U.S.C. §2258A*.

As the Vice President for Policy and Governmental Affairs, I had day-to-day involvement in the CyberTipline process and, over the years, witnessed the explosion of reports received, from 5,000 reports in 1998 to more than 500,000 reports in 2013 alone. This increase is caused by several factors: better training of law enforcement; heightened awareness and reporting by the Internet industry; more effective laws at the state and federal levels; and, indisputably, by the increased demand for images of child sexual exploitation.

The demand for images is at the heart of the child pornography industry. This is not merely an issue of possession and distribution of digital child pornography images. This is about the sexual abuse of children, which occurs as a direct result of the demand for images. Not only are these children victimized during the production of images, they are also victimized by the repeated sharing and downloading of images depicting their abuse for others' gratification. Further, the successful investigation of child pornography possession and distribution cases have led to the rescue of numerous child victims from their abusive situations.

As a result of technology – digital images, ease of Internet access and high volume electronic storage – the child pornography industry is thriving, growing, and global in scope. Technology, such as anonymizers and encryption software, has become more commonly used by those who know that law enforcement is aggressively investigating these cases. Because the Internet knows no borders, child pornography investigations often begin in one state and lead to one or more other states. Law enforcement and prosecutors must be able to successfully investigate and prosecute individuals who so heinously victimize children and utilize technology to evade detection.

The proposed amendments will greatly assist law enforcement while adhering to the Fourth Amendment. By authorizing a warrant issued by a magistrate judge, they follow strongly established legal precedent requiring a neutral, detached authority and an officer's affirmation that probable cause exists to believe that a criminal offense has taken, or is about to take, place.

In addition, these warrants would only be issued in narrowly-defined circumstances. These circumstances are not speculative – they are well-known by law enforcement. The computer forensic experts at the Justice Department's Child Exploitation and Obscenity Section can provide numerous examples of investigations that were stalled by the use of anonymizers and encryption software.

It is true that under certain prescribed, and legal, circumstances courts have held that individuals have a right to remain anonymous. However, there is a vast difference between the right to engage in legal activities with anonymity and the right to commit crimes against children with anonymity and, by extension, impunity.

The U.S. is a global leader in child protection. These proposed amendments to the criminal rules are a necessary tool for law enforcement and prosecutors in their efforts to help stop the sexual exploitation of children. I urge you to enact them.

Sincerely,

Carolyn Atwell-Davis

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8f7q-mnwn
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0008](#)

Testimony of Amie Stepanovich, on behalf of Access and the Electronic Frontier Foundation

Submitter Information

Name: Amie Stepanovich

Organization: Access and the Electronic Frontier Foundation

General Comment

See attached

Attachments

Testimony for Nov. 5 Hearing

Testimony of Amie Stepanovich
Senior Policy Counsel, Access
on behalf of
Access and the Electronic Frontier Foundation
Before the Advisory Committee on Criminal Rules
on the Matter of Proposed Amendments to Federal Rules of Criminal Procedure, Rule 41

I would like to thank the members of the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States for allowing me to testify in front of you today. My name is Amie Stepanovich and I am Senior Policy Counsel with Access, an international digital rights non-governmental organization.¹ Founded in the wake of the 2009 Iranian post-election crackdown, Access seeks to defend and extend the digital rights of users around the world.² Today I am also testifying on behalf of the Electronic Frontier Foundation.³ The Electronic Frontier Foundation, or EFF, was founded in 1990 and champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development.⁴

Introduction

My testimony today will focus on the second proposed change to Federal Rule of Criminal Procedure 41.⁵ Specifically, the proposed change I would like to discuss grants magistrate judges authority to issue warrants within an investigation under the Computer Fraud

¹ Access, <https://www.accessnow.org> (last visited Oct. 29, 2014).

² *About Us*, Access, <https://www.accessnow.org/about> (last visited Oct. 29, 2014). I would like to thank Access Junior Policy Counsel Drew Mitnick, Access Policy Intern Jack Bussell, and Access Tech Policy and Programs Manager Michael Carbone for their contributions to this testimony.

³ Electronic Frontier Foundation, <https://www.eff.org> (last visited Oct. 29, 2014).

⁴ *About EFF*, Electronic Frontier Foundation, <https://www.eff.org/about> (last visited Oct. 29, 2014). EFF Staff Attorney Hanni Fakhoury, Senior Staff Technologist Seth Schoen, Senior Staff Attorney Jennifer Lynch, and Senior Staff Attorney Lee Tien contributed to this testimony.

⁵ Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil and Criminal Procedure, 338-42 (August 2014), *available at* <http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf>.

and Abuse Act to remotely search protected computers that have been damaged without authorization and to seize or copy electronically stored information on those computers when the computers are located in five or more districts and are not otherwise within that magistrate's jurisdiction.⁶ As discussed in the relevant Committee Note, this change specifically involves the creation and control of "botnets."⁷ Today, I will provide to the committee some technical background on botnets, the unique natures of botnets that would cause the rule change to have an overbroad, substantive impact on computing, and how the Department of Justice's interpretation of the Computer Fraud and Abuse Act,⁸ or CFAA, could compound these impacts. I will end discussing how the proposed change could cause more harm than good in practice. Instead, we propose that a statutory solution is pursued to address the special challenges of unlawful botnets.

What are botnets?

The term "botnet" is short for "robot network." A botnet is a network of computers that have been linked together.⁹ Botnets can consist of anywhere from a few computers to several million, as was the case with the Mariposa botnet, which was shut down in 2009,¹⁰ as well as the most infamous botnet, the Conficker, first discovered in 2008.¹¹ Unlawful botnets are created when computers are infected with malicious code, known as malware.¹² The type of malware that creates a botnet allows the infected computer to be remotely access and controlled by a

⁶ *Id.*

⁷ *Id.*

⁸ Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2014).

⁹ *Build you own botnet with open source software*, WIRED, http://howto.wired.com/wiki/Build_your_own_botnet_with_open_source_software#Business_Usages (last visited Oct. 29, 2014).

¹⁰ John Leyden, *How FBI, police busted massive botnet*, The Register (Mar. 3, 2010), *available at* http://www.theregister.co.uk/2010/03/03/mariposa_botnet_bust_analysis/.

¹¹ *The 'Worm' That Could Bring Down The Internet*, NPR (Sept. 27, 2011 12:12 PM ET), <http://www.npr.org/2011/09/27/140704494/the-worm-that-could-bring-down-the-internet>.

¹² *Malware*, Norton by Symantec, http://us.norton.com/security_response/malware.jsp (last visited Oct. 29, 2014).

third party, often without the owner's knowledge.¹³ The infected computers in a botnet are sometimes known as "zombies."¹⁴

Botnet malware may sit stagnant on an infected computer for months or years without causing any additional harm to the computer itself or any other system, and without coming to the attention of the computer's owner or operator. Some botnets may never actually be utilized and may be patched without incident. In the case of Conficker, the botnet went largely unused despite its massive size, resiliency, and duration.¹⁵

Not all networked computers are intended for malicious or unlawful purposes. Lawful systems that closely resemble botnets in structure also exist and are used for communication and coordination.¹⁶ In business contexts, these systems may be used to create a cloud computing system, to capitalize on spare computing resources, to balance application loads, and for testing purposes.¹⁷ They may also be created and used to harness processing power in order to conduct scientific experiments or monitor emerging weather patterns.¹⁸

Substantive impacts of the proposed Rule 41 amendment

On account of their distributed nature, investigations of unlawful botnets undoubtedly pose a significant barrier to law enforcement. Access and EFF empathize with these challenges and are willing to work with members of Congress and leaders in law enforcement to develop an

¹³ *Bots and Botnets--A Growing Threat*, Norton by Symantec, <http://us.norton.com/botnet/> (last visited Oct. 29, 2014).

¹⁴ *Id.*

¹⁵ One version of the botnet was eventually utilized to download and install additional malware. *Conflicker*, Wikipedia.org, https://en.wikipedia.org/wiki/Conflicker#End_action (last visited Oct. 29, 2014).

¹⁶ *About Eggdrop*, Eggsheads Development Team (Oct. 2, 2011), <http://cvs.eggheads.org/viewvc/eggdrop1.6/doc/ABOUT?view=markup>. Additionally, other lawful computer networks are encompassed under the terms of the proposed rule, namely systems of protected computers located in five or more districts. Examples are CDNs, P2P systems, and websites run on shared resources.

¹⁷ *Build your own botnet with open source software*, WIRED, http://howto.wired.com/wiki/Build_your_own_botnet_with_open_source_software#Business_Usages (last visited Oct. 29, 2014).

¹⁸ *ATLAS@Home*, CERN, <http://atlasathome.cern.ch/> (last visited Oct. 29, 2014); Katherine Smyrk & Liz Minchin, *How your computer could reveal what's driving record rain and heat in Australia and NZ*, The Conversation (March 25, 2014, 11:24 EDT), <http://theconversation.com/how-your-computer-could-reveal-whats-driving-record-rain-and-heat-in-australia-and-nz-24804>.

appropriate and rights-respectful response. However, due to the same considerations, the proposed rule change presented today as a procedural modification would have a significant substantive impact, including on rights otherwise guaranteed under the Fourth Amendment and international law. Accordingly, we urge the rejection of the proposed amendment to Rule 41 in favor of pursuit of a statutory solution promulgated democratically in an open, public, and accountable legislative process.

The CFAA, initially passed in 1986, has traditionally been used to prosecute the theft of private data or damage to systems by way of malicious hacking.¹⁹ The CFAA was designed to provide justice for victims of these activities by offering a remedy against the perpetrators - the plain text of the relevant section of the CFAA clearly focuses on knowing or intentional malicious activity.²⁰ Using this authority, magistrate judges issue warrants against those who create and use unlawful botnets, controlling the infected computers of otherwise innocent users.²¹ However, the proposed amendment unilaterally expands these investigations to further encompass the devices of the victims themselves - those who have already suffered injury and are most at risk by the further utilization of the botnet.²² And, as noted, a single botnet can include millions (or tens of millions) of victim's computers, which may be located not only across the United States, but anywhere around the world.²³

Victims of botnets include journalists, dissidents, whistleblowers, members of the military, lawmakers and world leaders, or protected classes. Each of these users, and any other user subject to search or seizure under the proposed amendment, has inherent rights and

¹⁹ See, e.g., *United States v. Norris*, 928 F.2d 504, (2nd Cir. 1991); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012).

²⁰ See 18 U.S.C. § 1030(a)(5) for “knowingly” and “intentionally” language.

²¹ See *Microsoft Corp. v. Does 1-18*, No. 1:13cv139 (LMB/TCB), 2014 WL 1338677, (E.D. Va. April 2, 2014).

²² *Supra* note 5. The proposed amendment would permit law enforcement to “. . . use remote access to search electronic storage media [when] the media are protected computers . . .”

²³ Notably, the provision in the CFAA relevant to the rule change addresses harm to a single computer - each provision in 18 U.S.C. § 1030(a)(5) addresses access to a “protected computer” - that is, one single computer, or, perhaps in some circumstances, a small network of computers operated by a single entity. A “protected computer” has been, at its most expansive, a corporate or government computer network.

protections under the U.S. Constitution, the International Covenant on Civil and Political Rights, and/or other well-accepted international law.²⁴ Without reference to or regard for these rights and protections, the proposed change would subject any number of these users to state access to their personal data on the ruling of any district magistrate. This is a substantive expansion of the CFAA. Today we are in the midst of a national, not to mention global, conversation about the appropriate scope of government surveillance. The U.S. Congress is actively considering a number of proposals to reform both international and domestic surveillance activities.²⁵ The proposed amendment is an end run around this process.

Further complicating matters, the proposed change being considered here today will likely have ramifications for a large number of users who are not even a part of a botnet. These users may be tangentially connected to a botnet through any number of means, such as the use of a common shared server or service provider. For example, earlier this year Microsoft applied to a federal judge for a court order to assist in dismantling a pair of botnets that encompassed a total of about 18,000 computers.²⁶ The resulting action led to the disruption of service for nearly 5,000,000 legitimate websites or devices on which 1,800,000 additional non-targeted users

²⁴ See, e.g., *Scope: Extra-territorial Application of Human Rights Treaties*, Necessary and Proportionate, <https://en.necessaryandproportionate.org/LegalAnalysis/scope-extra-territorial-application-human-rights-treaties> (last visited Oct. 29, 2014).

²⁵ See, e.g., Kurt Opsahl & Rainey Reitman, *A Floor, Not a Ceiling: Supporting the USA FREEDOM Act as a Step Towards Less Surveillance*, Electronic Frontier Foundation (Nov. 14, 2013), <https://www.eff.org/deeplinks/2013/11/floor-not-ceiling-supporting-usa-freedom-act-step-towards-less-surveillance>; *The USA FREEDOM Act's Long Road*, Access, <https://www.accessnow.org/pages/usa-freedom-act> (last visited Oct. 29, 2014); Amie Stepanovich, *Virtual Integrity: Three steps toward building stronger cryptographic standards* (Sept. 18, 2014 4:43am), <https://www.accessnow.org/blog/2014/09/18/virtual-integrity-the-importance-of-building-strong-cryptographic-standards> ("U.S. Representative Alan Grayson and other lawmakers have introduced legislation to remove the mandatory requirement for NIST to consult with NSA (though still permit the consultation) and strictly prohibit the NSA from artificially weakening standards.").

²⁶ The court order applied to 18,000 subdomains. Many of these were likely individual personal computers, though it is possible that a small percentage were actually not individual computers. *Microsoft Corp. v. Mutairi et al.*, No. 14-cv-0987, (D. Nev. June 19, 2014) (Brief in support of App. for TRO), *available at* <http://www.noticeoflawsuit.com/docs/Brief%20in%20Support%20of%20Ex%20Parte%20Application%20of%20a%20TRO.pdf#page=9>. For clarity, we will refer to each subdomain as an individual computer.

were engaging in legitimate, constitutionally protected speech.²⁷ These other users had no connection to the botnets nor were they known to have broken any law, and instead were only guilty of using the same service as the botnet operators, a fact that caused a public outcry among the public and civil society.²⁸

While the Microsoft case was a civil action, and not pursued in a criminal context, it is a good example of the unsettled legal nature of these issues and the difficulty in crafting narrowly-tailored and appropriate remedies. This potential for far-flung damage requires a careful balancing of rights and responsibilities that is best accomplished through the public legislative process.

Overbroad application of the CFAA

The above problems are exacerbated by overbroad interpretations of the CFAA itself. Federal prosecutors have forcibly expanded the scope of the CFAA through the overuse of the “without authorization” prong to encompass a range of unanticipated, and patently inappropriate, activities: users have been charged with violating the CFAA for violating online terms of service, researching website vulnerabilities, and lying on social media profiles.²⁹

Aaron's Law - so named for technologist Aaron Swartz who was aggressively prosecuted under the CFAA eventually leading to his suicide - has been introduced in the House of Representatives by Representative Zoe Lofgren with six co-sponsors to restrict these overuses.³⁰ However, until either Congress or the U.S. Supreme Court are able to permanently

²⁷ Natalie Goguen, *Update: Detail on Microsoft Takeover*, noip.com (July 10, 2014), http://www.noip.com/blog/2014/07/10/microsoft-takedown-details-updates/?utm_source=email&utm_medium=notice&utm_campaign=microsoft-takedown-update.

²⁸ *Id.*; Nate Cardozo, *What Were They Thinking? Microsoft Seizes, Returns Majority of No-IP.com's Business*, Electronic Frontier Foundation (July 10, 2014), <https://www.eff.org/deeplinks/2014/07/microsoft-and-noip-what-were-they-thinking>; Brandon Moss, *So many botnets, so little time: U.S. Senate holds a hearing to combat “thing-bots,”* Access (July 18, 2014 4:03pm), <https://www.accessnow.org/blog/2014/07/18/the-senate-holds-a-hearing-to-combat-thing-bots>.

²⁹ See, e.g., *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012); *United States v. Drew*, 259 F.R.D. 449 (C.D. Ca. 2009); see also Declan McCullagh, *From ‘WarGames’ to Aaron Swartz: How U.S. anti-hacking law went astray*, C|NET (March 13, 2013 4:00 AM PDT), [Dhttp://www.cnet.com/news/from-wargames-to-aaron-swartz-how-u-s-anti-hacking-law-went-astray/](http://www.cnet.com/news/from-wargames-to-aaron-swartz-how-u-s-anti-hacking-law-went-astray/).

³⁰ Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (2013).

rectify these mis-applications of the CFAA, there is a danger that the proposed amendment could be used in a shocking number of unintended instances. This is particularly concerning because, as explained above, there are several properly-established and otherwise lawful computer networks that the proposed rule would likely encompass. Increasing the potential impact of the proposed amendment, any small networked group of computers may be subject to invasive surveillance at the whim of an overzealous prosecutor and a compliant judge. Further, as also explained above, since the proposed amendment targets victim computers and not the devices of bad actors, it would be enough for a computer connected to a lawful network to carry a virus or to have violated a standard shrinkwrap agreement to justify this surveillance, a move that carries heavy implications for constitutional rights and rights under international law.

The proposed amendment in practice

I have described how the proposal could bring an enormous number of computers belonging to innocent users into the purview of the CFAA and subject them to law enforcement surveillance. In applying the proposed amendment, it is likely that law enforcement could cause more harm to these users than the botnet it has seeks to investigate. Specifically, the use of the word “seizure” in the proposal, an undefined term, could authorize any amount of invasive activity. For example, as in the Microsoft case described above, law enforcement could intercept and re-route legitimate internet traffic. Further, the ambiguity in the language could potentially be interpreted to encompass a level of government hacking into private networks. Even groups that are supportive of this type of government activity concede that it necessarily requires statutory authorization.³¹

The range of offensive cybersecurity measures available to law enforcement vary from passive measures like beaconing - causing files to broadcast back to a preordained location - to

³¹ The IP Commission Report, 82, (May 2013), *available at* http://ipcommission.org/report/IP_Commission_Report_052213.pdf “Statutes should be formulated that protect companies seeking to deter entry into their networks and prevent exploitation of their own network information while properly empowered law-enforcement authorities are mobilized in a timely way against attackers.”

active and potentially harmful measures that interfere with the operation of the computer or its communications with other devices. The proper limits for use of offensive measures should be subject to public debate. While limits have been raised through various statutory vehicles in recent years, none have gained significant public support, and one has received not one, but two veto threats from the White House.³² It is not the place to pre-empt these continued conversations through implementation of a procedural measure.

Conclusion

The proposed amendment before the Committee today is a substantive change to federal law masquerading as a procedural measure. Once again, I urge you to reject the proposal and to, instead, support the exploration of appropriate statutory solutions for any legal gaps in the investigation, pursuit, and prosecution of those responsible for unlawful botnets. Thank you. I look forward to your questions.

³² See, e.g., Hayley Tsukayama, *CISPA critics bolstered by veto threat*, Washington Post (April 17, 2013), available at http://www.washingtonpost.com/business/technology/cispa-critics-bolstered-by-veto-threat/2013/04/17/2c2f761e-a76b-11e2-8302-3c7e0ea97057_story.html. See also Brandon Moss, *Access calls for President Obama to pledge to veto CISA*, Access (July 15, 2014 9:30 am), <https://www.accessnow.org/blog/2014/07/15/access-calls-for-president-obama-to-pledge-to-veto-cisa>; and Letter from Access and Civil Liberties Groups to President Obama (July 15, 2014), available at <https://www.accessnow.org/page/-/Veto-CISA-Coalition-Ltr.pdf>.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8f7q-9jqo
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0009](#)

Testimony of Joseph Lorenzo Hall, on behalf of The Center for Democracy & Technology

Submitter Information

Name: Joseph Lorenzo Hall

Organization: The Center for Democracy & Technology

General Comment

See attached

Attachments

Testimony for Nov. 5 Hearing

Written Statement
Of
The Center for Democracy & Technology
Before
The Judicial Conference
Advisory Committee on Criminal Rules
Friday, October 24, 2014

Members of the Committee, thank you for allowing the Center for Democracy & Technology (CDT) to testify on proposed changes to Rule 41 of the Federal Rules of Criminal Procedure (FRCrmP).¹ CDT is a nonprofit public interest organization dedicated to promoting policies and technical standards that protect civil liberties such as privacy and free expression globally.

CDT recognizes that law enforcement faces legitimate challenges in determining how to issue search warrants for computers with concealed locations in investigations. We also recognize the negative impact of malware, botnets, and illicit online activities undertaken using anonymity techniques that may obfuscate location. However, we believe the solution to this complex problem should arise through public and legislative debate. The proposal before the Advisory Committee on Criminal Rules to modify Rule 41 of the FRCrmP has significant implications for open legal and policy issues, as well as broad technological consequences affecting the privacy of computer users worldwide. We believe the Judicial Conference should withdraw the proposed changes to Rule 41 from its rulemaking process, and that the proposal should instead be deliberated in Congress.

I. The Proposed Amendment

Rule 41 of the FRCrmP is of fundamental importance to how the Fourth Amendment warrant requirement for government search and seizure applies in practice. Any changes to the Rule should be viewed in this context and carefully avoid creating new risks to privacy and security. However, the proposed modifications to FRCrmP Rule 41 would have significant legal and technical implications, described below, that merit open consideration by Congress, rather than a rulemaking proceeding of the Judicial Conference.

Under the current FRCrmP Rule 41, magistrates with authority in a particular district can issue warrants for the search and seizure of property:

- a. Located within the district at the time of the search;

¹ Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure, Committee on Rules of Practice and Procedure, Judicial Conference of the United States, pgs. 338-339, Aug. 2014, www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf.

- b. Located within the district at the time the warrant is issued, but which may move outside the district prior to the search;
- c. Located within or outside the district in terrorism cases if the magistrate has authority in a district in which activities related to terrorism may have occurred;
- d. Via tracking device, if the tracking device is installed in the district, even if it continues to function outside the district; and,
- e. Located outside the jurisdiction of any district, but within a U.S. territory, possession, commonwealth, or diplomatic mission.²

The proposed amendment to FRCrmP Rule 41 would provide magistrates with new powers to authorize warrants to remotely search and seize or copy electronic media located outside the magistrate's district.³ Per the proposal, magistrates would be able to exercise this power in two circumstances:

- a. When the physical location of the media or information is "concealed through technological means," or
- b. In an investigation of 18 U.S.C. 1030(a)(5), when the damaged protected computers are located in five or more districts.⁴

II. Legal Implications

The proposed modification to FRCrmP Rule 41 would make policy decisions about important questions of law that are not currently settled and would best be resolved through legislation.

A. **The proposed Rule 41 amendment would authorize searches that violate the particularity requirement of the Fourth Amendment.**

If the physical location of the electronic media to be searched is unknown, the search may not satisfy the particularity requirement of the Fourth Amendment, which requires that the "place to be searched" be particularly described.⁵ In *In Re Warrant to Search a Target Computer at Premises Unknown*, the magistrate judge rejected a government application for a warrant to search and copy information from a computer, the location of which was unknown at the time of the application. The court concluded that the application did not satisfy the particularity requirement of the Fourth Amendment because the application did not describe the place to be searched.⁶ The court also noted that, because the computer's location and owner were

² Rule 41(b)(1)-(5), Search and Seizure, Federal Rules of Criminal Procedure.

³ *Supra*, fn 1.

⁴ Under 18 U.S.C. 1030(e), the term "damage" means any impairment to the integrity or availability of data or a system, and the term "protected computer" means any computer affecting interstate or foreign communication - including computers located outside the United States.

⁵ "[...] no warrants shall issue, but upon probable cause [...] and particularly describing the place to be searched, and the persons or things to be seized." Fourth Amendment to the United States Constitution.

⁶ *In Re Warrant to Search a Target Computer at Premises Unknown*, F. Supp. 2d , 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013). "The court concludes that the revised supporting affidavit does not satisfy the Fourth Amendment's particularity requirement for the requested search warrant for the Target Computer."

unknown, the search could easily affect multiple innocent parties.⁷ The court's determination that the application was insufficient on Fourth Amendment grounds was wholly independent of the court's consideration of whether the current text of Rule 41 allows for warrants that authorize searches of computers in unknown locations.

The proposed FRCmP Rule 41 modification includes a note that states: "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 [...] leaving application of this and other constitutional standards to ongoing case law development."⁸ While we appreciate the fact that the Committee does not seek to address such questions in this rulemaking, the proposed modification to Rule 41 nonetheless does have direct bearing on these very questions since it specifically contemplates the issuance of warrants for computers in concealed locations.

B. The proposed Rule 41 amendment would authorize extraterritorial searches that circumvent the MLAT process and may violate international law.

If the physical location of a computer is concealed through technological means, the computer is potentially anywhere in the world. In commentary, the Department of Justice states that the proposed amendment does not purport to authorize courts to issue warrants that authorize the search of electronic media located in foreign countries.⁹ However, given the global nature of both the Internet and anonymizing tools,¹⁰ in practice the warrants will very likely be used to authorize searches of electronic media located outside the United States.

If the computer from which data is searched or copied is located abroad, then the search takes place abroad. Several cases hold that a seizure occurs when and where data is copied, even if the warrant to remotely search electronic media is issued in the United States, or if the agent reviewing data extracted remotely from electronic media is located in the United States. The Second Circuit, for example, held that the act of copying electronic data constitutes a seizure, even before an agent searches through the extracted data.¹¹ Other courts have held that a search or seizure of data occurs where the electronic storage media is located.¹²

⁷ *Id.* "The Government's application offers nothing but indirect and conclusory assurance that its search technique will avoid infecting innocent computers or devices[...] What if the Target Computer is located in a public library, an Internet café, or a workplace accessible to others? What if the computer is used by family or friends uninvolved in the illegal scheme?"

⁸ *Supra*, fn 1, at pg. 341.

⁹ Letter from Mythili Raman, U.S. Department of Justice, to Reena Raggi, Advisory Committee on the Criminal Rules, Sept. 18, 2013. Available at <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf> (pg. 174).

¹⁰ As an example, more than 85% of the users of Tor – a popular service that conceals computer location – are located outside the United States. Tor, Tor Metrics: Users, Top-10 countries by directly connecting users, <https://metrics.torproject.org/users.html> (last accessed Oct. 22, 2014).

¹¹ *U.S. v. Ganas*, 12-240-CR, 2014 WL 2722618 (2d Cir. June 17, 2014). See also *U.S. v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010).

¹² *U.S. v. Gorskhov*, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

Extraterritorial searches today typically take place in coordination with foreign governments under the Mutual Legal Assistance Treaty (MLAT) process.¹³ The issue of whether U.S. magistrates may circumvent MLATs and issue warrants to search data stored abroad is still under litigation.¹⁴ Yet the proposed amendment could be interpreted to authorize U.S. law enforcement to unilaterally search media located abroad, so long as the location is unknown at the time of the search. In practice, this will likely result in U.S. law enforcement agencies circumventing the MLAT process far more often than in present circumstances.

Unilateral extraterritorial searches may violate the international obligations of the United States. Established and binding customary international law provides that a state (i.e., a nation) may not exercise its power in any form in the territory of another state without that state's consent. As a corollary of this rule, U.S. law enforcement officers may only exercise their functions in the territory of another state with the consent of the other state, given by duly authorized officials of that state, and in compliance with the laws of both the United States and the other state.¹⁵ The Restatement (Third) of the Foreign Relations Law of the United States describes this stricture as "universally recognized."¹⁶ The proposed changes to FRCrMP Rule 41 could put U.S. law enforcement agencies at risk of violating this binding rule of sovereignty, as well as the principle of comity, when they unilaterally conduct searches of electronic media outside U.S. territory. Computer users abroad would have little or no remedy for an improper search by the U.S. government, including if that search or seizure damages the user's computer.

C. The proposed Rule 41 amendment would make changes through judicial rulemaking that have thus far occurred through legislation.

The proposed amendment to FRCrMP Rule 41 would authorize magistrates to issue warrants to search property that is located outside of their districts both when the warrant is issued and when the search occurs. Currently, Rule 41 grants magistrates limited authority to issue warrants to search property outside their districts. Only under subsections (b)(3) and (b)(5) of the Rule do magistrates have authority to issue warrants for property that is not located in the district both at the time when the warrant is issued and when the search is performed.¹⁷ In comments, the Department of Justice has analogized the language of the proposed amendment to Rule 41 to the current language in subsections (b)(3) and (b)(5) of Rule 41.¹⁸

¹³ MLATs and Mutual Legal Assistance Agreements (MLAA) allow for the exchange of evidence in criminal matters between nations party to the treaty or agreement. The United States has an MLAT or MLAA in place with a large number of foreign nations. See 2012 International Narcotics Control Strategy Report: Treaties and Agreements, Dept. of State, Mar. 7, 2012, available at <http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm>.

¹⁴ See, e.g., Stipulation Regarding Contempt Order, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, Case Nos. 13-MAG-2814, M9-150, S.D.N.Y. (Sep. 2014), available at http://media.scmagazine.com/documents/91/microsoft_contempt_filing_22623.pdf.

¹⁵ Restatement (Third) of the Foreign Relations Law of the United States, §§ 432(2), 433.

¹⁶ *Ibid.* at § 432, comment (b).

¹⁷ Rule 41(b)(1)-(5), Search and Seizure, Federal Rules of Criminal Procedure.

¹⁸ *Supra*, fn 9.

However, both (b)(3) and (b)(5) have legislative roots not present in the newly proposed amendment to Rule 41.

Subsection (b)(3) of Rule 41 allows magistrates in any district in which terrorism-related activities have occurred to issue warrants for a person or property outside the district during investigations of domestic or international terrorism. This subsection was a Congressional amendment to Rule 41 as part of the USA PATRIOT Act of 2001.¹⁹

Subsection (b)(5) of Rule 41 was adopted in 2008 by the Judicial Conference as a rulemaking to allow magistrates to issue warrants for searches in areas under U.S. jurisdiction but outside of federal judicial districts, such as U.S. diplomatic or consular missions, located in foreign nations. However, U.S. jurisdiction in the areas listed in subsection (b)(5) was authorized by Congress. The Committee Notes to subsection (b)(5) state: “The rule is intended to authorize a magistrate judge to issue a search warrant in any of the locations for which 18 U.S.C. §7(9) provides jurisdiction.”²⁰ Accordingly, the language of subsection (b)(5) mirrors that of 18 U.S.C. §7(9), which was first codified through the USA PATRIOT Act of 2001.²¹

The Electronic Communications Privacy Act (ECPA) authorizes multi-district searches of computers.²² However, this too was an explicit grant of authority from Congress, not an instance of judicial rulemaking.

The proposed changes to FRCrMP Rule 41 are not a Congressional amendment, nor do they implement a direct expansion of extraterritorial jurisdiction codified in statute. Congress has not authorized extraterritorial or multi-district searches for computers with concealed locations or during investigations under 18 U.S.C. 1030(a)(5), as the proposed modification to Rule 41 contemplates. The proposed modification attempts to expand magistrates’ Rule 41 authority in a manner that has historically been accomplished by Congressional action. The proposed modification should be handled through Congress rather than judicial rulemaking.

D. The proposed Rule 41 amendment raises new risks of forum shopping.

Authorizing the government to obtain a warrant from any district to search or seize multiple computers located in any district raises a significant risk of forum shopping. The proposed change to Rule 41 would incentivize agents to seek out and reuse districts that were more inclined to approve warrant applications. In practice, this may frequently result in warrants issued in districts remote from the individual whose electronic media is searched or seized, making it prohibitively inconvenient or expensive for the individual to appear in the district to exercise her right to contest the warrant.

¹⁹ Sec. 219, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. Law 107-56, 107th Cong.

²⁰ Title 18, U.S. Code, Appendix, Federal Rules of Criminal Procedure, Title VIII, Rule 41, Committee Notes.

²¹ *Id.*, fn 19, Sec. 804.

²² 18 U.S.C. 2703(a), as modified by Sec. 220 of the USA PATRIOT Act of 2001.

III. **Technological Implications**

The proposed modification to Rule 41 would enable the U.S. government to gain authorization from any district in the United States to spread invasive malware – code that may penetrate, search, and copy electronic media without user authorization – to potentially any computer worldwide. This essentially allows law enforcement to hack computers with few restrictions on where an intrusion can take place and how many devices to which they may gain entry. It is tailored poorly and can reach practically any computing device while it also implicates many types of common and lawful methods of using the Internet. Finally, the act of intrusion into these devices may substantially damage the devices, the data resident on them, or the functions the devices mediate.

A. **“Concealed through technological means” is overly broad.**

The trigger language in the proposed amendment that the location of a target device be “concealed through technological means” before a warrant can be issued is overly broad, encompassing legitimate Internet use globally, not just within the United States, on devices for which the primary function is unknown to the government.

The Internet and software that interacts with it – email clients, web browsers, apps, etc. – have developed many ways to conceal a user’s location, either intentionally to protect privacy but often as a side effect of accomplishing another goal, such as confidentiality. The intent of this part of the rule amendment seems to be to allow agents of law enforcement to de-anonymize users of online anonymity tools, such as the Tor network. However, there is a much larger ecosystem of similar technologies that encompass technical methods that effectively re-route traffic over the Internet. Close to half of all U.S. businesses use Virtual Private Network (VPN) technologies or other forms of secure proxies.²³ VPNs and secure proxies seek to ensure that a user can interact with sensitive data – e.g., trade secrets, medical data, financial data – even when they are forced to use potentially hostile local networking environments, such as the unencrypted free wireless Internet access offered at hotels, airports, and coffee shops. These technologies establish a fully encrypted secure connection with a trusted server on the Internet, and that trusted server “proxies” their network activity – meaning it appears as if all network traffic comes from the proxy server instead of the user’s real network location.

There exist additionally a set of techniques that are designed to misreport identifiers that may associate a user’s identity with their activity online. For example, to protect the privacy of the hundreds of millions of users of Apple’s iOS mobile operating system from forms of in-store retail tracking that can follow shoppers from store to store, Apple has begun randomizing a common network identifier – the MAC address.²⁴ This will have the effect of “concealing through technical means” the network location of a device. Finally, the proposed amendment

²³ 42% of U.S. business respondents across company size segments use VPNs. See, Nav Chander, “Choosing the Best Enterprise IP VPN or Ethernet Communication Solution for Business Collaboration,” *International Data Corporation* (whitepaper produced for AT&T, Inc.), (June 2014), available at: http://www.business.att.com/content/whitepaper/vpn_ethernet.pdf (pg. 2).

²⁴ Lee Hutchinson, “iOS 8 stymie trackers and marketers through MAC address randomization,” *Ars Technica* (June 9, 2014), available at: <http://arstechnica.com/apple/2014/06/ios8-to-stymie-trackers-and-marketers-with-mac-address-randomization/> (last accessed October 23, 2014).

seems to reach somewhat trivial forms of location obfuscation that are not technically technical but could be construed as such. For example, if a user of a social network service such as Facebook misreports the city in which they live, or if a user of a web browser modifies how the browser reports their native language, these seem to qualify as “concealing through technical means” the user’s location. Legitimate uses of technology that have the effect of “concealing through technological means” a user’s location, e.g., using a VPN or Apple’s iOS mobile operating system, should not trigger the ability for a judge to issue a Rule 41 warrant.

The pervasive nature of technical means that have the purpose or effect of concealing the user’s location is indicative that concealment does not necessarily indicate a crime. In fact, the core technology this rule amendment seeks to reach, the Tor network and Tor Browser software, was developed primarily for two purposes that are fundamentally legitimate: the need of law enforcement as well as military and civilian intelligence agencies to access information services in hostile environments and the need of dissidents in repressive regimes to communicate with the larger, outside world.²⁵ Additionally, users that may be concerned about their privacy or security given threats online or to their person also use proxy technologies that securely obfuscate their location; this can encompass stalking victims and public servants that face threats of physical harm. Employees of businesses that deal in sensitive data such as finance or medicine may be required to use these kinds of technologies within the scope of their employment; for example, some businesses require their employees to route all traffic through a proxy that can detect viruses or malware, examine traffic for attempts to exfiltrate valuable intellectual property, or even a “caching proxy” that seeks to ease the load on a network by storing commonly retrieved resources such as images, videos, or other large files. Finally, we cannot rule out the possibility that an attempt to conceal location could actually be a simple misconfiguration or other error such that details like a computer’s Internet Protocol (IP) address may be misreported.

Of course, technically, a device that uses any of the techniques mentioned above can be anywhere in the world, and the context of the device’s true function (or contents) will in general be uncertain. As we outline above in Section II.B, this legally extends U.S. law enforcement jurisdiction globally. To the extent U.S. law enforcement uses this rule to hack into devices around the world, we should not be surprised when law enforcement entities from other nations conclude they should have this ability as well. Outside the question of the compatibility of legal regimes that are best dealt with in formal MLAT processes, there are serious questions about the uncertain functional context of a target device. That is, if the location of a device is unknown, concealed, or uncertain, we should expect that the purpose of the device will also be equally if not more uncertain. Law enforcement will have little data from which to ascertain how careful they need be while executing the search and seizure, lest they irreversibly damage the device, connected devices, or critical functionality the device may mediate. Unlike in the physical world, where the implications of an intrusion into a premises are relatively certain and easy to understand, the consequences in cyberspace can be very difficult to estimate. By way of analogy, in the physical world, agents of law enforcement can be reasonably confident that breaking and entering into premises won’t cause the entire building to fall down. Similarly, they can also be reasonably confident that such an intrusion won’t also cause the collapse of a

²⁵ See, e.g., “Who uses Tor?” available at: <https://www.torproject.org/about/torusers.html.en>.

series of nearby buildings or, for that matter, that a building they thought was a typical family home isn't actually the control system for a nuclear power plant. In cyberspace we cannot be so confident.

B. “Damaged” computers, under 18 U.S.C. 1030(a)(5), covers a very large quantity of machines.

The proposed changes to Rule 41 would allow the government to obtain a warrant in any district to remotely search five or more “damaged” computers during investigations of 18 U.S.C. 1030(a)(5). The justification for this proposal has been discussed in context of law enforcement action against botnets – networks of private computers infected with malware that enables an unauthorized party to use or control all or parts of the infected computers remotely.²⁶ As the FBI notes, millions of infected computers can be part of a botnet.²⁷ However, 18 U.S.C. 1030(a)(5) does not only encompass botnets.

18 U.S.C. 1030(a)(5) prohibits causing “damage” to protected computers intentionally without authorization or recklessly. “Damage” is defined broadly under the statute to include any malware, virus, Trojan, or even benign code that impairs “the integrity or availability of data.”²⁸ While botnets may involve using infected computers to commit additional crimes (such as distributed denial-of-service attacks), computers infected with viruses are not necessarily committing any subsequent crime – though the act of damaging the computer by infecting it with a virus is a crime under 1030(a)(5).

Because the proposed modification to Rule 41 would apply to investigations into any violation of 1030(a)(5), not just botnets, the proposed modification would enable the government to more easily remotely search computers infected with any virus or other damaging code. Approximately 30 percent of all computers worldwide, as well as in the United States, are estimated to be infected with some type of malware.²⁹ The number of computers that may therefore be subject to multidistrict searches under the proposed Rule 41 amendment is massive.

C. Data stored on devices is increasingly sensitive and intrusion may damage the device, its data, and/or dependent systems.

The language of the proposed amendment that allows law enforcement to “use remote access to search electronic storage media to seize or copy electronically stored information” will allow access to data of an exceedingly sensitive nature in many cases.

While the particularity of a warrant under the 4th Amendment requires the government to specify exactly the materials they seek to search for and seize, the proposed amendment would grant access to a panoply of sensors on modern computing platforms. Desktop

²⁶ *Supra*, fn 9, pg. 172.

²⁷ Botnets 101, Federal Bureau of Investigation, Jun. 5, 2013, available at http://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them.

²⁸ 18 U.S.C. 1030(e)(8).

²⁹ Panda Security, Annual Report PandaLabs, 2013 Summary, pg. 5, available at press.pandasecurity.com/wp-content/uploads/2010/05/Annual-Report-PandaLabs-2013.pdf.

computers, laptop computers, tablet computers and mobile computing devices contain an increasing array of sensors capable of reading current environmental and personal data – for example, microphones, cameras, motion sensors, and more complex accessories such as fitness tracking devices that measure fine-grained body data. Using these sensors, these devices store a multitude of sensitive data over time – personal photographs and videos, financial data, medical records, educational materials. As the Supreme Court recognized recently, networked devices like smartphones increasingly hold “a digital record of nearly every aspect of [our] lives – from the mundane to the intimate.”³⁰ As mentioned above, the target device can be potentially any device attached to the Internet from personal computing devices to industrial control systems to Internet voting systems. Allowing law enforcement a broad remit to remotely access such sensitive information systems will have grave consequences for personal privacy and liberty, as well as the integrity of critical systems.

The acts of intrusion onto a device and/or seizing data may result in impairment of the device or data resident on the device. Intrusion methods necessarily exploit weakness in the defenses of a device to gain access. Practically speaking, “network investigative techniques” employ flaws or bugs in software like web browsers such that law enforcement can gain access to the larger system. Vulnerabilities or flaws in a system are by definition features the designers of the system did not plan the system’s functionality to take into account. “Network investigative techniques” used by law enforcement can vary from relatively simple Computer and Protocol Address Verifier (CIPAV) tools that seek to assess and report network identifiers and information back to law enforcement agents to deeper forms of persistent access where invasive methods like rootkits – i.e., programs designed to completely evade system defenses and be highly resistant to removal – which can potentially permanently damage a device. Further, it is unclear from the text of the proposed amendment and relevant jurisprudence if the extent of “seizing” data does not merely copy the data but may also render it unusable by the user. If seizing and copying are distinct in this manner, a seizure of data could potentially deprive the user of critical data or system functionality without due process before a finding of guilt has been made.

The act of intrusion and installing a “network investigative technique” can not only harm the device but also potentially result in further follow-on damage due to vulnerabilities introduced into the system or exacerbated by the technical act of gaining entry. To the extent the intrusion technique causes damage or triggers malware that causes ancillary damage, the device itself may be no longer functional, along with any data it holds and any actions in the real world it performs. There are examples of adversarial network investigation that resulted in taking an entire country off the Internet³¹ as well as buggy law enforcement intrusion code that left targeted devices seriously vulnerable to subsequent malicious attacks.³²

³⁰ *Riley v. California*, 573 U. S. ____ (2014) at 19.

³¹ Spencer Ackerman, “Snowden: NSA accidentally caused Syria’s Internet blackout in 2012,” *The Guardian* (August 13, 2014), available at: <http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war> (last accessed October 23, 2014).

³² Chaos Computer Club, “Chaos Computer Club analyzes government malware,” (October 8, 2011), available at: <https://www.ccc.de/en/updates/2011/staatstrojaner> (last accessed October 23, 2014).

D. Concealment of the location of “information” can potentially reach even more devices.

The proposed amendment does not just trigger on concealing the location of a device with technical means but also concealment of the location of information. Similarly to the discussion above in Section III.A of the variety of activities that by their nature obscure the location of a device, there are a number of modern computing techniques that obscure the location of information, mostly for efficiency gains related to data mining and analysis.

For example, rather than keeping very large databases of information in a single location, many modern computing techniques rely on a technique called “sharding,” or the process of breaking up individual pieces of a database and redistributing them across disparate computing facilities. If a target machine has information sharded across tens or hundreds of additional machines, the proposed amendment would appear to reach all of those devices as well. There are more exotic types of data structures – for example, hash tables and bloom filters – that do similar things from the perspective of technically concealing the location of information; some of these techniques are very difficult – by design – to map onto a physical location or the specific device on which the data may be stored.

IV. Practical implications

In addition to the legal and technical implications, we are concerned that a slew of negative practical implications may be relevant once law enforcement gains the abilities contemplated by the proposed rule.

First, the rule essentially eliminates existing practical limits on law enforcement search and seizure in networked computing. The Department of Justice indicated that under the current Rule 41, agents seeking authority to search computers in multiple districts must obtain warrants with magistrates in every district in which the computers are known to be located (except in cases of domestic or international terrorism).³³ As a practical matter, agents currently must be judicious in deciding which computers to remotely search. However, if the requirement to obtain warrants from each district in which the property is known to be located were removed, the likely effect would be for far more remote searches of far more machines. As we argue above, the number of computers for which location is concealed, or which are “damaged” may well run to many millions. The potential for abuse or overzealous and sloppy law enforcement hacking is very real.

Further, there are follow-on implications from this collapsing of practical limitations. Authorizing law enforcement to operate in this manner may lead to more intrusive methods being brought to bear. If malware that reveals computer location is easily bypassed or rendered ineffective, law enforcement may have to use more powerful techniques that are more likely to threaten the integrity of the target device or information. For example, a simple web beacon that can report a device’s IP address back to law enforcement can be blocked by common software (e.g., Little Snitch) that prohibits network requests to unknown addresses. The government

³³ *Supra*, fn 9, pg. 173.

may then attempt more intrusive – necessarily less reasonable – searches of the contents of media to gather clues regarding location.

Finally, the proposed rule amendment and the law enforcement hacking that may result has the potential to spark a deadly arms race. Malicious hackers may begin to purposefully stage attacks from computers running critical infrastructure and applications. If an intrusion renders these devices inoperable – either by design or accident – the implications for just one such incident could be profound for society. We may very well see staging of malware on critical infrastructure coupled with “trip wires” that are armed to cause damage and havoc when an attempted intrusion is detected.

V. **This is an issue for Congress**

Law enforcement clearly faces challenges in remotely searching electronic media in concealed locations. However, the proposed rule has important technical, legal, and practical implications that necessitate the deliberation of Congress. We recommend that the Judicial Conference reject the proposed changes to Rule 41 and instead urge Congress to address the issue of remote searches of electronic media located in multiple districts or in unknown locations.

END

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8f7q-rd5k
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0010](#)

Testimony of Alan Butler, on behalf of Electronic Privacy Information Center (epic.org)

Submitter Information

Name: Alan Butler

Organization: Electronic Privacy Information Center (Epic.org)

General Comment

See attached

Attachments

Testimony for Nov. 5 Hearing



Testimony and Statement for the Record of

Alan Butler
Senior Counsel
Electronic Privacy Information Center

on

Proposed Amendments to Rule 41
of the Federal Rules of Criminal Procedure

before the

Judicial Conference Advisory Committee on Criminal Rules

November 5, 2014

Judge Raggi, Members of the Advisory Committee on the Federal Rules of Criminal Procedure, thank you for the opportunity to participate in today's hearing on the proposed amendments. My name is Alan Butler and I am Senior Counsel at the Electronic Privacy Information Center ("EPIC").

EPIC is a non-partisan research organization in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.¹ We work with a distinguished panel of advisors in the fields of law, technology, and public policy.² EPIC has previously filed *amicus* briefs in cases concerning the core procedural protections granted under the Fourth Amendment: notice and the opportunity to challenge the scope of a government search. For example, in 2002 EPIC filed a brief in *United States v. Bach*, arguing that the Fourth Amendment requires officer presence during the execution of a warrant and that it was therefore unlawful to serve a warrant on an Internet Service Provider via facsimile.³

EPIC has a particular interest in ensuring that Fourth Amendment privacy rights are not eroded by the use of emerging surveillance technologies. As Justice O'Connor famously addressed in *Arizona v. Evans*, "[w]ith the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities."⁴ In an effort to maintain these constitutional responsibilities, EPIC routinely participates as *amicus curiae* in major Supreme Court cases addressing Fourth Amendment rights in the context of emerging technologies.

For example, in 2011 EPIC, joined by thirty legal scholars and technical experts, filed a brief in *United States v. Jones*, arguing that the use of invasive GPS tracking systems is a search requiring a warrant under the Fourth Amendment.⁵ The Court ultimately found that the warrantless installation and use of a GPS device to track an individual over 30 days violated the Fourth Amendment.⁶ In 2012, EPIC, joined by thirty-two legal scholars and technical experts, as well as eight transparency organizations, filed a brief in *Clapper v. Amnesty International, USA*, arguing that the NSA's Signals Intelligence capabilities have expanded to the point where it would be reasonable for United States persons to assume that all of their communications sent abroad are being routinely collected.⁷

In 2013, EPIC, joined by twenty-four legal scholars and technical experts, filed a brief in *Riley v. California*, arguing that modern cell phones provide access to a wealth of sensitive

¹ *About EPIC*, EPIC, <https://epic.org/epic/about.html>.

² *EPIC Advisory Board*, EPIC, http://epic.org/epic/advisory_board.html.

³ See Brief of *Amicus Curiae* EPIC in Support of Appellee, *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238).

⁴ 514 U.S. 1, 17-18 (1995); see also *EPIC, Sandra Day O'Connor's Legacy*, <https://epic.org/privacy/justices/oconnor/>.

⁵ See Brief of *Amici Curiae* EPIC and Legal Scholars and Technical Experts in Support of the Respondent, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259).

⁶ *Jones*, 132 S. Ct. at 949.

⁷ See Brief of *Amici Curiae* EPIC, Thirty-two Technical and Legal Scholars, and Eight Transparency Organizations in Support of Respondents, *Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138 (2013) (No. 11-1025).

personal data and that phones should not be subject to warrantless searches incident to arrest.⁸ In *Riley*, the Court unanimously held that officers may not search the contents of a cell phone without a warrant, even where that phone is seized during a lawful arrest.⁹ The Court in *Riley* addressed the importance of the procedural protections established by the Fourth Amendment. Rejecting the government’s argument that law enforcement protocols would suffice to limit access to certain sensitive information, the Court emphasized that “the Founders did not fight a revolution to gain the right to government agency protocols.”¹⁰ The Court also found that cell phone searches could be particularly invasive because they would allow the inspection of remotely stored files.¹¹

We appreciate the Committee’s important work in maintaining the Federal Rules of Criminal Procedure. In my statement today, I will: (1) describe the history of two key Fourth Amendment requirements relevant to Rule 41: notice and officer presence upon execution of a warrant; (2) discuss the history of and limitations on “covert entry” warrants; and (3) recommend that the proposed amendment not be adopted because it would authorize unreasonable law enforcement practices and inhibit the development of Fourth Amendment standards for remote access searches.

I. It is Well Established That Notice, Officer Presence, and Other Formalities Are Key to Fourth Amendment Reasonableness

The Fourth Amendment was adopted to ensure that there were procedural safeguards against the arbitrary exercise of governmental authority, “securing to the American people, among other things, those safeguards which had grown up in England to protect the people from unreasonable searches and seizures”¹² The Supreme Court’s decision in *Weeks v. United States* heralded the dawning of the age of constitutional criminal procedure, in which the Court established the exclusionary rule, prohibiting introduction of evidence obtained in violation of the Fourth Amendment, and identified the core practices and formalities that now circumscribe lawful searches. The exclusionary rule was essential to the protection of Fourth Amendment rights because introduction of unlawfully obtained evidence at trial would “affirm by judicial decision a manifest neglect if not an open defiance of the prohibitions of the Constitution, intended for the protection of the people against such unauthorized action.”¹³

The Court in *Weeks* recognized that prohibiting the government’s use of improperly obtained evidence was necessary to ensure that the formalities and procedural safeguards required by the Fourth Amendment were followed. “The effect of the 4th Amendment is to put the courts of the United States and Federal officials, in the exercise of their power and authority, under limitations and restraints as to the exercise of such power and authority. . . .”¹⁴ Relaxing

⁸ See Brief of *Amicus Curiae* EPIC and Twenty-four Technical Experts and Legal Scholars in Support of Petitioner, *Riley v. California*, 134 S. Ct. 2473 (2014) (No. 13-132).

⁹ *Riley*, 134 S. Ct. at 2494.

¹⁰ *Id.* at 2491.

¹¹ *Id.* (citing Brief for Electronic Privacy Information Center in No. 13-132, at 12-14, 20).

¹² *Weeks v. United States*, 232 U.S. 383, 391 (1914).

¹³ *Id.* at 394.

¹⁴ *Id.* at 393.

well-established procedures would lead to “gradual depreciation of the rights secured by [the Fourth Amendment] by imperceptible practice of courts or by well-intentioned but mistakenly over-zealous executive officers.”¹⁵

Even where an officer conducts a search pursuant to an authorized warrant, the Fourth Amendment requires that certain procedural formalities be followed to protect against abuse. Since the 1700s, United States law has required an officer’s presence during the service of a search warrant.¹⁶ An officer’s presence discourages government abuse of power and unwarranted intrusion upon privacy by ensuring guarantees of trustworthiness and accountability. The Supreme Court has long recognized the importance of strict adherence to procedural safeguards in the execution of search warrants, because “[i]t may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing . . . by *silent approaches and slight deviations from legal modes of procedure.*”¹⁷ Therefore, “[i]t is the duty of the courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachment thereon.”¹⁸

But officer presence alone is not sufficient to make the service of a warrant reasonable under the Fourth Amendment; the method of entry into the place to be searched is also an important consideration. As the Supreme Court stated, “we have little doubt that the Framers of the Fourth Amendment thought that the method of an officer’s entry into a dwelling was among the factors to be considered in assessing the reasonableness of a search or seizure.”¹⁹ In fact, the Court has held that notice provided in advance of a search is an important element of Fourth Amendment reasonableness.

In *Wilson v. Arkansas*, the Court found that advanced notice was a clearly established requirement of a reasonable search based on the common law history and practice.²⁰ The Court also found that its own cases supported the principle of prior notice as being “embedded in Anglo-American law.”²¹ The Court unanimously held that the “common-law ‘knock and announce’ principle forms a part of the reasonableness inquiry under the Fourth Amendment,” specifically stating that “an officer’s unannounced entry into a home might be unreasonable under the Fourth Amendment.”²²

Notice, officer presence, and other formalities are necessary to guarantee accountability and trustworthiness in the exercise of police power. As the Supreme Court has emphasized, “[t]he value judgment that [has historically] motivated a united democratic people fighting to defend those very freedoms from totalitarian attack is unchanged.”²³ Procedural formalities are

¹⁵ *Gouled v. United States*, 255 U.S. 298, 304 (1921).

¹⁶ *See Boyd v. United States*, 116 U.S. 616, 624 (1886) (detailing the history of search and seizure law and procedure).

¹⁷ *Boyd*, 116 U.S. at 633. (emphasis added).

¹⁸ *Id.*

¹⁹ *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995).

²⁰ *Id.* at 931.

²¹ *Id.* at 934 (quoting *Miller v. U.S.* 357 U.S. 301, 313 (1958)).

²² *Id.* at 929, 934.

²³ *Watchtower Bible & Tract Soc’y of N.Y., Inc. v. Vill. of Stratton*, 122 S. Ct. 2080, 2091 (2002).

critical in preserving our privacy in order to maintain cherished values of humanity and civil liberty. In *McVeigh v. Cohen*, which addressed unauthorized access to electronic communications, the court stated:

In these days of “big brother,” where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed.²⁴

Fundamental principles “established by years of endeavor and suffering” cannot be sacrificed to the needs or convenience of law enforcement.”²⁵ Notice and officer presence are key elements of reasonableness under the Fourth Amendment and courts should only allow deviation from these requirements with caution and under very strict and limited conditions.

II. Courts Have Only Allowed Delayed Notice and Permitted Covert Entry Warrants in Limited Circumstances

In certain limited circumstances, courts have held that law enforcement officers may execute search warrants through covert means and without prior notice to the subject.²⁶ The authority to conduct “surreptitious searches and seizures”²⁷ has been limited to cases where (1) delayed notice and covert entry is necessary, and (2) notice will be provided within a reasonable time after the search.²⁸ This is consistent with the Supreme Court’s holding that notice is an element of Fourth Amendment reasonableness.²⁹

The judicial authorization of surreptitious searches, initiated without prior notice to or confrontation of the subject, is a relatively new development in the history of Fourth Amendment law. Covert entry warrants were not contemplated during the founding era, and no published opinions in the United States addressed them until 1985. In *United States v. Frietas*, the Ninth Circuit found the Fourth Amendment requires that “surreptitious entries be closely circumscribed.”³⁰ Drawing on the limitations on wiretapping outlined in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520, the court in *Frietas* found that both “the necessity for the surreptitious seizure and the subsequent notice” were an important element of the Fourth Amendment reasonableness analysis.³¹

The Ninth Circuit in *Frietas* noted that the Fourth Amendment does not prohibit all surreptitious entries, as the Supreme Court’s held in *Dalia v. United States*,³² but that “absence of

²⁴ 983 F. Supp. 215, 220 (D.D.C. 1998).

²⁵ *Weeks*, 232 U.S. at 393.

²⁶ See Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment “Rule Requiring Notice,”* 41 Pepp. L. Rev. 509, 519-25 (2014).

²⁷ Also referred to as “sneak and peek” or “sneak and steal” warrants.

²⁸ See *United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990).

²⁹ *Wilson v. Arkansas*, 514 U.S. 927, 929 (1995).

³⁰ *United States v. Frietas*, 800 F.2d 1451, 1456 (9th Cir. 1985).

³¹ *Id.*

³² 441 U.S. 238 (1979).

any notice requirement in the warrant casts strong doubt on its constitutional adequacy.”³³ The Court in *Dalia* rejected a defendant’s argument that officers’ covert entry into his office to install “bugging equipment” violated the Fourth Amendment.³⁴ The Court found that “[t]he Fourth Amendment does not prohibit *per se* a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment.”³⁵ However, in its finding that the surreptitious entry was constitutional, the Court relied upon the lower court finding that the “safest and most successful method of accomplishing the installation of the wiretapping device was through breaking and entering [the office].”³⁶ The Court also found that delayed notice equivalent to that provided under Title III would be a “constitutionally adequate substitute for advance notice” in the case of a covert entry warrant.³⁷

The U.S. Court of Appeals for the Second Circuit later addressed the validity of surreptitious search warrants in a series of cases beginning in 1990. In *United States v. Villegas*, the Second Circuit considered a defendant’s challenge to a surreptitious search of his farmhouse, executed pursuant to a warrant but without notice until his arrest two months later.³⁸ The court found that “certain safeguards are required where the entry is to be covert,” but concluded “appropriate conditions were imposed” in that case.³⁹ Specifically, the court found that “two limitations on the issuance of warrants for covert-entry searches for intangibles are appropriate.”⁴⁰ The first requirement is that officers show a “reasonable necessity” for not providing advance notice of the search.⁴¹ The second requirement is that delayed notice must be given “within a reasonable time after the covert entry.”⁴² The court agreed with the Ninth Circuit’s finding in *Frietas* that “as an initial matter, the issuing court should not authorize a notice delay of longer than seven days,” but may grant extensions thereafter based on a “fresh showing of the need for further delay.”⁴³ Subsequent lower court decisions, addressing covert entry warrants, have failed to recognize that notice is an important element of Fourth Amendment reasonableness, as the Supreme Court found in *Wilson v. Arkansas*.⁴⁴

Congress later authorized the issuance of delayed notice warrants in Section 213 of the USA PATRIOT Act, but only in certain circumstances.⁴⁵ The law includes three express limitations on the issuance of delayed notice warrants, similar to those imposed by the Ninth Circuit in *Frietas* and the Second Circuit in *Villegas*: first, the issuing court must find “reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result,” second, the warrant must prohibit the seizure of tangible property and electronic files, “except where the court finds reasonable necessity for the seizure,”

³³ *Frietas*, 800 F.2d 1456.

³⁴ *Dalia*, 441 U.S. at 241-42.

³⁵ *Id.* at 248.

³⁶ *Id.* at 248 n.8.

³⁷ *Id.* at 248.

³⁸ 899 F.2d 1324, 1336 (2d Cir. 1990).

³⁹ *Id.*

⁴⁰ *Id.* at 1337.

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ See Witmer-Rich, *supra*, at 524 n.86.

⁴⁵ 18 U.S.C. § 3103a.

and finally, the warrant must provide for notice within a “reasonable period not to exceed 30 days.”⁴⁶ Prior to the enactment of the Patriot Act, some courts had held that the failure to provide notice is not *per se* unconstitutional,⁴⁷ but these decisions do not fully address the fact that notice is a core element of Fourth Amendment reasonableness, as the Court found in *Wilson*.

Existing precedents do not support the conclusion that surreptitious warrants may be issued without first establishing that delayed notice is necessary and providing for future notice within a reasonable period of time.

III. The Proposed Amendment to Rule 41 Would Depart from Established Precedent and Inhibit the Future Fourth Amendment Development

Because it would authorize the issuance of digital surreptitious search warrants without requiring a showing that such methods are necessary or that notice be given within a reasonable amount of time after the search, the proposed amendment to Rule 41 would be inconsistent with well-established Fourth Amendment precedents.

The rule would grant magistrates the authority to “issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information” if either (1) “the district where the media or information is located has been concealed through technological means” or (2) “in an investigation of a violation of 18 U.S.C. § f1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.”

An officer applying for a remote access warrant under the proposed revision of Rule 41 would not have to make any showing that the delay in notifying the target of the search is reasonably “necessary” for the investigation. Rather, the Rule would authorize issuance of a surreptitious search warrant in any case where the target of the search has used an online proxy tool. There may be some cases where a court would find it is reasonably necessary to use remote access tools, but that will not be the case in every instance where the target is using a proxy service. Without a requirement that the requesting officer establish necessity as required for all other covert search warrants, the proposed rule will be overbroad.

Furthermore, the proposed amendment to Rule 41(f)(1) would not require an officer to provide notice within a reasonable time. Instead, the rule would require that the officer “make reasonable efforts” to serve a copy of the warrant. That is certainly necessary, but it is not sufficient, as the Court established in *Wilson* and circuit courts recognized in *Frietas* and *Villegas*. Even the delayed notice provision in the Patriot Act, which has been widely criticized for being overbroad, provides for notice within a “reasonable period not to exceed 30 days,” with a requirement that any further extensions be independently justified.

⁴⁶ 18 U.S.C. § 3103a(b).

⁴⁷ *See, e.g.,* United States v. Simons, 206 F.3d 392, 402-03 (4th Cir. 2000); United States v. Pangburn, 983 F.2d 440, 455 (2d Cir. 1993).

As drafted, the amended Rule 41 would authorize the issuance of overly broad covert search warrants and would not require sufficiently prompt notice to satisfy Fourth Amendment scrutiny.⁴⁸

The proposed amendments to Rule 41 would not only be constitutionally defective, they would also inhibit development of Fourth Amendment law in the area of remote electronic searches. Fourth Amendment law develops primarily through suppression motions filed by defendants in response to the use of new law enforcement techniques.⁴⁹ However, this process breaks down where the exclusionary rule is not available as a remedy to the defendants who might seek to challenge a new investigative technique.⁵⁰ The exclusionary rule is not an available remedy when the officer relied in good faith upon a warrant issued by a magistrate, even when that warrant is later deemed invalid.⁵¹

It would therefore be improper to grant new warrant authority by amending Rule 41 without first establishing that proposed rule is consistent with the Fourth Amendment. Future defendants who are subject to a search authorized under the amended rule would have no available remedy, and therefore no incentive to challenge potentially unconstitutional intrusions into their computer networks. In that case, the amendment itself would resolve the constitutional question before it is properly presented in an individual case.

Conclusion

The proposed amendments to Rule 41 would authorize searches beyond the scope permissible under the Fourth Amendment. Specifically, the rule would allow for surreptitious searches without the required showing of necessity, and the resulting warrants would not include the requirement that notice be served within a reasonable time after the search. For these reasons, the Committee should not adopt the proposed amendments as drafted.

Thank you for the opportunity to participate in today's hearing. I will be pleased to answer your questions.

⁴⁸ For example, the Seattle Times recently reported that the FBI used a link to a fake version of the newspaper's website to remotely install surveillance software on a suspect's computer. Mike Carter, *FBI Created Fake Seattle Times Web Page to Nab Bomb-threat Suspect*, (Oct. 27, 2014), http://seattletimes.com/html/localnews/2024888170_fbnewspaper1xml.html. The FBI special agent in charge was quoted as saying the FBI only uses remote access techniques "when there is sufficient reason to believe it could be successful in resolving a threat." *Id.*

⁴⁹ Orin Kerr, *Good Faith, New Law, and the Scope of the Exclusionary Rule*, 99 *Geo. L. J.* 1077, 1090 (2011).

⁵⁰ *Id.* at 1092-95.

⁵¹ *See United States v. Leon*, 468 U.S. 897, 925 (1984).

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8fht-7b3m
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0011](#)

Testimony of Kevin S. Bankston, on behalf of New America's Open Technology Institute

Submitter Information

Name: Kevin S. Bankston

Organization: New America's Open Technology Institute

General Comment

See Attached

Attachments

Testimony for Nov. 5 Hearing

**Testimony of Kevin S. Bankston,
Policy Director of New America’s Open Technology Institute**

**On Proposed Amendments to Rule 41
of the Federal Rules of Criminal Procedure**

**Before The Judicial Conference Advisory Committee
on Criminal Rules**

November 5, 2014

Members of the Committee,

Thank you for allowing New America’s Open Technology Institute (“OTI”)¹ to testify and share our concerns about the proposed amendment to Federal Rule of Criminal Procedure 41 regarding “remote access” searches of electronic devices.²

I am here today to question the basic and quite substantive premise implicit in the proposed amendment: that “remote access” searches by the government—or more accurately, the government’s surreptitious hacking into computers or smartphones in order to plant malware that will send data from those devices back to the government—are allowed by the Fourth Amendment.

Based on precedent almost half a century old, we believe the proposed amendment authorizes searches that are unconstitutional for lack of adequate procedural protections tailored to counter those searches’ extreme intrusiveness—much like the New York state electronic

¹ New America’s Open Technology Institute (“OTI”), <http://newamerica.org/oti/>.

² Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure: Request for Comment (Proposed Amendments Draft), 338-342 (Aug. 2014), *available at* <http://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0001> (authorizing issuance of warrants “to use remote access to search electronic storage media and to seize or copy electronically stored data” in cases where the target computer’s location “has been concealed by technological means” or in a computer crime investigation where the computers to be searched “have been damaged without authorization and are located in five or more districts”).

eavesdropping law that was struck down as unconstitutional by the Supreme Court in *Berger v. New York* nearly 50 years ago.³ There, the court held that because electronic eavesdropping “by its very nature...involves an intrusion on privacy that is broad in scope,” authority to conduct such surveillance should only be granted “under the most precise and discriminate circumstances” in order to ensure that the Fourth Amendment’s particularity requirement is met.⁴

In response to that 1967 case, Congress in 1968 passed the federal wiretapping statute often referred to as Title III.⁵ There, Congress addressed the Supreme Court’s Fourth Amendment concerns by providing a precise and discriminate warrant procedure for wiretapping and electronic eavesdropping,⁶ with procedural safeguards so demanding that commentators routinely refer to Title III orders as “super-warrants.”⁷

Foremost among those Title III safeguards are the four that are intended to enforce the Fourth Amendment’s particularity requirement consistent with the *Berger* decision, which held that “[t]he need for particularity...is especially great in the case of eavesdropping.”⁸ The court in *US v. Torres*,⁹ the first of many circuit courts to find that these four *Berger*-derived requirements are also constitutionally required for video surveillance,¹⁰ summarized them well:

³ 388 U.S. 41 (1967).

⁴ *Id.* at 56.

⁵ Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III” or the “Wiretap Act”), 18 U.S.C. § 2510 *et seq.*

⁶ *Id.* at §2518.

⁷ *See, e.g.,* Orin S. Kerr, *Lifting the “Fog” of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 *Hastings L.J.* 805, 815 (2003).

⁸ *Berger*, 388 U.S. at 56.

⁹ *United States v. Torres*, 751 F.2d 875 (7th Cir. 1984), *cert. denied*, 470 U.S. 1087 (1985).

¹⁰ *See United States v. Biasucci*, 786 F.2d 504, 508-10 (2d. Cir. 1986), *cert. denied*, 479 U.S. 827 (1986), *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251-52 (5th Cir. 1987), *United States v. Mesa-Rincon*, 911 F.2d 1433, 1436-39 (10th Cir. 1990), *United States v. Koyomejian*, 970 F. 2d 536, 538-42 (9th cir. 1991) (*en banc*), *cert. denied*, 506 U.S. 1005 (1992), *United States v. Falls*, 34 F.3d 674, 678-80 (8th Cir. 1994), and *United States v. Williams*, 124 F.3d 411, 416 (3rd Cir. 1997).

[T]he judge must certify that [1] “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous,” 18 U.S.C. § 2518(3)(c), and that [2] the warrant must contain “a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates,” § 2518(4)(c), [3] must not allow the period of interception to be “longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days” (though renewals are possible), § 2518(5), and [4] must require that the interception “be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under [Title III].¹¹

As the *Torres* court concluded, “Each of these four requirements is a safeguard against electronic surveillance that picks up more information than is strictly necessary and so violates the Fourth Amendment's requirement of particular description.”¹²

Title III, consistent with *Berger* and the Fourth Amendment's demand of reasonableness, also includes a clear requirement of service of notice on the target of the surveillance soon after the surveillance is completed—with no exceptions for failure to notify.¹³ And finally, Title III includes a number of additional “super-warrant” checks and balances intended by Congress to further ensure the reasonableness of the surveillance to balance its intrusiveness, including a requirement that such surveillance only be used in the investigation of specifically identified serious crimes.¹⁴ Only with such super-warrant protections in place have warrants for electronic surveillance been found constitutional under the Fourth Amendment.

Today, nearly half a century later, we are faced with a digital surveillance technique that is substantially more invasive than the analog electronic surveillance techniques of the past. Yet this

¹¹ *Torres*, 751 F.2d at 883-84.

¹² *Id.* at 884.

¹³ 18 U.S.C. §2518(8)(d).

¹⁴ 18 U.S.C. §2516(1); *see also Torres*, 751 F.2d at 890-91 (summarizing additional Title III requirements).

Committee, without any support from Congress or the courts, is poised to explicitly authorize warrants for such remote access searches with no additional protections at all and with a constitutionally novel allowance for no notice in certain cases. This is particularly concerning because the procedural protections required in cases of eavesdropping, wiretapping and video surveillance are even more necessary here, when the devices to which the government seeks access can contain an unprecedented wealth of private data—our digital “papers and effects.”

Indeed, the one published decision to address a warrant application regarding a remote access search—Magistrate Judge Smith’s opinion in Houston last year, the *In Re Warrant* case—rejected the application based not only on Rule 41 considerations but also based on a failure to satisfy the Fourth Amendment’s particularity requirement, including the enhanced *Berger/Torres* particularity requirements typically applied to electronic surveillance.¹⁵

The proposed amendment, in attempting to address the Rule 41 issue raised by Judge Smith’s opinion, necessarily also makes a substantive judgment regarding the Fourth Amendment’s application to remote access searches. It does so first by authorizing remote access searches where the location of the target computer is unknown—a type of search that Judge Smith found was a *per se* violation of the requirement that the “place to be searched” be particularly described¹⁶—and second by choosing not to insist that remote access searches meet the *Berger/Torres* requirements that undoubtedly apply.

Those requirements undoubtedly apply, as Judge Smith held,¹⁷ because remote access searches implicate and amplify all of the same problems as electronic surveillance, by virtue of providing access to an even greater wealth of private information. As he described, computers contain—and the government’s remotely installed software has the capacity to access—“Internet browser history, search terms, e-mail contents and contacts, ‘chat’, instant messaging logs, photographs, correspondence, and records of applications run, among other

¹⁵ *In Re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 758-61 (S.D. Tex. 2013).

¹⁶ *Id.* at 758-760.

¹⁷ *Id.* at 760-61

things....”¹⁸ Not only can government software secretly “search the computer's hard drive, random access memory, and other storage media,” but it can also “activate the computer's built-in camera[,] generate latitude and longitude coordinates for the computer's location[,] and[] transmit [all of that] extracted data to the FBI....”¹⁹

Like Judge Smith, the Supreme Court recently recognized the unprecedented amount of private data that may be stored on an electronic device such as a computer or a smartphone. As the Court explained in this year's *Riley v. California* decision regarding searches of cell phones incident to arrest, many cell phones “are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.”²⁰ These devices, with “immense storage capacity,” can hold “every picture [their users] have taken, or every book or article they have read,” and “even the most basic phones that sell for less than \$20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.”²¹ Stand-alone computers that could be reached by a remote access search can store even more—and even more types—of private data than the smartphones that the Supreme Court sought to protect against unreasonable searches. Ultimately, as the Supreme Court explicitly held, the search of a modern electronic device such as a smartphone or a computer is more privacy invasive than even “the most exhaustive search of a house”.²²

In this technological context, the constitutional necessity of applying the *Berger/Torres* particularity requirements to remote access searches is clear. That need—especially in regard to minimizing the search of devices or the seizure of data that are not particularly identified in the warrant—is amplified even further by several other risks that have been discussed at length by other commentators as well as Judge

¹⁸ *Id.* at 760.

¹⁹ *Id.* at 755.

²⁰ *Riley v. California*, 134 S. Ct. 2473, 2489 (U.S. 2014).

²¹ *Id.*

²² *Id.* at 2491.

Smith.²³ These risks include the privacy risk to non-suspects who share the target computer, which might be a public terminal at a library or a café;²⁴ the risk that the government’s software may spread to non-target computers;²⁵ the possibility, in cases of botnet investigations or so-called “watering hole” attacks, that thousands or even millions of computers may be infected with remote access software;²⁶ and the risk that software used to remotely access any of those computers may end up causing damage, either by altering or deleting data or creating security vulnerabilities that may be exploited by others.²⁷

Indeed, it may be that remote access searches carry so many risks that they are unreasonable under the Fourth Amendment or as a policy matter even if they satisfy the *Berger/Torres* requirements; notably, neither the courts nor Congress have yet addressed those questions. This brings us back to my starting proposition: that by explicitly authorizing remote access searches, the proposed amendment represents a substantive judgment regarding the constitutionality of those searches and a policy judgment regarding the appropriateness of such searches, regardless of the Committee Note’s claim that “[t]he amendment does not address constitutional questions.”²⁸

The proposed amendment’s explicit authorization of remote access searches where the computer location is not known, in the face of the one published decision on the matter finding that such searches are *per*

²³ *In Re Warrant*, 958 F. Supp. 2d at 759.

²⁴ *Id.*

²⁵ *Id.*

²⁶ *See, e.g.*, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning “Remote Access” Searches of Electronic Storage Media at 6-8, 14-15 (Oct. 31, 2014), *available at*

https://www.aclu.org/sites/default/files/assets/aclu_comment_on_remote_access_proposal.pdf (“ACLU Comments”) (discussing “watering hole” attacks on visitors to popular websites); Written Statement of the Center for Democracy & Technology Before the Judicial Conference Advisory Comm. on Criminal Rules at 8, 10 (Oct. 24, 2014), *available at* <https://cdt.org/insight/testimony-for-the-judicial-conferences-advisory-committee-on-criminal-rules-rule-41/> (“CDT Comments”) (discussing how botnet investigations may implicate millions of computers).

²⁷ *See, e.g.*, ACLU Comments at 9-10, 17-18; CDT Comments at 8-9.

²⁸ Proposed Amendments Draft at 341.

se violations of the Fourth Amendment's particularity requirement, represents a substantive legal judgment.

The proposed amendment's unprecedented allowance for situations where notice may not reach the target, in the context of case law that has never provided any exception to the rule that notice must be served, is a substantive legal judgment.

The proposed amendment's authorization of remote access searches without requiring satisfaction of the *Berger/Torres* particularity requirements, contrary to the one published decision finding that those requirements do apply, is a substantive legal judgment. So too would it be a substantive legal judgment for the Committee to include those requirements, which just further demonstrates how the substantive and procedural questions on this issue are inextricably intertwined.

Ultimately, such substantive expansions of the government's authority as those represented in this proposed amendment are not the province of this Committee. We therefore urge that this Committee reject the proposed amendment to Rule 41 and leave these substantive constitutional and policy questions where they belong, in the courts and in Congress.

Thank you for your consideration, and I welcome your questions.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8f8k-obj
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0012](#)

Comment from Steven Bellovin, Matt Blaze and Susan Landau, NA

Submitter Information

Name: Steven Bellovin

Organization: NA

General Comment

See attached file(s)

Attachments

rsearch

Comments on Proposed Remote Search Rules

Steven M. Bellovin
Columbia University*

Matt Blaze
University of Pennsylvania*

Susan Landau
Worcester Polytechnic Institute*

Thank you for the opportunity to submit comments on the proposed amendments to the Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure¹ rules for remote search. We are focusing our comments on the suggested changes to Rule 41, and in particular to the discussion of remote search. While we do not oppose the concept in principle, it poses a number of very serious concerns that must be resolved first. Above all, it should be the subject of sustained public discussion, and should most likely be authorized by specific legislation.

The three of us are technologists, and we address the topic initially from a technological perspective. We note, however, that our research has long focused on the intersection between technology and public policy. We have previously published law review articles, including one paper relevant to this discussion.² The issues we discuss include jurisdiction, chain of custody and authenticity of evidence, specificity of search, and notice.

Searches of Victim Computers

Botnets, a collection of compromised computers that are controlled by a “command-and-control” system, pose a complex challenge to law enforcement. First, they are large; they can range in size from several thousand to well over a million “bots,” the name for victims’ machines that have been taken over to perform tasks determined by the “botmaster,” or command-and-control system. The challenge is two-fold: a botnet can be very large, and the machines taken over are *victims’* devices.

It is precisely the multiplicity of the victims that encourages law enforcement to seek a single warrant approach, but this approach must be avoided. It is legally and technically dangerous to use a “common scheme to infect the victim computers with malware.”³

From a technical standpoint, the danger is that such a common scheme may easily go out of control. Current botnet technology is simple: the malware is virtually the same on all victims’ machines, and thus it is easy to know where to find out and how to disable it. *There is no technical reason why, in future, botnet malware may not be far more sophisticated.* In particular, botnet malware could be configured in a multiple of different ways that would not necessarily be easily predictable. What this means is that the “common scheme to infect the victim computers with malware” may fail, and not simply fail by not working. Such a scheme could easily fail by damaging the victims computers in unpredictable and unexpected ways. As we know from such examples as Stuxnet, malware downloaded on victims’ machines must be carefully tailored

*Affiliation listed for identification purposes only.

¹Committee on Rules of Practice and Procedure of the Judicial Conference of the United States. *Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure*. Aug. 2014. URL: <http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf> (henceforth cited as Preliminary Draft).

²See Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. “Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet”. In: *Northwestern Journal of Technology & Intellectual Property* 12.1 (2014). URL: <http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1/>.

³See *Preliminary Draft* at 325.

to the device.⁴ This is both to prevent the malware from damaging other parts of the victims computer (important for the uses being prescribed in the change to Rule 41) and also to prevent the malware from causing damage should it escape the victim’s computer.

From a legal standpoint, the lack of specificity is highly problematic. As noted in the paragraph above, currently botnet command-and-control malware is typically found in only a few places on a victim’s machine. *There is no theoretical reason why this should be so.* What that means is that a technically sophisticated criminal could hide data in victims’ machines in different places on their machines. If furthermore, the botnet information were to be encrypted—and thus not visible in plain sight—the resulting search would be essentially indistinguishable from a general warrant.

For these two sets of reasons, we strongly urge you to reject the multiple-victims-one-search-warrant approach, which we find exceedingly dangerous.

Location and Jurisdiction

One very crucial issue is the location of the target computer and hence jurisdiction. Apart from the legal issue of determining from which judicial district a valid warrant may be issued, finding the location of an arbitrary computer is not an easy task, even if its IP address is known.⁵

This is a serious concern. This must be addressed because of the uncertainty caused by *In re Warrant*.⁶

There are certainly times when ascertaining location is extremely difficult or impossible. Tor (“The Onion Router”) is designed to provide strong guarantees of anonymity; finding Tor nodes without remote search is difficult at best.⁷ Open standards and procedures for making location determination are essential. The proposed rule is problematic, though. (b)(6)(A) provides that any magistrate in a district affected may issue a warrant if “the district where the media or information is located has been concealed through technological means.” This does not deal well with situations where location is not readily nor not correctly ascertainable even though the subject has not taken any steps to “conceal” location. For example, some of us regularly use Virtual Private Networks (VPNs) to our campuses, not to conceal our location or identity but because public and hotel networks are notoriously insecure;⁸ indeed, even some cellular network providers are known to tamper with web traffic.⁹ What should happen to the fruits of a search in event of erroneous location determination is a purely legal issue that we are not qualified to opine on; we nevertheless note that such outcomes are not at all improbable, even when no concealment has been attempted. We also note the ‘forum-shopping’ issues raised by Professor Orin Kerr regarding the transformation of physical searches into remote ones.¹⁰

In a minor vein, we note that the current text of Rule 41 requires that warrants generally be executed during “daytime” in the subject’s local timezone.¹¹ Obviously, if a location is incorrect, the timezone may

⁴See Nicolas Falliere, Liam O Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Symantec Security Response. Version 1.4. Feb. 2011. URL: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

⁵There is a technology known as “IP geolocation” which maps an IP address to a location. Accuracy of geolocation mechanisms vary; they are at their least accurate when dealing with smartphones. One of us has seen a situation where a phone located in Singapore was identified as being in Kuwait. Apparently, the geolocation mechanism being used relied on the registration address of the cellular company.

⁶*In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013)

⁷See <https://www.torproject.org/>.

⁸See e.g., Maurits Martijn. “Maybe Better If You Don’t Read This Story on Public WiFi”. In: *Medium* (Oct. 15, 2014). URL: <https://medium.com/matter/heres-why-public-wifi-is-a-public-health-hazard-dd5b8dcb55e6>.

⁹See e.g., David Kravets. “Comcast Wi-Fi Serving Self-Promotional Ads via JavaScript Injection”. In: *Ars Technica* (Sept. 8, 2014). URL: <http://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/> and Robert Lemos. “Verizon Wireless injects identifiers that link its users to Web requests”. In: *Ars Technica* (Oct. 24, 2014). URL: <http://arstechnica.com/security/2014/10/verizon-wireless-injects-identifiers-link-its-users-to-web-requests/>.

¹⁰Orin Kerr, Memo to Members of the Rule 41 Committee, February 8, 2014, as cited in *Advisory Committee on Criminal Rules*, New Orleans, LA, April 7–8, 2014, at 251–252, Advisory Committee on Criminal Rules

¹¹*Federal Rules of Criminal Procedure* Rule 41(e)(2)(A)(ii).

be incorrect as well. Presumably, this would be dealt with by an explicit exemption in the warrant itself, as is permitted by the current rules.

The fact that a target machine may be abroad makes this even more critical. While US law may permit such searches, the law of the host country almost certainly does not. Coordination with other signatories to a mutual legal assistance treaty (MLAT) is essential;¹² in particular, law enforcement must be sure that American criteria for remote access are valid abroad. Some countries, in fact, prohibit such activity. Russia has charged an FBI agent with hacking for a remote search; the German courts have held that their constitution prohibits remote search entirely.¹³ It is not clear that these issues have been properly considered in promulgating the proposed rule.

Danger and Intrusiveness

One fact that every working computer programmer or system administrator learns early on is that software often fails. This is especially true of patches or modifications to existing code. To give just one example, a recent release of iOS broke the ability of some iPhones to make calls.¹⁴ The key word is “some”: Apple presumably tested the iOS 8.0.1 update before shipping it, but on *some* machines it had serious side-effects.

There are many reasons for this difficulty, but one is that every computer is different. They all have different software or different usage patterns or a different network environment. This means that testing *cannot* be comprehensive; there will *always* be some situation that will occur on deployed code that was never tried in the test lab. Therein lies danger: all too often, an unsuspected failure can occur.

Remote search software is not immune. In fact, given some of its characteristics—it must run as a privileged (“root” or “administrator”) program, in order to hide and to override file protections and examine hidden parts of the machine—it is more likely to cause unanticipated problems. Furthermore, errors in privileged programs can cause more damage; the same privileges that let them read protected files will also let them overwrite or delete files.

Two incidents widely attributed to intelligence agencies illustrate this point. In the “Athens Affair”, someone subverted the lawful intercept mechanism on a mobile phone switch operated by Vodaphone Greece.¹⁵ Over a period of ten months, about a hundred phones were tapped, including the Prime Minister’s. The penetration was detected because a programming error by the intruder caused a switch malfunction: text messages weren’t being delivered properly. It is quite striking (and not at all surprising to the technical community) that the flaw affected a part of the switch not directly involved in the tap.

A second case is the Stuxnet attack on the Iranian nuclear centrifuge plant in Natanz.¹⁶ The direct impact on the centrifuges was not noticed; however, some of the PCs were behaving so suspiciously that one was sent to a security firm in Belarus for examination. This company found the attack software.

We are certainly not asserting that remote search software will always fail, or even that it will do so most of the time. However, if it is used on enough machines, e.g., when doing a large-scale search of bots, there almost certainly will be problems on some of them. Apart from the ethical issue of causing further damage to victims’ computers, too much interference with their operation might render the search invalid. In one case,¹⁷ the 9th Circuit held that turning a car’s telecommunications system into a remote bug violated the requirement in 18 U.S.C. §2518(4) for a “minimum of interference with the services.” While this holding, pertaining to wiretap law, was based on statutory language, and was highly fact-specific, it does suggest

¹²Microsoft has stressed the need for proceeding according to an MLAT with Ireland; See Document 15, Case 1:13-mj-02814-UA, filed June 6, 2014, U.S. District Court for the Southern District of New York. <https://www.documentcloud.org/documents/1184809-brief-in-microsoft-case-to-search-email-outside.html>

¹³See Susan W. Brenner. “Law, Dissonance, and Remote Computer Searches”. In: *North Carolina Journal of Law and Technology* 14 (Fall 2012–2013), pp. 43–92.

¹⁴See Andrew Cunningham. “iOS 8.0.1 disabling cellular and TouchID on some phones”. In: *Ars Technica* (Sept. 24, 2014). URL: <http://arstechnica.com/apple/2014/09/apple-releases-ios-8-0-1-with-healthkit-keyboard-iphone-6-fixes/>.

¹⁵See Vassilis Prevelakis and Diomidis Spinellis. “The Athens Affair”. In: *IEEE Spectrum* 44.7 (July 2007), pp. 26–33. URL: <http://spectrum.ieee.org/telecom/security/the-athens-affair/0>.

¹⁶See *W32.Stuxnet Dossier*, footnote 4, *supra*.

¹⁷See *Company v. United States*, 349 F.3d 1132 (9th Cir. 2002)

that there is a threshold of interference beyond which law enforcement should not normally go. The rules for executing search warrants are also intended to minimize excess interference with the subject's normal life; consider the the normal restriction to daytime execution.¹⁸ Searches that have a significant chance of causing damage to victims' computers is an even larger problem.

Discussion of Techniques

Surreptitious collection of evidence by compromising computers (and computerized devices such as mobile telephones) is an inherently technical endeavor, involving the use of methods that will vary widely depending on the particular hardware and software used by the target. Over time, these techniques will change to adapt to new target devices and to circumvent new countermeasures. In practice, we would expect these tools to be constantly evolving, often quite rapidly.

It is natural to expect law enforcement and prosecutors to resist disclosing the specific tools and techniques they use to obtain access to their targets, citing the desirability of preserving sensitive "sources and methods" that might be used against other targets in the future. However, this goal must be balanced against a number of other risks, whose significance may not be immediately apparent to a non-technically trained judge.

First, it is imperative that any judge or magistrate authorizing a technical computer intrusion understand certain aspects of the specific technology that will be used to conduct the intrusion. This is necessary in order to meaningfully analyze the scope of the intrusion (what other information besides the evidence being sought will be exposed) and the risks that the technique to be employed might exceed the scope of the authorization. This is particularly important when, as is often the case, the target's device is used for real-time communication (with content covered by the wiretap statutes) as well as for processing and storing information.

A defendant, similarly, will often require detailed technical information about how an intrusion was conducted in order to raise challenges as to whether a search improperly exceeded its authorization. Forensic examination of a possibly-hostile computer is difficult,¹⁹ and software bugs in the examination process can affect the results. We note that the Federal Rules of Evidence state that "But the expert may be required to disclose those facts or data on cross-examination."²⁰ Similarly, expert testimony must be "the product of reliable principles and methods."²¹ It is impossible to meet these conditions without disclosing the tools that extracted that data and making them available to the defense for examination.

The techniques used to obtain access to a computer can also have bearing on the authenticity, provenance, and context of the evidence collected. For example, it is possible that, depending the technical details, that a law enforcement intrusion could expose the target's computer (and any evidence collected from it) to tampering by others. Such claims can only be raised by the defense (or refuted) through analysis, possibly involving expert testimony, of the specific tools and techniques used. Other fields of forensic examination have been plagued by bad science;²² the best assurance of quality is the adversarial process.

For these reasons, it is imperative that as much information as possible about the technology used to conduct a remote search be disclosed to the judge authorizing the search as well as to the defense in any case in which such evidence is used.

Chain of Custody and Authenticity of Evidence

It is much harder to maintain the integrity of evidence during a remote search than in a normal search done on a physically seized computer. Normal forensic procedures require that all analysis be done on a copy of

¹⁸ *Federal Rules of Criminal Procedure* Rule 41(e)(2)(A)(ii). 41(a)(2)(B) defines "daytime".

¹⁹ See Gary C. Kessler. "Anti-Forensics and the Digital Investigator". In: *Australian Digital Forensics Conference*. 2007. URL: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1000&context=adf>.

²⁰ *Federal Rules of Evidence* §705.

²¹ *Id.*, §702(c).

²² See e.g., Jane Campbell Moriarty and Michael J. Saks. "Forensic Science: Grand Goals, Tragic Flaws, and Judicial Gatekeeping". In: *Judges Journal* 44 (2005), pp. 16–33.

a seized disk. Kerr describes the process well.²³

To ensure the evidentiary integrity of the original evidence, the computer forensics process always begins with the creation of a perfect “bitstream” copy or “image” of the original storage device saved as a “read only” file. All analysis is performed on the bitstream copy instead of the original. The actual search occurs on the government’s computer, not the defendant’s.

A bitstream copy is different from the kind of copy users normally make when copying individual files from one computer to another. A normal copy duplicates only the identified file, but the bitstream copy duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original. Whereas casual users make copies of files when their machines are running, analysts generally create bitstream copies using special software after the computer has been powered down. The bitstream copy can then be saved as a “read only” file so that analysis of the copy will not alter it.

The accuracy of the bitstream copy often is confirmed using something called a “one way hash function,” or, more simply, a “hash.” A hash is a complicated mathematical operation, performed by a computer on a string of data, that can be used to determine whether two files are identical. If two nonidentical files are inputted into the hash program, the computer will output different results. If the two identical files are inputted, however, the hash function will generate identical output. Forensic analysts can use these principles to confirm that the original hard drive and the bitstream copies are identical.

There are a number of very important points in this excerpt. First, proper handling procedure for evidence requires that an “image copy” be made of the target disk. One reason for doing an analysis on a read-only image copy is that normal mechanisms for examining files change some of the metadata. Figure 1 is an example taken from one author’s Mac computer while composing this submission: note the column labeled “Date Last Opened”. Simply displaying a file will change that value.

Kerr notes that image copies also include the “slack space”—the free space—on the disk. This is very important for forensic analysis: when a file is deleted, its data is generally *not* overwritten; rather, the disk blocks are simply returned to the list of free storage. Indeed, information can be concealed there deliberately: “Even if the agents know specific information about the files they seek, the data may be mislabeled, encrypted, stored in hidden directories, or embedded in ‘slack space’ that a simple file listing will ignore.”²⁴

Finally, Kerr notes that the image file and the original device should be “hashed” to ensure that the two are identical. Even a difference of a single bit will change the hash output. It is not possible to calculate a useful hash of a disk drive that is booted, even if the computer is idle; there are too many hard-to-notice changes occurring because of normal operating system activities.

All of this is important for evidentiary reasons. If a defendant challenges the authenticity of prosecution evidence, the case is much stronger if these procedures are followed. In a recent hearing in the “Silk Road” case, precisely such challenges have been made.²⁵

Yet technology does not match needs. Simply making an image copy from a machine right next to the user can take hours. Creating such an image copy is infeasible for remote search; disks are too big and communications lines are too slow. Consider a two terabyte disk (normal on new desktop computers) and a 25M bps Internet link. Running the link flat-out, the minimum time to copy the entire drive is 640,000 seconds, more than one week. Real throughput rarely exceeds half the link speed; furthermore, latency—the

²³See Orin S. Kerr. “Searches and Seizures in a Digital World”. In: *Harvard Law Review* 119.2 (Dec. 2005), pp. 531–585. URL: <http://www.jstor.org/stable/4093493> at 540–541. Internal citations omitted.

²⁴See Office of Legal Education. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. 2009. URL: <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> at 76.

²⁵The case is 1:14-cr-00068-KBF, U.S. District Court for the Southern District of New York. The judge did not rule on the merits of the argument. See Brian Krebs. “Silk Road Lawyers Poke Holes in FBI’s Story”. In: *Krebs on Security* (Oct. 14, 2014). URL: <http://krebsonsecurity.com/2014/10/silk-road-lawyers-poke-holes-in-fbis-story/> for a description of the technical dispute.

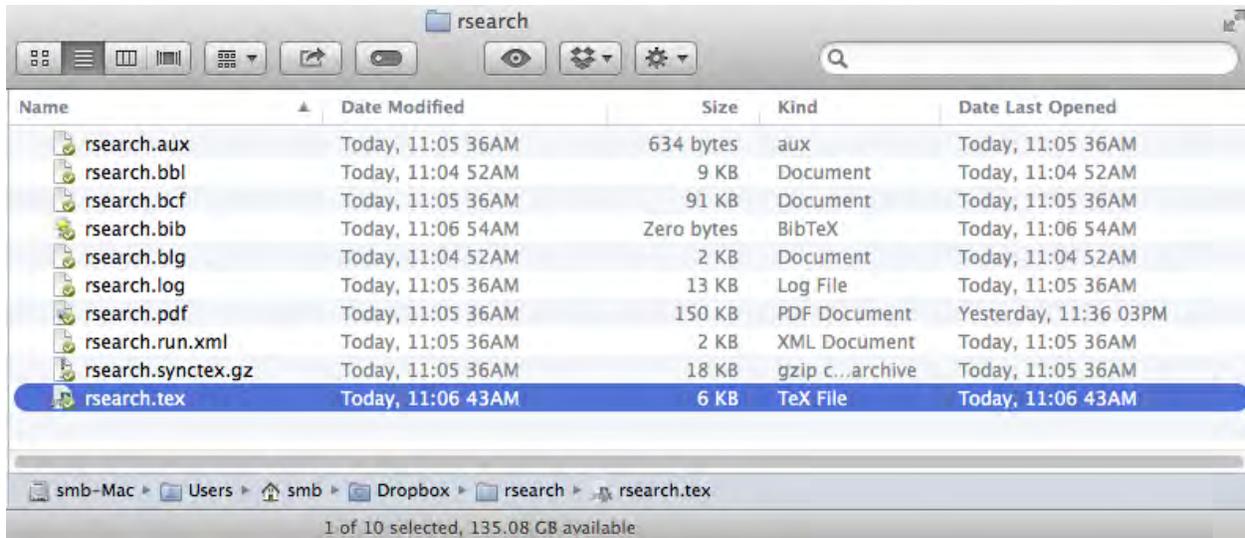


Figure 1: A screen shot noting that the last time a file is used is recorded by some operating systems.

round trip time between the source and the destination, which is limited by the speed of light—is inversely proportional to the effective bandwidth.²⁶ Copying a disk from San Francisco to Washington is inherently much slower than a similar copy from New York, simply because of the distance. The issue of the difficulty of creating an image copy has been ignored in the discussion of the proposed amendment, yet it is extremely important.

Specificity

As noted, the meaning of “specificity” for electronic searches remains the subject of continuing constitutional debate.²⁷ While we are not opining on the general question, we note that this issue becomes particularly serious when victim computers are the targets of remote search warrants. As the Preliminary Draft observed, botnets “may range in size from hundreds to millions of compromised computers”.²⁸ While no one seriously calls into question whether a police officer, taking a crime report from a victim, should act if contraband is in plain view, scale makes a difference. The situation is not a single victim, or even a pair of victims, but potentially millions of such targets. Allowing broader seizures of information from millions of machines simply because they were the victims of computer crime seems wrong. Per our comments on page 1, we suggest an explicit requirement that all remote search software be configured extremely narrowly when used on victim computers.

Because searching a victim’s computer for botnet malware exposes a non-suspect, the victim, to an unwitting search, it is particularly crucial to limit the reasons that such a search might be conducted. There would seem to be only three legitimate objectives for doing so: to demonstrate that a crime has indeed taken place (and even that is debatable, since arguably probable cause would be sufficient), to find pointers to the individual responsible for the botnet, and to ascertain the extent of the damage. We can separate this into two cases: when the behavior of the botnet is understood, and when it is not.

When dealing with known botnets, law enforcement should be able to develop a clear understanding of exactly how the malware in question works. In particular, the computer security community has had great

²⁶See the TCP bandwidth equation, given in Matthew Mathis, Jeffrey Semke, Jamshid Mahdavi, and Teunis Ott. “The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm”. In: *ACM SIGCOMM Computer Communication Review* 27.3 (1997), pp. 67–82. URL: <http://dl.acm.org/citation.cfm?id=264023> at 68. “RTT” is the round trip time.

²⁷*Preliminary Draft* at 341.

²⁸*Preliminary Draft* at 325.

success studying botnets and locating their “command and control” nodes without hacking into other victim computers. The computer security community uses so-called “honeypot” systems—machines intended to be infected, and that engage in the same sort of risky behavior as unwitting machines do—that can be instrumented and monitored.²⁹ While law enforcement needs evidence to prove guilt beyond a reasonable doubt, the use of honeypots provides a less intrusive method of investigation, and law enforcement should use this type of approach first. Even if this does not suffice, the evidence will be in a very few, easy-to-locate places. It is thus feasible to construct search software that looks precisely and solely for the necessary indicia, rather than rummaging more broadly through the computer.

The alternative situation involves a more sophisticated sort of attack, where the necessary evidence may not be in a single, easy-to-examine place. A sophisticated attacker may, for example, split a contraband file into several pieces and stash them in different places. There are techniques known that allow a file to be split in such a way that some subset of the total number of shares will suffice to reconstruct it, but no information is gained by fewer shares.³⁰ While we haven’t heard of criminals actually using such sophisticated techniques (so-called *m* out of *n* secret-sharing), it is certainly possible. That sort of scenario will likely require an examination that is less easily automated. But the complexity of the search *involving many locations on a victim’s machine* would indicate that the victim should be necessarily be informed prior to downloading malware to track the attack. Given the sophistication of the attack, and the problems that could conceivably ensue on the victim’s machine, we suspect that most victims would be happy to cooperate at ridding their own systems of the infection.

There is an alternative to searching the victims’ machines for evidence; one could instead find such evidence at the ISP used by the victims. ISPs have been experimenting with sending notices to owners whose machines appear to be infected by a botnet; the ISP uses their knowledge of the machine’s IP address to associate this with a billing address and thus an out-of-band mailing. An approach using Internet Service Providers (ISPs), discussed briefly in a paper by one of us,³¹ has the advantage that it also provides law enforcement with a better way to inform the victim of the problem. ISPs might also be used to detect infection, though this also raises privacy issues that deserve a thorough policy vetting.

We thus suggest that language mandating narrow searches, especially of victim machines, be added to the rule:

An application for a warrant issued pursuant to (b)(6)(B) must include a statement specifying precisely which data is to be seized. The warrant itself must limit the investigation to those specific facts.

To do otherwise would be to turn a phishing attack into a fishing expedition.

Notice

Search warrants generally require notice to the target, including a receipt for items seized.³² As noted in the proposal, this is problematic for remote search.³³ We feel that the problem is even more difficult than indicated.

We can think of only four feasible mechanisms for notifying the target of a search: a file left on the computer; a pop-up window; an email message; or a physical letter. All are problematic, especially for mass searches.

A file left on a computer probably won’t be noticed, but the most serious concern is that the user has no way to determine the authenticity or provenance of such a note. If such files were actually to become a

²⁹See Kirill Levchenko et al. “Click trajectories: End-to-end analysis of the spam value chain”. In: *IEEE Symposium on Security and Privacy*. IEEE. 2011, pp. 431–446. URL: <http://www.icir.org/christian/publications/2011-oakland-trajectory.pdf> for a description of a non-intrusive analysis of a bonnet.

³⁰See, e.g., Adi Shamir. “How to Share a Secret”. In: *Communications of the ACM* 22.11 (1979), pp. 612–613, for a description of how to do this with encryption keys.

³¹**Clark:2010aa**

³²*Federal Rules of Criminal Procedure* Rule 41(f)(1)(C).

³³*Preliminary Draft* at 327.

legitimate form of communication, hackers would immediately start emailing files that looked just like the real ones, except with a URL to click on “to acknowledge the message”. Naturally, these URLs would not be benign.

Email, of course, would have similar problems. The FBI itself has warned of malicious spam email purporting to be from them.³⁴ There are, at least in theory, technical solutions involving digitally signed messages and a Public Key Infrastructure. Experience with both Web browsers and phishing emails suggest that these do not work in the absence of careful training of users.

Hackers will abuse law enforcement-generated pop-up messages in similar ways. Indeed, they already have abused similar mechanisms, to serve ads.³⁵ Furthermore, there is little evidence that people would pay attention to such boxes; indeed, one online source jokingly defines a “dialog box” as “A window in which resides a button labeled ‘OK’ and a variety of text and other content that users ignore.”³⁶

Physical mail might suffice, but it will often be too time-consuming and expensive. While we do not have precise cost figures for criminal investigations, reports indicate that ISPs find such requests burdensome and charge accordingly.³⁷ Physical email is also very difficult when dealing with unknown search targets. While a more extensive search of the target computer might yield a physical address, per the discussion in the prior section such a search would be extremely intrusive.

The language in the proposed rule—“reasonable efforts”—is probably correct; given these difficulties, we do not know how it can be done. We thus suggest that the Department of Justice develop and (after suitable public comment) promulgate binding regulations for how this should be accomplished.

Remote Access and Security Mechanisms

While not directly addressed in the proposed rules, the proposal anticipates, at least implicitly, that surreptitious remote computer searches will become an increasingly prevalent law enforcement technique in the future. We agree that this is likely, and it is important that rules of evidence and criminal procedure address them. However, these methods also raise a number of policy issues that will need to be addressed by the courts and by lawmakers. We raised some of these in our recent papers on the subject,³⁸ but they bear some discussion here.

Law enforcement reliance on remote computer intrusions exposes a conflict between solving some crimes by collecting evidence and preventing other crimes by better securing computers. Virtually any vulnerability (whether due to a software flaw or an explicit “backdoor”) that can be exploited by law enforcement for investigative purposes has the potential for illicit exploitation by criminals and foreign intelligence services. And the computer software, hardware, and devices used by criminals (and from which evidence is collected) are also used by thousands—or millions—of innocent citizens to store, process, and communicate the most important and sensitive details of their lives and businesses.

³⁴ See <http://www.fbi.gov/scams-safety/e-scams>:

Ransomware Purporting to be from the FBI is Targeting OS X Mac Users

07/18/13—In May 2012, the Internet Crime Complaint Center posted an alert about the Citadel malware platform used to deliver ransomware known as Reveton. The ransomware directs victims to a drive-by download website, at which time it is installed on their computers. Ransomware is used to intimidate victims into paying a fine to “unlock” their computers. Paying the fine does nothing to solve the problem with the computer; do not follow the ransomware instructions. The ransomware has been called “FBI Ransomware” because it uses the FBI’s name. . .

Several of us have received other spam messages purporting to be from the FBI.

³⁵ Washington State Office of the Attorney General. *Pop-Up Ads*. URL: <http://www.atg.wa.gov/InternetSafety/PopUpAds.aspx>.

³⁶ <http://www.w3.org/2006/WSC/wiki/Glossary>.

³⁷ See Nate Anderson. “Big Cable fed up with endless P2P porn subpoenas”. In: *Ars Technica* (Feb. 4, 2011). URL: <http://arstechnica.com/tech-policy/2011/02/big-cable-getting-fed-up-with-endless-p2p-porn-subpoenas/> for a news story about a civil case, where plaintiffs were offered a limited number of subpoenas per month at the discounted price of \$95 apiece. For a discussion of the technical difficulties ISPs face when fielding such requests see Richard Clayton. “Anonymity and Traceability in Cyberspace”. Also published as technical report UCAM-CL-TR-653. PhD thesis. University of Cambridge, Darwin College, 2005. URL: <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html>.

³⁸ See “Lawful Hacking”, footnote 2, *supra*.

This means that that any flaw used by law enforcement for laudable evidence collection purposes also represents a risk to innocent people. As discussed above, it is natural to expect law enforcement to hold information about exploitable flaws closely, to maximize their useful lifetime for investigative use. But other public policy goals must be weighed against this. In addition to the rights of defendants to use information about these techniques to challenge evidence (discussed above), there is the broader question of reporting the vulnerabilities that law enforcement exploits to vendors so they can be fixed.³⁹ That is, the use of vulnerabilities for law enforcement must be balanced against the need to protect citizens from criminals who might exploit them themselves.

While we recognize that such policy questions may be beyond the scope of this particular proposal, we believe that it is imperative that they be addressed comprehensively. A piecemeal solution, such as is proposed here, is likely to leave society more vulnerable than less so. Thus any proposal to expand the use of vulnerability exploitation by law enforcement must be accompanied by a broader policy discussions of these inexorably related questions.

Recommendations

As is undoubtedly clear, we have a number of concerns with the current proposal, which does not appear to have undergone a thorough vetting from the technical side. Because we are not sure of the best way to proceed to satisfy law enforcement's needs, our recommendations are a response to the current proposal rather than a complete set of recommendations. Any proposal to change Rule 41 should satisfy the following recommendations, but there are likely to be other requirements, both technical and legal, that should be met as well.

- We recommend against the use of a single warrant to conduct multiple simultaneous searches on victims' computers. Blanket warrants cover far too many machines, without the necessary specificity; furthermore, they pose a great risk of damage to some of them.
- We recommend that when a warrant is issued for searching a victim's computer, the warrant include precise, particularized specifications of the area of the computer that is to be searched.
- Remote search carries significant risk of causing international complications. Guidance to law enforcement, and perhaps the rule itself, should stress this. Except for extremely serious cases, such searches should be done only with the cooperation of the host country.
- As noted in the proposed rules, giving notice of a search is problematic. We suggest a two-pronged approach. First, there needs to be explicit guidance to law enforcement on what mechanisms should be used and under what circumstances; the conditions when notice can be omitted should also be described. Second, the Department of Justice should engage the technical community in an effort to devise better mechanisms.

We have stated previously that we think that targeted hacking, with a search warrant and under suitable conditions, is a useful investigative tool.⁴⁰ However, such searches must be targeted, both to comply with legal requirements and to avoid some of the technical risks.

Depositing malware to investigate victims' machines is a very tricky business; it should never be attempted lightly. The current proposal, which does not pay enough attention to complex technical issues, must be substantially reworked to take this concern into account. Otherwise, law enforcement could be creating more damage than that which it is seeking to prevent, an approach that can neither be constitutional nor desired.

³⁹We discussed this issue in detail in "Lawful Hacking", footnote 2, *supra*.

⁴⁰See Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. "Going Bright: Wiretapping without Weakening Communications Infrastructure". In: *IEEE Security & Privacy* 11.1 (Jan.–Feb. 2013), pp. 62–72. ISSN: 1540-7993. DOI: 10.1109/MSP.2012.138. URL: <https://www.cs.columbia.edu/~smb/papers/GoingBright.pdf> and "Lawful Hacking", footnote 2, *supra*. The former discusses technical aspects; the latter concentrates on the legal and policy issues.

We have made recommendations on changes that should be made to the proposal, but we believe more than simple changes are required. While in this note we have identified a number of specific technical flaws with the proposed changes to Rule 41, there may be others that we have missed. In addition, for the most part, we have not addressed the many legal complexities in this proposal. So we suggest—and we have argued this at greater length earlier⁴¹—that a legislative fix would be best. There is, to our knowledge, no explicit statutory authority for law enforcement to hack into computers; given the intrusiveness and danger of such activities, there is a need for balance. The legislative process is best suited to address this.

⁴¹See “Lawful Hacking”, footnote 2, *supra*.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8fak-o6t9
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0013](#)

Comment from Nathan Wessler, on behalf of American Civil Liberties Union (10/31/14)

Submitter Information

Name: Nathan Wessler

Organization: American Civil Liberties Union

General Comment

See attached file.

Attachments

ACLU Second Comment on Rule 41 Proposal 103114



MEMORANDUM

To: Members of the Advisory Committee on Criminal Rules
From: American Civil Liberties Union
Date: October 31, 2014
**Re: Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning
“Remote Access” Searches of Electronic Storage Media**

Dear Members of the Committee,

The American Civil Liberties Union submits these comments to aid the Committee’s consideration of the proposed amendment to Rule 41 concerning “remote access” searches of computers and other electronic devices. The amendment was proposed by the Department of Justice last year, and modified by the Committee at its April 2014 meeting.¹

We appreciate the careful scrutiny that the Committee has given to the proposed amendment so far and, in particular, the changes made during the Committee’s April 2014 meeting. By narrowing the proposed circumstances in which warrants for remote access searches may be sought, the Committee addressed many of the problems identified by the ACLU in the original proposal.

Nonetheless, we continue to have serious concerns about the breadth of the proposed amendment, and we urge the Committee to reject the proposal in full.

This comment raises questions about the first prong of the proposal, which would permit law enforcement agencies to remotely install surveillance software on a target’s computer if “the district where the media or information is located has been concealed through technological means.”² Although the second prong of the proposal, which the government has argued is necessary for botnet investigations,³ also raises serious questions, the ACLU leaves it to others to flesh out those questions.⁴

¹ See generally Advisory Comm. on Criminal Rules, Materials for April 7–8, 2014 Meeting 155–266 (“Advisory Committee Materials”), available at

<http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf>

² Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure: Request for Comment 338 (Aug. 2014) (“Proposed Amendments Materials”), available at <http://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0001>.

³ See Advisory Committee Materials at 172.

⁴ Given the technical complexity associated with the botnets, we recommend that the committee solicit input from botnet experts from both academia and industry.

This comment begins by describing the technological means by which law enforcement agencies will likely carry out the “remote access searches” that would be authorized by the proposed amendment, and the computer security and policy concerns raised by such operations. It then explains that the proposal does not merely regulate procedure, but in fact affects substantive rights and substantively expands the government’s investigative power. Finally, it argues that the substantive authority sought by the government through its proposal raises serious constitutional questions. On the basis of these serious policy and constitutional questions, the ACLU recommends that the Committee reject the proposal as going beyond the scope of the Rules’ limited purpose and defer to Congress to address this issue in the first instance.

We very much appreciate the Committee’s consideration of this comment and look forward to discussing our concerns with the Committee during the upcoming public meeting.

I. The Means Available to the Government to Conduct “Remote Access” Searches

The proposed amendment to Rule 41 would allow a magistrate judge to issue a warrant authorizing law enforcement “to use remote access to search electronic storage media and to seize or copy electronically stored information.”⁵ Neither the proposed amendment nor the proposed committee note define “remote access.” Submissions from the Department of Justice to the Subcommittee on Rule 41 provide some description of what is meant by “remote access” and how such searches might be carried out, but crucial details remain missing.⁶ In order for the Committee to make an informed assessment of the implications of the proposed amendment, we begin this comment with a detailed explanation of what the government means by “remote access” search, how such surveillance is carried out, and why authorizing use of these techniques raises serious technological and policy concerns.

A. Federal law enforcement agencies have used malware for nearly fifteen years.

Since at least 2001, federal law enforcement agencies have used sophisticated surveillance software as part of criminal and national security investigations.⁷ This software, whether delivered through trickery, by hacking into the computers of targets,⁸ or through other covert techniques, permits agents to track and locate the computers and mobile devices of targets, as well as access private information stored on them.

⁵ Proposed Amendments Materials at 338.

⁶ See generally Advisory Committee Materials at 179–235.

⁷ See *FBI Sheds Light on 'Magic Lantern' PC Virus*, Reuters, Dec. 13, 2001, <http://usatoday30.usatoday.com/life/cyber/tech/2001/12/13/magic-lantern.htm>.

⁸ The Department of Justice has stressed that it is merely engaging in remote computer searches, not “hacking.” See Advisory Committee Materials at 245. However, internal FBI emails use the terms “penetration” and “exploit” when describing the CIPAV software, which, like hacking, are both terms of art from the computer security community. See Email from [redacted] (OTD) (FBI) to [redacted] (OTD) (FBI) et al. (June 20, 2007), available at <https://www.eff.org/document/fbicpav-08pdf>, p. 50; Email from [redacted] (OGC) (FBI) to [redacted] (SL) (FBI) (Nov. 20, 2008), available at <https://www.eff.org/document/fbicpav-08pdf> at p. 154. Using the term “hacking” is descriptively accurate.

In 2001, journalists revealed that the FBI had developed a software suite capable of covertly accessing information stored on suspects' computers.⁹ In the initial media reports revealing the existence of the FBI's *Magic Lantern* tool, a spokesperson for the FBI described it as a "a workbench project" that had not yet been deployed. One year later, in a then-classified memo, a DOJ prosecutor wrote that the tool, later renamed the Computer and Internet Protocol Address Verifier (CIPAV), had already entered regular use, and was "being used needlessly by some agencies."¹⁰

Although the existence of this tool was first revealed by the press in 2001, it was not until 2007 that journalists discovered a case in which it had been used.¹¹ Indeed, although the FBI has employed similar surveillance software for nearly fifteen years, only a handful of cases have come to the public's attention. This is, we believe, due to a concerted policy by the FBI of keeping everything about its use of this technology out of the public eye.¹² For now, the only law enforcement agency known to use malware¹³ is the FBI. However, it is likely that other federal, state and local law enforcement agencies have also acquired hacking software.¹⁴

⁹ *FBI Sheds Light on 'Magic Lantern' PC Virus*, Reuters, *supra*.

¹⁰ See Memorandum from [redacted] to CTCs 1 (Mar. 7, 2002), available at <https://www.eff.org/document/fbicipav-05pdf>.

¹¹ See Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, Wired (July 18, 2007), http://archive.wired.com/politics/law/news/2007/07/fbi_spyware?currentPage=all ("The court filing offers the first public glimpse into the bureau's long-suspected spyware capability, in which the FBI adopts techniques more common to online criminals.").

¹² See Email from [redacted], Unit Chief, FBI Cryptologic and Electronic Analysis Unit to [redacted] (SE) (FBI) (July 18, 2007), available at <https://www.eff.org/document/fbicipav-08pdf> at p.10 ("[W]e try to make every effort possible to protect the FBI's sensitive tools and techniques...we want to ensure that the capabilities of the CIPAV are minimized [in future media reports], if discussed at all. This and many tools deployed by the FBI are law enforcement sensitive and, as such, we request that as little information as possible be provided to as few individuals as possible."); see also Email from [redacted] (OTD) to [redacted] (OTD) (CON) et al. (Aug. 15, 2004), available at https://www.eff.org/files/filenode/cipav/fbi_cipav-07.pdf at p.11 ("We never discuss how we collect the [information about a target computer obtained by the CIPAV software] in the warrants/affidavits or with case agents, AUSAs, squad supervisors, outside agencies, etc.").

¹³ "Malware" and "spyware" are terms of art in the computer security community that describe software used to covertly gain access to and extract information from the computers of targets. See *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1171 (9th Cir. 2009) (describing "malicious software, known as 'malware,' that can compromise the security and functionality of a computer"); see also Morgan Marquis-Boire et al., *Police Story: Hacking Team's Government Surveillance Malware*, Citizen Lab (July 24, 2014), <https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/> (describing the capabilities of a malware tool sold by a commercial surveillance company to law enforcement and intelligence agency customers around the world); *Worldwide Threat Assessment of the US Intelligence Community: Hearing on Global Security Threats and Intelligence Operations Before the S. Select Comm. on Intelligence*, 113th Cong. 3 (2013) (statement of James Clapper, Director of National Intelligence), available at <http://intelligence.senate.gov/130312/clapper.pdf> ("[A] handful of commercial companies sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products.").

¹⁴ See Cora Currier & Morgan Marquis-Boire, *Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide*, Intercept (Oct. 30, 2014), <https://firstlook.org/theintercept/2014/10/30/hacking-team/> ("Hacking Team's efforts include a visible push into the U.S. . . . The company has made at least some sales to American entities . . ."); Kade Crockford, *Spy Tech Secretly Embeds Itself in Phones, Monitors and Operates Them from Afar*, PrivacySOS (Aug. 18, 2012), <https://www.privacysos.org/node/789> (describing the capabilities of mobile malware sold by a Virginia-based company, Oceans' Edge, which has apparently sold its software to both the FBI and DEA).

B. Capabilities of the FBI's surveillance software

Like much of the commercially available 'lawful interception' malware sold by surveillance companies to governments around the world, it appears that the FBI's malware tools have a number of capabilities that can be customized for the particular operation, depending on what features are needed, and what the magistrate judge has approved.

In one of the more basic modes of operation, for example, the software can collect the IP address of the targeted computer. This is particularly useful when the target is using an anonymizing proxy, which hides his or her IP address.¹⁵ With an IP address, agents can subpoena subscriber information from the Internet Service Provider responsible for that IP address, and then search the home or business where the targeted computer is believed to be located.

In another mode of operation, the software can collect a long list of information about a target computer, including, but not limited to: IP address; MAC address (identifying the WiFi or Ethernet card); a list of running programs; the operating system type, version and serial number; the default internet browser and version; the registered user of the operating system, and registered company name, if any; the current logged-in user name; and the address of the last website visited in the user's web browser.¹⁶

If a more thorough search of the computer is required, the FBI has software capable of searching a target's computer to obtain "records of Internet activity, including firewall logs, caches, browser history and cookies, 'bookmarked' or 'favorite' Web pages, search terms that the user entered into any Internet search engine, and records of user-typed Web addresses," as well as "saved user names and passwords, documents, browsing history, user profiles, e-mail contents, e-mail contacts, chat messaging logs, photographs, and correspondence."¹⁷

In addition to the ability to access essentially any data already stored on the target's computer, the FBI also has the ability to remotely access and enable the GPS chip, microphone, or webcam in a target's computer or mobile device.¹⁸ As such, the FBI has the capability to

¹⁵ See Application for a Search Warrant at 40, *In re Search of Computers that Access the Website "Bulletin Board A"*, No. 8:12-MJ-356 (D. Neb. Nov. 16, 2012), available at <http://www.documentcloud.org/documents/1261620-torpedo-affidavit.html> (listing the types of information to be obtained by the Network Investigative Technique, including the "activating" computer's IP address and information about the operating system software running on the computer).

¹⁶ Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, *supra*.

¹⁷ See *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 755-56 (S.D. Tex. 2013).

¹⁸ See *id.* at 3; see also Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, Wall St. J., Aug. 3, 2013, <http://online.wsj.com/articles/SB10001424127887323997004578641993388259674> ("[T]he bureau can remotely activate the microphones in phones running Google Inc.'s Android software to record conversations, one former U.S. official said. It can do the same to microphones in laptops without the user knowing, the person said."); see also Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post, Dec. 6, 2013, http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html ("The FBI has been able to covertly activate a computer's camera — without triggering

generate location information, to capture audio through the microphone, and to capture photographs or videos using the target's webcam. According to an ex-senior FBI official, the FBI even has the capability to disable a webcam's indicator light, so that there will be no way of knowing that the camera is recording.¹⁹

C. Methods for infecting the computers of targets with malware

There are several ways in which agents can deliver malicious software to the computer or mobile device of a target. We introduce several of the most popular methods here. This is by no means an exhaustive list, as law enforcement and intelligence agencies can be extremely creative in their efforts to surveil targets and covertly bug computers and mobile devices.

i. Social engineering

In a social engineering operation, agents will send an email or other communication to a target, with the goal of convincing the target to take a particular action, such as clicking on a link in the message, or opening an attachment.²⁰ Such operations almost always involve some degree of deception, as targets are unlikely to perform the desired action if it is clear from the sender information (i.e., the "From" line of an email) that it is from a law enforcement agency. As a result, agents engaging in such operations are likely to impersonate third parties, such as the target's associates,²¹ or organizations known to the target. For example, in 2007, FBI agents successfully delivered CIPAV surveillance software by sending a link to a fake Associated Press article, created by agents for that investigation, to the target of the operation.²² Presumably, as soon as the target clicked on the link to the article, the CIPAV was delivered to his computer. The FBI likely exploited a security vulnerability in his web browser to deliver the CIPAV software.

The success of this operation depends on being able to trick the target into taking the desired action. For sophisticated targets, particularly those with expertise in computer security, this may be difficult.

the light that lets users know it is recording — for several years, and has used that technique mainly in terrorism cases or the most serious criminal investigations, said Marcus Thomas, former assistant director of the FBI's Operational Technology Division in Quantico.”).

¹⁹ See Timberg & Nakashima, *FBI's Search for 'Mo,' Suspect, supra*.

²⁰ See Jennifer Valentino-DeVries & Danny Yadron, *supra* (“Officers often install surveillance tools on computers remotely, using a document or link that loads software when the person clicks or views it.”).

²¹ See T. N. Jagatic et al., *Social Phishing*, Comm. of the ACM, Oct. 2007, at 94, available at <http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf> (demonstrating that phishing attacks which impersonate a friend of the target are more successful than those in which the sender is not known to the target).

²² See Ellen Nakashima & Paul Farhi, *FBI Lured Suspect with Fake Web Page, but May Have Leveraged Media Credibility*, Wash. Post, Oct. 28, 2014, http://www.washingtonpost.com/world/national-security/fbi-lured-suspect-with-fake-web-page-but-may-have-leveraged-media-credibility/2014/10/28/e6a9ac94-5ed0-11e4-91f7-5d89b5e8c251_story.html.

ii. Surreptitious entry

The FBI has a long, controversial history of secretly breaking into the homes or offices of targets and installing covert recording devices.²³ Surreptitious entry operations, commonly known as *black bag jobs*, are also used to install surveillance software and hardware on the computers of targets.²⁴ The earliest publicly known example of a black bag job was in 1999.²⁵ These operations of course require that agents know the physical location of the target.

iii. Watering hole attacks

Agents wishing to install surveillance software onto the computers of many individuals who all share a common interest or association may decide to perform a so called *watering hole attack*. In such operations, agents will install custom code on a website popular with the target group, which will infect the computers of everyone who visits the site. This technique has been repeatedly used by the FBI,²⁶ as well as by foreign state actors.²⁷ When this technique is used, agents may not know the identity of a particular target or targets, and may in fact not know ahead of time the identities of *any* of the targets whose computers will be eventually be compromised.

iv. Third-party service provider-aided delivery of surveillance software

By enlisting the assistance of third-party service providers, such as telecommunications and internet service providers, agents can leverage the trusted access that such providers have to a target's communications and, in some cases, their computers or mobile devices.

In a *man in the middle* attack, surveillance software can be delivered, typically with special-purpose surveillance hardware installed in an internet provider's data center (and thus, with the assistance of that company), by intercepting requests from a target's computer to access internet content, impersonating the server the target is attempting to connect to, and then sending

²³ See, e.g., FBI Records: The Vault, Surreptitious Entries (Black Bag Jobs), [http://vault.fbi.gov/Surreptitious%20Entries%20\(Black%20Bag%20Jobs\)%20](http://vault.fbi.gov/Surreptitious%20Entries%20(Black%20Bag%20Jobs)%20); Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Final Report: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans 355 (1976), available at <https://web.archive.org/web/20070414214706/http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIII.htm>.

²⁴ See Valentino-DeVries & Yadron, *supra* (“In some cases, the government has secretly gained physical access to suspects' machines and installed malicious software using a thumb drive, a former U.S. official said.”).

²⁵ See *United States v. Scarfo*, 180 F. Supp. 2d 572, 577 (D.N.J. 2001) (“Because the encrypted file could not be accessed via traditional investigative means, [the judge's] Order permitted law enforcement officers to ‘install and leave behind software, firmware, and/or hardware equipment which will monitor the inputted data entered on [defendant's] computer in the TARGET LOCATION so that the F.B.I. can capture the password necessary to decrypt computer files by recording the key related information as they are entered.’”).

²⁶ See Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, *Wired* (Aug. 5, 2014), http://www.wired.com/2014/08/operation_torpedo/; see also Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, *Wired* (Sept. 13, 2013), <http://www.wired.com/2013/09/freedom-hosting-fbi/>.

²⁷ See Michael Mimoso, *Council on Foreign Relations Website Hit by Watering Hole Attack, IE Zero-Day Exploit*, *Threatpost* (Dec. 29, 2012), <http://threatpost.com/council-foreign-relations-website-hit-watering-hole-attack-ie-zero-day-exploit-122912/77352>.

malicious software back to the target instead.²⁸ This technique exploits the fact that much of the content accessed on the web is unencrypted, and thus vulnerable to tampering by third parties. There are several companies that sell products designed to deliver surveillance software in this manner,²⁹ at least one of which has sold its products to the FBI.³⁰

Another example of third-party-company-aided delivery involves forcing a service provider to push surveillance software disguised as a security update to customers. This technique has been used by at least one foreign government, using software made by a California-based surveillance company.³¹

D. The surveillance software infection process

The process of delivering surveillance software to a target's computer or mobile device generally consists of a number of different steps. In order to understand the important public policy and legal issues associated with the use of this surveillance technique, it is necessary to first understand the way in which this software is delivered to targets.

Step 1: Reconnaissance

In this step, agents determine a *selector* that can identify each target. For individual targets, this might be an email address, username, telephone number or IP address. For watering hole attacks, the agents will identify the website or server that will be used. If agents plan to infect the target device in-person, through a black bag job, then they must locate the home, office or hotel room where the target's computer or mobile device will be.

Step 2: Attack setup

In this step, agents create the phishing email, prepare the code that will be added to the webpage that the user will visit, or customize the surveillance software that will subsequently be delivered and run on the target's device.

Step 3: Delivery / Acquisition

²⁸ See Barton Gellman, *U.S. Firm Helped the Spyware Industry Build a Potent Digital Weapon for Sale Overseas*, Wash. Post, Aug. 15, 2014, http://www.washingtonpost.com/world/national-security/spyware-tools-allow-buyers-to-slip-malicious-code-into-youtube-videos-microsoft-pages/2014/08/15/31c5696c-249c-11e4-8593-da634b334390_story.html (“Merely by playing a YouTube video or visiting a Microsoft Live service page, for instance, an unknown number of computers around the world have been implanted with Trojan horses by government security services that siphon their communications and files. . . . Network injection allows products built by Gamma and Hacking Team to insert themselves into an Internet data flow and change it undetectably in transit.”).

²⁹ See Ryan Singel, *Law Enforcement Appliance Subverts SSL*, Wired (Mar. 24, 2010), <http://www.wired.com/2010/03/packet-forensics/>.

³⁰ See Fed. Bus. Opportunities, Request for Quotations: Network Equipment (FBI Sept. 24, 2014), https://www.fbo.gov/index?s=opportunity&mode=form&id=bbec3296f333fa5c8f23973be4882ec7&tab=core&_cvi=0.

³¹ See John Timmer, *UAE Cellular Carrier Rolls Out Spyware as a 3G “Update”*, Ars Technica (July 23, 2009), <http://arstechnica.com/business/2009/07/mobile-carrier-rolls-out-spyware-as-a-3g-update/>.

In this step, agents deliver the government's surveillance software to the target's computer. If agents use social engineering, agents will send the previously prepared phishing message to an address known to be used by the target. In a watering hole attack, agents will insert the previously prepared code into the webpage on the site that targets will visit. If agents are engaged in a black bag job, in this step, agents will gain covert access to the house, office or hotel of the target, and locate the computer or mobile device.

Step 4: Exploitation

In this step, the exploit shellcode, a special piece of malicious software, is executed on the target's computer, bypassing or circumventing any security software or other built-in protections present in the targeted software application.³² If agents use a social engineering attack, the shellcode might be executed because the target clicks on a link in the phishing email. If a watering hole attack is used, the exploitation will take place merely when the target visits the web page that has been modified by the agents. If the agents have conducted a black bag job, the agents will install the software themselves, likely using removable media such as a USB thumb drive.

In many cases, particularly in so-called *drive by download attacks*,³³ where the target's computer is infected merely by clicking on a link or visiting a particular website, the exploitation step will typically involve the exploitation of one or more security vulnerabilities in the web browser, word processor or operating system of the target's device, *infra* Part I.C. The use of exploits enables the surveillance software to be covertly installed on the target's computer.

Step 4a: Validation (optional)

In some operations, particularly when agents may not be confident that the device they have exploited is the correct target, an optional validation step may take place, in which specific information is extracted from the infected computer in order to identify the device and its owner. Examples of such information might include, for example, the computer's IP address, the MAC address identifying the WiFi interface, and other permanent device identification numbers.

Step 5: Installation

In this step, the full surveillance software suite, or *payload*, will be downloaded and installed on the computer of the target.

Step 6: Exfiltration

³² Amit Klein, *Multi-Stage Exploit Attacks for More Effective Malware Delivery*, Trusteer Blog (May 2, 2013), <http://www.trusteer.com/blog/multi-stage-exploit-attacks-for-more-effective-malware-delivery> ("Most drive-by exploit kits use a minimal exploit shellcode that downloads and runs the final payload. This is akin to a two-stage ICBM (InterContinental Ballistic Missile) where the first stage, the exploit, puts the rocket in its trajectory and the second stage, the payload, inflicts the damage. In the cybercrime world, the de-coupling of the first stage from the payload is designed to make sure that an exploit kit is as generic as possible and can deliver all possible payloads.").

³³ Marco Cova et al., *Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code*, Proceedings of the 19th International Conference on World Wide Web (2010), *available at* http://www.site.uottawa.ca/~nelkadri/CSI5389/Papers/40-Cova_et_al_WWW2010.pdf.

In this step, the surveillance software collects the desired information on the target and then transmits that information back to a server controlled by the government. This may involve searching documents or other files on the computer, as well as activating the webcam or microphone in the device. In some operations, the surveillance software may collect the information sought, transmit it back to the government, and then erase itself from the target's computer. In other cases, where long-term surveillance is desired, the software may remain on the target's computer, collecting data, and regularly transmitting that data back to the government.

II. Technological and Policy Concerns

There are a number of serious technical and policy concerns related to the covert installation and use of surveillance software by law enforcement agencies.

A. Security flaws in surveillance software can weaken the security of the target's device and expose it to compromise by other unauthorized parties

In 2011, security researchers in Germany obtained a copy of surveillance software that the German authorities had, for two years, used to remotely monitor targets in criminal investigations. The researchers analyzed the software, and discovered that the developers of the software had made elementary programming mistakes,³⁴ the most serious of which exposed devices running the surveillance software to remote control by other, unauthorized parties.³⁵ This is not the only example of security vulnerabilities being discovered in surveillance software. Indeed, significant security flaws have repeatedly been discovered in several widely used interception and surveillance software products.³⁶

That security vulnerabilities exist in surveillance software is not surprising. All software programs have bugs, some of which may eventually be exploited by hackers. But as one leading scholar has noted, security flaws in surveillance systems can be particularly problematic, as their exploitation can lead to a catastrophic loss of communications confidentiality.³⁷ The risk of these

³⁴ See Admin, *Chaos Computer Club Analyzes Government Malware*, Chaos Computer Club (Oct. 8, 2011), <http://ccc.de/en/updates/2011/staatstrojaner> ("The analysis also revealed serious security holes that the trojan is tearing into infected systems. The screenshots and audio files it sends out are encrypted in an incompetent way, the commands from the control software to the trojan are even completely unencrypted. Neither the commands to the trojan nor its replies are authenticated or have their integrity protected. Not only can unauthorized third parties assume control of the infected system, but even attackers of mediocre skill level can connect to the authorities, claim to be a specific instance of the trojan, and upload fake data. It is even conceivable that the law enforcement agencies' IT infrastructure could be attacked through this channel. The CCC has not yet performed a penetration test on the server side of the trojan infrastructure.").

³⁵ *Id.*

³⁶ See Dan Goodin, *Root Backdoor Found in Surveillance Gear Used by Law Enforcement*, Ars Technica (May 28, 2014), <http://arstechnica.com/security/2014/05/root-backdoor-found-in-surveillance-gear-used-by-law-enforcement/>; Micah Sherr et al., *Can They Hear Me Now?: A Security Analysis of Law Enforcement Wiretaps*, CCS '09: Proceedings of the 16th ACM Conf. on Computer & Comms. Security (2009), at 512-523, available at <http://www.crypto.com/papers/calea-ccs2009.pdf>.

³⁷ Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix -- Doctrine to Follow*, 14 N.C. J. L. & Tech. 489 (2013).

flaws being exploited is not theoretical. Sophisticated state actors have hacked into communications surveillance systems and databases on multiple known occasions,³⁸ in some cases using security flaws in the surveillance software itself.³⁹

B. The US government, and the FBI in particular, do not have a strong track record of technical excellence.

If the US government had a strong track record of creating and deploying secure software, perhaps the risks associated with security flaws in government surveillance software could be ignored. Unfortunately, the government's track record is less than solid. The government's information technology (IT) procurement process is widely acknowledged to be broken, leading to the government paying far too much money for poorly written, often flawed software.⁴⁰ Examples of botched IT procurement can be found in practically every agency. High-profile instances include Healthcare.gov⁴¹ and the FBI's Sentinel case management system.⁴²

Federal government agencies have a particularly poor track record when it comes to data security. Agencies struggle with the most basic security practices, such as using good passwords, updating anti-virus software, and encrypting internet traffic on their websites.⁴³ The results are predictable: data breaches by federal agencies are now routine—there were a staggering 25,000

³⁸ See, e.g., Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair*, IEEE Spectrum (June 29, 2007), <http://spectrum.ieee.org/telecom/security/the-athens-affair> (describing how “hackers broke into a [Greek] telephone network and subverted its built-in wiretapping features for their own purposes While the hack was complex, the taps themselves were straightforward. When the [Greek] prime minister, for example, initiated or received a call on his cellphone, the exchange would establish the same kind of connection used in a lawful wiretap—a connection to a shadow number allowing it to listen in on the conversation.”); see also Ellen Nakashima, *Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, Wash. Post, May 20, 2013, http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

³⁹ See Nat'l Sec. Agency, DOCID No. 352694, *Phone Freaks Can Invade Your Privacy* (1976), available at <http://explodingthephone.com/docs/db904> (declassified NSA memo describing how interfaces used by phone company employees to determine if a line was busy were subverted by outsiders to listen to phone conversations).

⁴⁰ See, e.g., Craig Timberg & Lena H. Sun, *Some Say Health-Care Site's Problems Highlight Flawed Federal IT Policies*, Wash. Post, Oct. 9, 2013, http://www.washingtonpost.com/business/technology/some-say-health-care-sites-problems-highlight-flawed-federal-it-policies/2013/10/09/d558da42-30fe-11e3-8627-c5d7de0a046b_story.html (“[T]he root cause is not simply a matter of flawed computer code but rather the government's habit of buying outdated, costly and buggy technology. The U.S. government spends more than \$80 billion a year for information-technology services, yet the resulting systems typically take years to build and often are cumbersome when they launch.”).

⁴¹ See Amy Goldstein, *Poor Planning and Oversight Led to HealthCare.gov Flaws, GAO Finds*, Wash. Post, July 30, 2014, http://www.washingtonpost.com/national/health-science/poor-planning-and-oversight-led-to-healthcaregov-flaws/2014/07/30/2f1a04aa-1814-11e4-9e3b-7f2f110c6265_story.html.

⁴² See Evan Perez, *FBI Files Go Digital, After Years of Delays*, Wall St. J., Aug. 1, 2012, <http://online.wsj.com/articles/SB10000872396390444130304577561361556532528>.

⁴³ See Minority Staff of the Homeland Sec. & Governmental Affairs Comm., 113th Cong., *The Federal Government's Track Record on Cybersecurity and Critical Infrastructure 7* (2014), available at <http://www.hsgac.senate.gov/download/?id=8BC15BCD-4B90-4691-BDBA-C1F0584CA66A>.

data breaches reported by federal agencies in 2013.⁴⁴ Foreign governments have repeatedly penetrated federal systems,⁴⁵ with the White House's network being the latest to be breached by foreign hackers.⁴⁶

Given the extreme difficulty of writing secure software and the federal government's poor track record in securing its own systems, it is extremely likely that the surveillance software that federal law enforcement agencies deploy will not be secure and will leave the computers of targets vulnerable to compromise by other parties.

C. Law enforcement agencies will increasingly need zero-day exploits

In order to exploit a security vulnerability in the software on a target's computer, the target's computer must either be running out-of-date software with a known software vulnerability, or agents must know of a vulnerability for which no update exists. As such, targets that regularly patch their software (or use software that automatically updates) may be much harder to infect with malware.

In order to be able to successfully compromise the computers of targets with up-to-date software, law enforcement and intelligence agencies are increasingly seeking to purchase or discover so called "zero-day" (or "0-day") software exploits. Zero-day exploits are special computer code that exploits vulnerabilities in software that are not known to the manufacturer of the software program, and thus, for which no software update exists.⁴⁷ Zero day exploits are extremely valuable, because there is no defense against them.⁴⁸

U.S. law enforcement and intelligence agencies have, in recent years, increasingly turned to zero-day exploits in order to gain access to the computers of high value targets.⁴⁹ This has in

⁴⁴ Jeryl Bier, *Security Breaches of Personal Information at Federal Agencies More than Doubles Since 2009*, Wkly. Standard (Apr. 3, 2014), http://www.weeklystandard.com/blogs/security-breaches-personal-information-federal-agencies-more-doubles-2009_786450.html.

⁴⁵ See Fred Barbash, *Chinese Hackers May Have Breached the Federal Government's Personnel Office*, U.S. Officials Say, Wash. Post, July 10, 2014, <http://www.washingtonpost.com/news/morning-mix/wp/2014/07/09/report-chinese-hacked-into-the-federal-governments-personnel-office/>.

⁴⁶ See Ellen Nakashima, *Hackers Breach Some White House Computers*, Wash. Post, Oct. 28, 2014, http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html.

⁴⁷ See Leyla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*, Proceedings of the 2012 ACM Conference on Computer and Communications Security (2012), available at http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf ("A zero-day attack is a cyber attack exploiting a vulnerability that has not been disclosed publicly. There is almost no defense against a zero-day attack: while the vulnerability remains unknown, the software affected cannot be patched and anti-virus products cannot detect the attack through signature-based scanning.").

⁴⁸ *The Digital Arms Trade*, Economist, Mar. 30, 2013, <http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade> ("It is a type of software sometimes described as 'absolute power' or 'God'. Small wonder its sales are growing.").

⁴⁹ See Craig Timber & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post, Dec. 6, 2013, http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html (describing the use of a zero-day exploit by the FBI to take over webcams without the indicator light turning on); see also Liam Murchu, *Stuxnet Using Three Additional Zero-Day*

turn fueled a largely unregulated market for zero-day exploits, in which government agencies are active and are often the highest bidder.⁵⁰

Governments spend a lot of money to acquire zero-day exploits. Although there is little verifiable data about the market for such exploits, anecdotal reports suggest that the cost of commercial exploits can be in the hundreds of thousands of dollars.⁵¹ These vulnerabilities are their most effective when no one else knows about them, so rather than alerting the companies whose software can be exploited, governments, including the United States, quietly exploit them.⁵² Quite simply, governments that rely on zero-day exploits have prioritized offense over defense.

Although zero-days undoubtedly make it easier to deliver malware to targets and to gain access to difficult-to-penetrate systems, there are significant collateral costs associated with the purchase and use of zero-days by governments. That is, by exploiting these vulnerabilities rather than notifying the companies responsible for the software, governments are putting their own citizens at risk.⁵³ Several senior ex-U.S. government officials have acknowledged these risks, including ex-NSA/CIA director Michael Hayden,⁵⁴ and ex-‘cyber czars’ Howard Schmidt⁵⁵ and Richard Clarke.⁵⁶

Vulnerabilities, Symantec Official Blog (Jan. 23, 2014), <http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities> (describing the use of zero days in Stuxnet, a piece of malware attributed to the US and Israeli governments); David Sanger, *Obama Orders Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times, June 1, 2012, <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all>.

⁵⁰ See, e.g., *The Digital Arms Trade*, *supra* (“Other reputable customers, such as Western intelligence agencies, often pay higher prices. Mr Lindelauf reckons that America’s spies spend the most on exploits. . . . [B]risk sales are partly driven by demand from defence contractors that see cyberspace as a “new battle domain”, says Matt Georgy, head of technology at Endgame, a Maryland firm that sells most of its best exploits for between \$100,000 and \$200,000.”); Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times, July 13, 2013, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=1&_r=1 (“But increasingly the businesses are being outbid by countries with the goal of exploiting the flaws in pursuit of the kind of success. . . that the United States and Israel achieved. . .”); Joseph Menn, *Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback*, Reuters, May 10, 2013, <http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510> (“Even as the U.S. government confronts rival powers over widespread Internet espionage, it has become the biggest buyer in a burgeoning gray market where hackers and security firms sell tools for breaking into computers.”).

⁵¹ See Perlroth & Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, *supra* (describing hackers searching for “secret flaws in computer code that governments pay hundreds of thousands of dollars to learn about and exploit”).

⁵² Joseph Menn, *U.S. Cyberwar Strategy Stokes Fear of Blowback*, Reuters, May 10, 2013, <http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510> (“The core problem: Spy tools and cyber-weapons rely on vulnerabilities in existing software programs, and these hacks would be much less useful to the government if the flaws were exposed through public warnings. So the more the government spends on offensive techniques, the greater its interest in making sure that security holes in widely used software remain unrepaired.”).

⁵³ *Id.* (“The strategy is spurring concern in the technology industry and intelligence community that Washington is in effect encouraging hacking and failing to disclose to software companies and customers the vulnerabilities exploited by the purchased hacks.”).

⁵⁴ *Id.* (“Acknowledging the strategic trade-offs, former NSA director Michael Hayden said: ‘There has been a traditional calculus between protecting your offensive capability and strengthening your defense. It might be time now to readdress that at an important policy level, given how much we are suffering.’”).

Indeed, at a time when cyber-attacks are, according to government officials, one of the biggest threats faced by this country,⁵⁷ the collateral damage associated with exploiting, rather than fixing, security vulnerabilities is a topic of considerable debate. For example, the President's NSA Review Group observed last year that "[a] vulnerability that can be exploited on the battlefield can also be exploited elsewhere"⁵⁸ and recommended that "US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks."⁵⁹ Moreover, "in almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities—'patching' them—strengthens the security of US Government, critical infrastructure, and other computer systems."⁶⁰

Because so little is known about how the FBI currently delivers malware to surveillance targets, we have no way of knowing how frequently it uses zero-days, or how many it has purchased or otherwise acquired. Even so, as the technology industry moves steadily towards automatic security updates,⁶¹ a practice largely motivated by cybersecurity concerns, the FBI

⁵⁵ *Id.* ("It's pretty naïve to believe that with a newly discovered zero-day, you are the only one in the world that's discovered it," said Schmidt, who retired last year as the White House cybersecurity coordinator. "Whether it's another government, a researcher or someone else who sells exploits, you may have it by yourself for a few hours or for a few days, but you sure are not going to have it alone for long."); see also Perloth & Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, *supra* ("Governments are starting to say, 'In order to best protect my country, I need to find vulnerabilities in other countries,'" said Howard Schmidt, a former White House cybersecurity coordinator. "The problem is that we all fundamentally become less secure.").

⁵⁶ Menn, *U.S. Cyberwar Strategy Stokes Fear of Blowback*, *supra* ("Former White House cybersecurity advisors Howard Schmidt and Richard Clarke said in interviews that the government in this way has been putting too much emphasis on offensive capabilities that by their very nature depend on leaving U.S. business and consumers at risk. 'If the U.S. government knows of a vulnerability that can be exploited, under normal circumstances, its first obligation is to tell U.S. users,' Clarke said. 'There is supposed to be some mechanism for deciding how they use the information, for offense or defense. But there isn't.'").

⁵⁷ James Clapper, the Director of National Intelligence, and James Comey, the Director of the FBI, have both told Congress that cyber-attacks are the most serious national security threat faced by the United States. See Jim Garamone, *Clapper Places Cyber at Top of Transnational Threat List*, Armed Forces Press Service, Mar. 12, 2013, <http://www.defense.gov/news/newsarticle.aspx?id=119500>; Greg Miller, *FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered*, Wash. Post, Nov. 14, 2013, http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html ("FBI Director James B. Comey testified Thursday that the risk of cyberattacks is likely to exceed the danger posed by al-Qaeda and other terrorist networks as the top national security threat to the United States and will become the dominant focus of law enforcement and intelligence services.").

⁵⁸ Review Grp. on Intelligence and Comm'n Techs., *Liberty and Security in a Changing World* 187 (2013), available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

⁵⁹ *Id.* at 37, 219.

⁶⁰ *Id.* at 220.

⁶¹ See Ellen Messmer, *Microsoft to Start Automatic Updates of IE Without Asking the User*, Network World (Dec. 15, 2011), <http://www.networkworld.com/article/2184071/windows/microsoft-to-start-automatic-updates-of-ie-without-asking-the-user.html>; see also Gregg Keizer, *Google's Chrome Now Silently Auto-Updates Flash Player*, Computer World (Apr. 1, 2010), <http://www.computerworld.com/article/2516595/networking/google-s-chrome-now-silently-auto-updates-flash-player.html>; Thomas Duebendorfer & Stefan Frei, *Why Silent Updates Boost Security* (2009), available at <http://www.tik.ee.ethz.ch/file/ef72343372ca8659a9ae8a98873167c0/TIK-Report-302.pdf>.

may increasingly need zero-days in the future, as it will no longer be able to rely on targets running out of date, insecure software.

For example, the FBI has performed several successful watering hole attacks targeting visitors to websites that could only be accessed using Tor.⁶² In at least one of these operations, the FBI's malware was delivered with code that exploited a security vulnerability for which a fix existed, and had been included in an update to the Tor Browser Bundle software that was made available a month before the FBI's operation.⁶³ Until September of 2014, the Tor Browser Bundle did not include a built-in security update mechanism.⁶⁴ When updates were available, users had to go to the Tor Project website and download the updates for themselves. Many users did not do this, and so it is not surprising that FBI was able to successfully deliver malware to a number of Tor users without needing to exploit a zero-day vulnerability. Earlier this year, The Tor Project introduced a mechanism to more easily update the Tor browser software, and the organization has long been working on making security updates automatic.⁶⁵

The Department of Justice has told this Committee that one of the primary motivations for its proposal is the problem posed by anonymizing technologies like Tor.⁶⁶ However, once the Tor Project completes the planned automatic security update feature, the successful compromise of Tor users will require zero day security vulnerabilities. This committee should therefore understand that if it wishes to provide law enforcement agencies the ability to identify and locate Tor users, then that ability will necessarily require blessing the exploitation of zero day vulnerabilities as a law enforcement technique. This raises significant public policy concerns.

D. The tech industry's embrace of cloud computing significantly complicates watering hole attacks.

In August 2013, all of the websites hosted by Freedom Hosting—a service that hosted websites through the Tor network— began serving an error message with hidden code embedded

⁶² See Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, *supra*; Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, *supra*. "Tor 'is a network of virtual tunnels that allows people to improve their privacy and security.' Originally developed by the Naval Research Lab and subsequently funded by the Defense Advanced Research Projects Agency ('DARPA') to facilitate anonymous online activities by government personnel. Tor is an 'onion routing' technology which hides a user's IP address, making it appear to originate from a Tor server rather than the actual address from which the user is connecting to the Internet." Pell, *supra*, at 38 (citations omitted).

⁶³ See Posting of Andy Isaacson, adi@hexapodia.org, to liberationtech@lists.stanford.edu (Aug. 5, 2013) (*available at* <https://mailman.stanford.edu/pipermail/liberationtech/2013-August/010498.html>) (stating that the fix to the exploit had been included in an update to the Tor Browser Bundle released on June 26, 2013).

⁶⁴ See mikeperry, *Tor Browser 3.6.5 and 4.0-alpha-2 Are Released*, Tor Blog (Oct. 30, 2014), <https://blog.torproject.org/blog/tor-browser-365-and-40-alpha-2-are-released> (describing the new update mechanism included in the 4.0 alpha-2 release of the Tor Browser bundle).

⁶⁵ See phobos, *Google Funds an Auto-Update for Vidalia*, Tor Blog (June 6, 2008), <https://blog.torproject.org/blog/google-funds-auto-update-vidalia>; see also Tor Browser Launcher, Micah Lee's Blog, <https://micahflee.com/torbrowser-launcher/> (describing an independent effort to create an automatic Tor security update delivery mechanism).

⁶⁶ See Advisory Committee Materials at 171 ("The proposed amendment would better enable law enforcement to investigate and prosecute botnets and crimes involving Internet anonymizing technologies, both which pose substantial threats to members of the public."); *id.* at 160 ("Currently, the Department obtains remote access warrants primarily to combat Internet anonymizing techniques.").

in the page.⁶⁷ That code was specifically designed to exploit a security flaw in a version of the Firefox web browser used to access Tor hidden servers.⁶⁸ According to an FBI agent who later testified in an Irish court, the Freedom Hosting service hosted at least 100 child pornography websites.⁶⁹ But the service also hosted a number of legitimate sites, including TorMail, a web-based email service that could only be accessed over the Tor network, and the Hidden Wiki, which one news site described as the “de facto encyclopedia of the Dark Net.”⁷⁰ Even though these sites were serving lawful content, the FBI’s watering hole attack was performed in an overbroad manner, forcing all of the Freedom Hosting sites to deliver malware to visitors, not just those sites that were engaged in the distribution of illegal content.

We are now firmly in the age of cloud computing, in which hundreds of websites may share resources provided by the same powerful servers. Law-abiding Internet users have no way of knowing if the sites that they are visiting are hosted on the same physical server as a site that facilitates illegal conduct. That websites with a potential connection to illegal conduct are hosted on the same server as legitimate websites is not sufficient reason to permit law enforcement agencies to hack into the computers of every person who interacts with a particular server.

The court order that the FBI presumably obtained before launching watering hole attacks from the many Freedom Hosting websites is not public. As such, it is impossible to know what the FBI agents told the court, or what the court authorized. We do not know if the judge authorized watering hole attacks against all visitors to all sites running on the server owned by Freedom Hosting, or if the FBI agents exceeded the scope of the warrant. In any event, this episode demonstrates the importance of strict limits on bulk delivery of remote access malware, including through watering hole attacks.

III. The Proposed Amendment Substantively Expands the Government’s Powers and Should Be Addressed by Congress in the First Instance

The Federal Rules of Procedure are limited to “regulating procedure.” *Sibbach v. Wilson & Co.*, 312 U.S. 1, 10 (1941). They may not “abridge, enlarge or modify any substantive right.” 28 U.S.C. § 2072(b). Although the proposed Committee Note purports to leave “constitutional questions” to be addressed in future case law,⁷¹ in practice the amendment will enlarge the government’s substantive power to conduct searches and will decide contested questions of law *sub silentio*.

By amending Rule 41, the government seeks to obtain the power to conduct a category of searches that it is currently barred from conducting. Where the government seeks to remotely search a computer the location of which is unknown, it does not now have a venue in which to

⁶⁷ See Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired (Sept. 13, 2013), <http://www.wired.com/2013/09/freedom-hosting-fbi/>.

⁶⁸ See Goodin, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, *supra*.
Attackers Wield Firefox Exploit to Uncloak Anonymous Tor Users, Ars Technica (Aug. 5, 2013), <http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/>.

⁶⁹ Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, *supra*.

⁷⁰ Patrick Howell O’Neill, *An In-Depth Guide to Freedom Hosting, the Engine of the Dark Net*, The Daily Dot (Aug. 4, 2013), <http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/>.

⁷¹ Proposed Amendments Materials at 341.

apply for a warrant. *In re Warrant to Search a Target Computer at Premises Unknown* [*In re Warrant*], 958 F. Supp. 2d 753, 756–58 (S.D. Tex. 2013). In effect, the government lacks the substantive authority to conduct remote access searches in such circumstances. For that reason, the proposed amendment will almost certainly result in a marked increase in government use of remote hacking techniques and zero-day exploits. What looks like a procedural change actually creates a new substantive power: to use zero-day exploits, malware, spyware, and other software packages to circumvent privacy-protective proxy services, including at least one, Tor, which was created by the US government, and continues to receive US government funding.

The government’s desire to augment the investigative tools available to it is understandable, but the best, and indeed the proper way to address the government’s asserted needs is for it to present its demand to Congress. Lawmakers can then craft a legislative solution to any gap in the government’s search powers. As the Supreme Court has remarked, “In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.” *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment) (citing Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805–806 (2004)); see also *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759 (2010) (“The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”).

When presented with similar questions of invasive technological searches and surveillance, Congress has opted to step in and set detailed legislative rules. This was true of the wiretapping and bugging of wire, oral, and electronic communications through Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III” or the “Wiretap Act”), 18 U.S.C. § 2518, and the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1804. It was likewise true of searches of the contents of stored electronic communications and other digital data in the Stored Communications Act, 18 U.S.C. § 2703, and of real-time individualized telephony metadata collection in criminal and national security investigations in the two acts addressing pen registers, 18 U.S.C. § 3123 and 50 U.S.C. § 1842. Congress clearly has the capacity and the will to legislate in this area, and legislative action is preferable because it lends itself to setting substantive limits on questionable search practices in a way that procedural rulemaking does not. Indeed, members of Congress have begun to take note of this proposed amendment,⁷² and would likely welcome the chance to hold hearings and contemplate legislative reform. The Federal Rules should not be amended to give the government new power to conduct remote access searches using zero-day exploits and spyware to defeat privacy-protective tools like Tor. Congress should be given the opportunity to weigh the competing constitutional and policy concerns that the government’s proposal raises, and to craft detailed statutory language regulating how, when, and where the government may conduct “remote access” searches.

Instead of using the procedural rulemaking process to suddenly and substantially increase the government’s use of remote hacking techniques in criminal investigations, the Committee should reject the proposed amendment and leave the government to present its case to Congress and the American people.

⁷² See Letter from Sen. Patrick Leahy to Attorney General Eric Holder (Oct. 30, 2014), available at <https://www.documentcloud.org/documents/1349789-leahy-to-holder-re-fbi-fake-ap-article.html>.

IV. The Proposed Amendment Raises Significant Constitutional and Statutory Concerns.

A. Use of Zero-Day Exploits and Malware May Constitute an Unreasonable Search.

Under the Fourth Amendment, use of zero-day exploits or malware may constitute an unreasonable search. It is well established that some searches in the physical world are too intrusive, destructive, or dangerous to be reasonable:

The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant. Excessive or unnecessary destruction of property in the course of a search may violate the Fourth Amendment, even though the entry itself is lawful and the fruits of the search are not subject to suppression.

United States v. Ramirez, 523 U.S. 65, 71 (1998) (citation omitted).

Surgically removing evidence from a suspect's body,⁷³ using a powerful motorized battering ram to break into a residence,⁷⁴ and "employ[ing] a flashbang device [to enter a house] with full knowledge that it will 'likely' ignite accelerants and cause a fire"⁷⁵ have all been ruled unreasonable under the Fourth Amendment. Zero-day exploits may well pose analogous concerns. When the government unleashes zero-day exploits and malware, it will rarely be able to control who can intercept the code in transmission, whether it will reach its intended target, whether it will be copied and reused by others, and whether it will spread virally across the internet and cause damage to innocent persons and businesses.⁷⁶ See Part II, *supra*. These factors are relevant to individual warrant applications, but also to the Advisory Committee's consideration of the proposed Rule amendment, because these outcomes are entirely predictable as a natural result of the kinds of searches the government wants the authority to conduct.

For example, when the United States and Israel launched the Stuxnet cyber-attack against Iranian nuclear enrichment facilities several years ago, it quickly spread beyond the targeted

⁷³ *Winston v. Lee*, 470 U.S. 753, 759, 766–67 (1985) (holding that the health risks posed by the "compelled surgical intrusion into an individual's body for evidence" make that search unreasonable under the Fourth Amendment); see also *Schmerber v. California*, 384 U.S. 757, 771–72 (1966) (requiring that a search involving drawing a suspect's blood be "performed in a reasonable manner," including that it be carried out by medical personnel in a medical environment); *Rochin v. California*, 342 U.S. 165, 172 (1952) (conduct by agents trying to obtain swallowed evidence, including "the forcible extraction of [the defendant's] stomach's contents," violates due process).

⁷⁴ *Langford v. Superior Ct. of L.A. Cnty.*, 729 P.2d 822, 827 (Cal. 1987) (holding that, because a motorized battering ram can cause "potential danger from collapse of building walls and ceilings or through rupture of utility lines," which could cause fires that "could threaten the safety not only of occupants, but of entire neighborhoods," "routine deployment of the ram to enter dwellings must be considered presumptively unreasonable unless authorized in advance by a neutral magistrate, and unless exigent circumstances develop at the time of entry").

⁷⁵ *Bing ex rel. Bing v. City of Whitehall, Ohio*, 456 F.3d 555, 570 (6th Cir. 2006).

⁷⁶ E.g., Rachel King, *Stuxnet Infected Chevron's IT Network*, Wall St. J., Nov. 8, 2012, <http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/>.

computer systems.⁷⁷ Major U.S. companies, including Chevron, discovered that the Stuxnet software had infected their networks as well.⁷⁸ If a piece of targeted malware developed with the vast resources of defense and national security agencies can go astray in this way, there is no reason to think law enforcement surveillance malware won't do so too.

Although it took several years before Stuxnet was discovered by security researchers,⁷⁹ the Stuxnet code and the zero-days it leveraged were extensively analyzed by a world-wide network of security experts. Although Microsoft rushed to develop and distribute patches for these vulnerabilities, criminals also took note, and exploited the same vulnerabilities for their own nefarious purposes.⁸⁰

More broadly, the use of malware and zero-day exploits is more invasive than other forms of permissible searches because the consequences and collateral damage associated with their use are inherently unpredictable and often irreversible. Because computers and the software they run are incredibly complicated systems, the consequences of their surreptitious penetration and exploitation by the government are inherently unpredictable. Malware can cause computer systems to fail in many unintended ways, causing the loss of property entirely unrelated to the government's searches. For example, a piece of malware could—whether through poor design or unpredictable interaction with other software on the target's computer—cause the destruction of data (such as family photos or document drafts) or the corruption of the operating system. The resulting data loss might or might not be reversible, depending on the circumstances.

The technological and internet-security implications of remote access searches are unavoidably complex. Before courts wade into the constitutional questions that the use of malware and zero-day exploits raise, it would be best for Congress to affirmatively address the wisdom and parameters of their use after informed public discussion. The policy and constitutional concerns that remote access searches raise are better suited to comprehensive legislative regulation than to authorization through procedural changes to the Federal Rules.

B. The Proposed Amendment Authorizes Searches That Can Only Be Carried Out Pursuant to a Title III Wiretap Order, and Would Be Illegal if Authorized by a Simple Rule 41 Warrant

Depending on the means used to conduct remote access searches and the information gathered, such searches may only be permissible pursuant to an order issued under the Wiretap Act, 18 U.S.C. § 2518, or a surveillance warrant containing equivalent protections. A normal warrant application submitted under Rule 41 may be constitutionally insufficient and infirm.

⁷⁷ Sanger, *supra* (“An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world.”).

⁷⁸ King, *Stuxnet Infected Chevron's IT Network*, *supra*.

⁷⁹ David Kushner, *The Real Story of Stuxnet*, IEEE Spectrum (Feb. 26, 2013), <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

⁸⁰ Pierluigi Paganini, *Kaspersky Revealed that Stuxnet Exploits Is Still Used Worldwide*, Security Aff. (Aug. 19, 2014), <http://securityaffairs.co/wordpress/27633/cyber-crime/stuxnet-flaw-still-targeted.html>.

The Wiretap Act, also known as Title III, applies when the government seeks to intercept wire, oral, or electronic communications in real time. Because this sort of electronic surveillance raises, “understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens,” special protections are required. *United States v. U.S. District Ct.*, 407 U.S. 297, 312 (1972). Under Title III, these protections include requirements that the government particularly describe the place and person to be surveilled, that the government show it has exhausted other investigative procedures prior to seeking a Title III order, and that the court limit the duration of the surveillance and require minimization of interception of non-pertinent communications. 18 U.S.C. § 2518(1)–(5). Moreover, unlike with search warrant applications, attorneys at DOJ’s Office of Enforcement Operations review each wiretap application before it is submitted to a court.⁸¹ Courts have also imposed Title III’s requirements on applications for warrants to authorize surreptitious video surveillance, even though such surveillance is not technically covered by the statute. *See, e.g., United States v. Cuevas–Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987); *United States v. Biasucci*, 786 F.2d 504, 510–11 (2d Cir. 1986); *United States v. Torres*, 751 F.2d 875, 884 (7th Cir. 1984). These requirements, for both wiretapping and video surveillance, derive from and are required by the Fourth Amendment. *See Berger v. New York*, 388 U.S. 41, 58–59 (1967) (wiretapping); *Torres*, 751 F.2d at 884 (video surveillance).

Remote access searches can raise identical or analogous concerns. Certainly, if the government seeks to activate the built-in camera on a target computer, it must meet the heightened requirements for video surveillance. *In re Warrant*, 958 F. Supp. 2d at 759–61. If the government’s remote access surveillance software is configured to turn on the target computer’s microphone or to collect the contents of incoming or outgoing electronic or wire communications (such as emails, instant messages, or internet-based phone calls), Title III procedures would be required. *See* 18 U.S.C. § 2518. Further, “[s]oftware that can retrieve [other stored] information—Internet browser history, search terms, e-mail contents and contacts, ‘chat’, instant messaging logs, photographs, correspondence, and records of applications run, among other things”—also calls for heightened Fourth Amendment protections, because surreptitious and remote retrieval of such a “volume of information” raises constitutional concerns. *In re Warrant*, 958 F. Supp. 2d at 760. Electronic surveillance that “is identical in its indiscriminate character to wiretapping and bugging” cannot be authorized by a normal Rule 41 warrant. *Torres*, 751 F.2d at 885 (emphasis omitted).

Indeed, as explained above, remote access searches raise even more significant concerns in that malware and the exploitation of zero-day flaws can cause entirely unpredictable and irreversible damage to a target’s computer or data. Reducing the likelihood of, or mitigating the harms of, such unintended consequences would require significant technical expertise and

⁸¹ H.R. Rep. No. 112-546, at 10 (2012), available at <http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt546/pdf/CRPT-112hrpt546.pdf> (“In a letter to Chairman Issa, the Deputy Attorney General acknowledged that the Office of Enforcement Operations (OEO), part of the Justice Department’s Criminal Division, is ‘primarily responsible for the Department’s statutory wiretap authorizations.’ According to the letter, lawyers in OEO review these wiretap packages to ensure that they ‘meet statutory requirements and DOJ policies.’ When OEO completes its review of a wiretap package, federal law provides that the Attorney General or his designee—in practice, a Deputy Assistant Attorney General in the Criminal Division—reviews and authorizes it. Each wiretap package includes an affidavit which details the factual basis upon which the authorization is sought.”).

regulation of the manner in which the government develops and deploys its remote access software. Courts are ill-suited to oversee such mitigation efforts in the first instance.

Any malware, spyware, or other government software that remains on a target computer and collects information on an ongoing basis also implicates these concerns. Clandestine entry into a person's computer, installation of software there, and use of that software to conduct real-time surveillance should require the heightened showing of a Title III order. A warrant issued under normal Rule 41 procedures that authorizes an ongoing search will necessarily violate the Fourth Amendment; restrictions are needed "to guarantee that . . . [these searches] occur[] only when there is a genuine need for [them] and only to the extent that [they are] needed." *Dalia v. United States*, 441 U.S. 238, 250 (1979). Yet, it is clear that the government is *already* collecting information about computer users on an ongoing basis using remote access malware without obtaining a Title III order or equivalent judicial process. Approving the proposed amendment would give sanction to this highly problematic practice.

In an investigation in Washington State in 2007, the FBI applied for a hybrid order to justify its installation and monitoring of the CIPAV surveillance software: a Rule 41 warrant to authorize transmission and installation of the software and its one-time use to collect location, identification, and other data from the target computer, combined with a pen register order to authorize ongoing collection of "routing and destination addressing information for electronic communications originating from the activating computer."⁸² A hybrid order of this type cannot substitute for the strictures of Title III.

A pen register order is intended to be served on a "person or entity providing wire or electronic communication service," 18 U.S.C. § 3123(a)(1), to compel their assistance in turning over "dialing, routing, addressing, or signaling information," *id.* § 3127(3). Installation of spyware on a person's computer and contemporaneous monitoring of information about all types of electronic communications originating from that computer is a good deal more invasive, because it relies on entry into a person's private space and maintenance of a presence there to collect information. This is, in effect, a trespassory search. *Cf. United States v. Jones*, 132 S. Ct. 945, 949 (2012) (holding that a Fourth Amendment search occurred when "[t]he Government physically occupied private property for the purpose of obtaining information"). It is also the kind of unusually intrusive surveillance to which the heightened standard of Title III applies. The government appears to want to use the pen register statute to authorize what a Rule 41 warrant cannot standing alone, but that defies common sense. As Judge Stephen Smith explained while rejecting a variant of the government's hybrid order theory in another context, "[s]urely if these various statutory provisions were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way. This is especially so given that no other form of electronic surveillance has th[is] mixed statutory parentage." *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 764–65 (S.D. Tex. 2005). Invasive monitoring carried out by

⁸² Affidavit of Norman B. Sanders Jr. at 4, 13, *In re Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Message(s) Delivered to that Account by the Government*, MJ-07-88 (W.D. Wash. June 12, 2007), available at <https://www.eff.org/document/fbicpav-08pdf>.

installing malware on a target’s computer should require a Title III order—or new congressional legislation—not a cobbled-together patchwork of lesser permissions.

Adopting the proposed amendment to Rule 41 risks facilitating violations of Title III and deciding by administrative rulemaking a question better left to Congressional regulation—how to regulate and circumscribe the controversial and invasive search techniques at issue here.

C. The Proposed Amendment Will Facilitate Violations of the Fourth Amendment’s Particularity Requirement and Will Result in Searches of Non-Suspects as to Whom There is No Probable Cause.

The proposed amendment would allow police to remotely search many people’s computers using a single warrant, often without particularly describing those computers or demonstrating probable cause as to their owners or users. A warrant that does not particularly describe the place to be searched and things to be seized is invalid. *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (citing U.S. Const. amend IV). For this reason, courts have been skeptical of warrants authorizing searches of multiple locations not owned by the same person.⁸³ In the context of physical searches, “[t]he general rule is that a warrant for a building that has multiple units must specify the individual unit that is the subject of the search to satisfy the particularity requirement.”⁸⁴ The same concerns and rules should apply when police search digital “occupancies.” Indeed, “[t]he need for particularity . . . is especially great in the case of eavesdropping.” *Berger*, 388 U.S. at 56. So, too, for remote access hacking.

Further, a search warrant that demonstrates probable cause as to one suspect or location does not thereby justify any search anywhere. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 554 (1978) (second emphasis added) (“[V]alid warrants may be issued to search *any* property, whether or not occupied by a third party, *at which there is probable cause* to believe that fruits, instrumentalities, or evidence of a crime will be found.”)⁸⁵ The Wiretap Act illustrates application of this principle to warrants authorizing invasive electronic surveillance: the government must demonstrate not only that there is probable cause of commission of a qualifying criminal offense, but also that there is probable cause for belief “that particular communications concerning that offense will be obtained through such interception” and that the facilities or places to be wiretapped or bugged are being used in connection with the offense or

⁸³ “[I]n the case of multi-location search warrants, the magistrate must be careful to evaluate each location separately. ‘A search warrant designating more than one person or place to be searched must contain sufficient probable cause to justify its issuance as to each person or place named therein.’” *Greenstreet v. Cnty. of San Bernardino*, 41 F.3d 1306, 1309 (9th Cir. 1994) (quoting *People v. Easley*, 671 P.2d 813, 820 (Cal. 1983)).

⁸⁴ Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 *Stan. L. Rev.* 1005, 1045 n.173 (2010) (citing *Jacobs v. City of Chicago*, 215 F.3d 758, 767 (7th Cir. 2000)). *See also United States v. Hinton*, 219 F.2d 324, 325–26 (7th Cir. 1955) (“For purposes of satisfying the Fourth Amendment, searching two or more apartments in the same building is no different than searching two or more completely separate houses.”); *United States v. Clark*, 638 F.3d 89, 98 (2d Cir. 2011) (warrant defective where issuing judge was not informed of building’s size or number of residential units and was incapable of making probable cause determination of defendant’s control of entire multi-family building).

⁸⁵ *See also, e.g., Commonwealth v. Cefalo*, 409 N.E.2d 719, 726 (Mass. 1980) (“In the case of a search warrant, . . . the affidavit must, in order to establish probable cause, contain enough information for the issuing magistrate to determine that the items sought are related to the criminal activity under investigation, *and that they may reasonably be expected to be located in the place to be searched.*” (emphasis added)).

used by the targeted person. 18 U.S.C. § 2518(3)(a)–(d). Remote, surreptitious computer searches should be held to the same standard.

Authorizing the kinds of remote access searches that the government seeks to conduct threatens to violate the Fourth Amendment’s particularity and probable cause requirements in several ways. First, if the government configures a website or server to deliver malware to the computer of every person who visits it (a watering hole attack), it will likely end up searching the computers of people who it cannot particularly identify or describe and as to whom it lacks probable cause. There do exist a small subset of websites or servers where all access may violate the law (websites that do nothing more than distribute child pornography might qualify). However, issuing a search warrant authorizing the surreptitious delivery of malware onto the computers of an unknown number of targets raises serious legal and policy questions. Moreover, even if orders for bulk installation of malware are deemed to be proper, the vast majority of websites or servers that the government might commandeer to deliver malware to visitors’ computers will be visited by both legitimate targets and non-targets alike. For example, members of the press, researchers, policymakers, and attorneys regularly visit websites associated with terrorist groups, cyber-criminals, and drug dealers.⁸⁶ Were courts to authorize the installation of malware to all visitors to these and other types of websites, the government would undoubtedly end up searching the computers of innocent people who are not engaged in any crime, who have a perfectly valid reason to have visited the site, and as to whom there is no probable cause.

The same may be true of more targeted delivery of remote access hacking software. For example, when the government delivered spyware to a suspect in a 2007 investigation in Washington, it did so by creating a fake Associated Press story and then sending a link to one of the suspect’s social media accounts.⁸⁷ “When the suspect clicked on the link, the hidden FBI software [installed itself on his computer and] sent his location and Internet Protocol information to agents.”⁸⁸ Had the suspect forwarded the link to acquaintances, posted it on social media, or otherwise distributed it, people as to whom the government lacked probable cause would likely have clicked on the link and triggered a search of their computers. The same would have happened if the government had posted the link to a public portion of the suspect’s social media account (it is not known whether the government did so because public information about the search is limited). Likewise, if an internet search engine had indexed the fake page,⁸⁹ any internet user could have happened upon the link during a search, clicked on it, and triggered a search of their computer. Once released into the world, government malware is difficult to contain.⁹⁰ A warrant could not have authorized these collateral, but foreseeable searches because

⁸⁶ Indeed, the reason the American public learned about the Target data breach (and many others) is because a journalist regularly reads invitation-only cyber-crime forums. See Brian Krebs, *Cards Stolen in Target Breach Flood Underground Markets*, Krebs on Security (Dec. 20, 2013), <http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/#more-24093>.

⁸⁷ Gene Johnson, *FBI Says It Faked AP Story to Catch Bomb Suspect*, Associated Press, Oct 28, 2014, <http://bigstory.ap.org/article/29ae75189b254e47bfb79c3a0de256ec/ap-seattle-times-upset-about-fbi-impersonation>; see also Mike Carter, *FBI Created Fake Seattle Times Web Page to Nab Bomb-Threat Suspect*, Seattle Times, Oct. 27, 2014, http://seattletimes.com/html/localnews/2024888170_fbnewspaper1.xml.html.

⁸⁸ Carter, *supra*; see also Johnson, *supra*.

⁸⁹ See Google, *Crawling & Indexing*, <http://www.google.com/insidesearch/howsearchworks/crawling-indexing.html> (“We use software known as ‘web crawlers’ to discover publicly available webpages.”).

⁹⁰ See, e.g., Rachel King, *Stuxnet Infected Chevron’s IT Network*, Wall St. J., Nov. 8, 2012, <http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/>.

the government would have lacked probable cause as to the people searched, and could not have particularly described the places to be searched or digital files to be seized.

Individual magistrate judges reviewing warrant applications may be able to address some of these concerns in some cases. But because these defects will pervade remote access warrant applications and are entirely predictable, the best course is to reject the proposed amendment and allow Congress the opportunity to set detailed rules concerning particularity and probable cause.

D. The Proposed Amendment Weakens Rule 41's Notice Requirement

The proposed amendment modifies Rule 41's notice requirement so that for remote access searches the government "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."⁹¹ The means of service must be "*reasonably calculated* to reach that person."⁹² This departs from the normal requirement that "[t]he officer executing the warrant *must* give a copy of the warrant and a receipt for the property taken to the person" subject to the search. Fed. R. Crim. P. 41(f)(1)(C) (emphasis added).

The proposed language clearly contemplates searches for which no notice can be provided. Indeed, the circumstances in which the government will likely seek authority to conduct remote access searches all but guarantee that notice will be difficult if not impossible to provide in many or most cases. If, for example, the government seeks to learn the identity and location of a particular internet user, it might often be the case that all it learns is that the user is connected to the internet from an IP address associated with a coffee shop in a large urban area. It is not at all clear that any means would be available to the government to reliably provide notice in that likely typical scenario.

But failure to provide notice "casts strong doubt on [a warrant's] constitutional adequacy." *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (citing *Berger*, 388 U.S. at 60). As the Ninth Circuit has explained,

[a] warrant [i]s constitutionally defective [if it] fail[s] to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. . . . We take this position because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed.

Id.; see also *United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) ("[I]f a delay in notice is to be allowed, the court should nonetheless require the officers to give the appropriate person notice of the search within a reasonable time after the covert entry.").

⁹¹ Proposed Amendments Materials at 340 (emphasis added).

⁹² *Id.* (emphasis added).

Surreptitious entry into a repository of a person’s electronic files, containing digital analogues of her diaries, address books, letters, and photo albums, raises no less important concerns. See *United States v. Payton*, 573 F.3d 859, 861–62 (9th Cir. 2009) (“There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers.”). Even when police seek to search only a limited set of data on a computer, the importance of notice is paramount. Computers “store and intermingle a huge array of one’s personal papers in a single place[, which] increases law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs.” *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009). And even if no data is copied during the search, the surreptitious entry itself raises concerns, particularly when it is achieved using means that may expose the computer user to malicious incursions by other actors taking advantage of the government’s means and method of entry.⁹³

Another problem with the proposed amendment is that it will allow the government to provide notice to either “the person whose property was searched *or* whose information was seized or copied.”⁹⁴ When those are different people, notice should be given to both. If, for example, the government were to conduct a remote access search of a computer owned by one person but used by others, it could interpret the rule to allow it to provide notice to only the owner, but not to the person whose files (“information”) were actually seized or copied. This would be so even if the seized files were located in a password-protected folder and were clearly identifiable as being the property of someone other than the computer’s owner. The computer’s owner may fail to, or be ordered not to, inform the target of the search upon receiving notice from the government. Thus, the target might never learn of the search, and therefore never be able to challenge its constitutionality. To avoid this problem, “*or*” should be replaced with “*and*.”

Finally, even in situations where the government’s efforts to provide notice to the proper person eventually succeed, notice will often be delayed. An increase in delayed-notice searches occasioned by the proposed amendment raises concerns. In the context of Title III, Congress has implicitly authorized covert entry and delayed notice when installing and operating surveillance equipment, but only when the government complies with “detailed restrictions” that “guarantee that wiretapping or bugging occurs only when there is a genuine need for it and only to the extent that it is needed.” *Dalia*, 441 U.S. at 250; see 18 U.S.C. § 2518 (imposing duration and minimization requirements on wiretap orders). Similar safeguards have been imposed by courts to regulate video surveillance. See, e.g., *Biasucci*, 786 F.2d at 510–11. Delayed notice may be permissible if it is of short duration and reviewed by a judge, but it has the potential to interfere with substantive Fourth Amendment rights if too heavily, widely, or extensively used. To the extent “remote access” searches are permissible at all, any delay of notice must be specifically

⁹³ The proposed amendment may also violate the knock-and-announce rule. As the Supreme Court has explained, the Fourth Amendment does not “permit[] a blanket exception to the knock-and-announce requirement for [an] entire category of criminal activity.” *Richards v. Wisconsin*, 520 U.S. 385, 388 (1997). Neither the government nor courts may “dispens[e] with case-by-case evaluation of the manner in which a search [is] executed,” including when it comes to knock-and-announce. *Id.* at 392. To the extent that remote access search warrants are permissible at all, unannounced searches may sometimes be justified by a specific factual showing under the circumstances of a particular case. But a categorical rule permitting unannounced searches may violate the Fourth Amendment.

⁹⁴ Proposed Amendments Materials at 340 (emphasis added).

justified in the individual case, notice must be given “within a reasonable time after the covert entry,” and the restrictions currently imposed on wiretap and video surveillance warrants must be observed. *Villegas*, 899 F.2d at 1336–37.

It is perhaps for the very reason that remote access searches raise intractable notice problems that neither Congress nor the courts have yet seen fit to permit the government the general authority to search individuals whose locations are entirely unknown. It may be that the inability to guarantee notice in the mine-run of remote access searches could be overcome in some technological or legislative manner. But that possibility is best left to congressional inquiry in the first instance.

V. The Proposed Amendment Raises Wide-Ranging Questions That the Committee Should Consider Now, Because Those Questions are Unlikely to Be Addressed in Individual Cases for Years to Come

The Advisory Committee should proceed with extreme caution before expanding the government’s authority to conduct remote electronic searches. As explained above, the proposed amendment would significantly expand the government’s authority to conduct searches that raise troubling and wide-ranging constitutional, statutory, and policy questions. If the Committee approves the proposed amendment, courts are unlikely to address these questions in individual cases, at least not in the foreseeable future. Therefore, it is vital that the Committee carefully consider all of the implications of the proposed amendment now. If those implications cannot be adequately addressed through a change to the Federal Rules—which they cannot—the Committee’s best course would be to reject the proposal and leave it to Congress to take up the question.

Even if the Advisory Committee determines that the proposed amendment will “govern[] only ‘the manner and the means’ by which the litigants’ rights are ‘enforced,’” and will not “alter[] ‘the rules of decision by which [the] court will adjudicate [those] rights,’” *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 407 (2010) (second and third alterations in original), it should still be reticent to approve the amendment. The constitutional questions raised by the amendment include what limitations the particularity, probable cause, and reasonableness requirements of the Fourth Amendment impose on remote access searches. These will likely not be addressed by courts for years, if ever. Moreover, important policy questions involving cybersecurity and government exploitation of internet and software vulnerabilities are implicated, as are conflicts with the text and intent of the Wiretap Act. In order to prevent violations of the Fourth Amendment and an unchecked expansion of government power, this Committee should grapple with these issues now. The Department of Justice should request the authority it seeks from Congress, so as to permit a public debate about the propriety of the intrusive techniques it proposes to use and about possible alternatives that Congress would be in a unique position to craft.

There are several reasons why courts are unlikely to address Fourth Amendment limits on remote access searches in the near future. For one, warrant applications are considered by judges *ex parte* and without adversarial argument. While magistrate judges are experienced in assessing general questions of particularity and probable cause in run-of-the-mill warrant applications, they

are likely to be ill-equipped to provide robust review of applications for remote access warrants without adversarial briefing, particularly when the search warrant applications do not make clear that agents are seeking permission to hack into the computers of surveillance targets. Full appraisal of these applications requires technical expertise about electronic data storage issues, internet architecture, and cybersecurity. Applications that appear reasonable on their face in light of a magistrate judge's limited technical understanding may in fact fail the particularity and reasonableness requirement upon closer study. But without detailed technical knowledge—or adversarial briefing explaining the issues—many of these concerns will go unnoticed and unaddressed.

Further, orders granting or denying warrants are rarely published and are usually sealed.⁹⁵ The likelihood of magistrate judges *sua sponte* publishing detailed opinions analyzing Fourth Amendment issues involved in electronic searches is particularly low when they are unable to independently identify the constitutional infirmities of the warrant application. Indeed, although the government has already sought warrants to authorize remote access searches,⁹⁶ there is only one published opinion of a magistrate judge grappling with the Fourth Amendment issues involved. *See In re Warrant*, 958 F. Supp. 2d 753. There is no telling how long it will be until there is another.

Additionally, notice may be delayed for significant periods of time, thus forestalling the time when the target of a remote access search could challenge its constitutionality. *See Fed. R. Crim. P. 41(f)(3); 18 U.S.C. § 3103a(b)–(c)*. And even when notice is given, *ex post* judicial review is limited by doctrines precluding or discouraging a ruling on the constitutionality of the government's conduct. In criminal prosecutions, defendants may challenge the constitutionality of a search through motions to suppress. In response to such motions, the government is likely to argue that investigating officers were relying in good faith on a facially valid warrant when conducting the search. *See United States v. Leon*, 468 U.S. 897 (1984). Courts frequently address the good-faith exception before—and to the exclusion of—the substantive Fourth Amendment claim when denying motions to suppress.⁹⁷ Thus, even in cases where a remote access warrant fails the particularity, probable cause, or reasonableness requirements of the Fourth Amendment, courts will generally avoid ruling on the issue.

The doctrine of qualified immunity functions in much the same way to preclude substantive adjudication in suits seeking damages for violations of Fourth Amendment rights.⁹⁸

⁹⁵ *See* Laura Donahue, Professor, Georgetown Univ. Law Ctr., Remarks at Panel on the Legal and Policy Implications of Hacking by Law Enforcement at Yale Law School (“Remarks by Laura Donahue”), at 18:00–21:40 (Feb. 18, 2014), <http://vimeo.com/88165230> (stating knowledge of dozens of cases involving government use of hacking tools, but explaining that most of the relevant magistrate judge orders are sealed).

⁹⁶ *Id.*

⁹⁷ *See, e.g., United States v. Clay*, 646 F.3d 1124, 1128 (8th Cir. 2011) (“[T]he district court properly denied [the defendant’s] motion to suppress based on the *Leon* good-faith exception. In light of this conclusion, we need not reach the underlying question of probable cause.”); *United States v. Woodbury*, 511 F.3d 93, 99 (1st Cir. 2007) (“We need not address [the defendant’s] particularity arguments because we find that the *Leon* good faith exception applies.”); *United States v. Cherna*, 184 F.3d 403, 407 (5th Cir. 1999) (“If [the *Leon* good faith exception applies], we end our analysis and affirm the district court’s decision to deny the motion to suppress. . . . If the good-faith exception applies, we need not reach the question of probable cause.”).

⁹⁸ *See Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388 (1971). Suits for injunctive and declaratory relief are likely to be barred by standing doctrine, on the basis that a person targeted by a remote

Qualified immunity “protects government officials from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.” *Pearson v. Callahan*, 555 U.S. 223, 231 (2009) (internal quotation marks omitted). Courts have discretion to address qualified immunity before determining whether the government has violated a plaintiff’s constitutional rights, *id.* at 236, and they frequently do so. Courts often dispose of cases seeking relief for Fourth Amendment violations by concluding that there was no clearly established law at the time of the search which would have put law enforcement on notice that their conduct was unconstitutional. *See, e.g., Messerschmidt v. Millender*, 132 S. Ct. 1235 (2012) (finding qualified immunity and declining to rule on whether facts stated in a warrant application established probable cause). The issues raised by warrants for remote, extra-district electronic searches are necessarily novel because the Federal Rules have not heretofore authorized them. Therefore, the government will almost certainly argue that qualified immunity applies. Perversely, the very absence of case law addressing these searches will mean there is likely to be little development of case law addressing the constitutionality of these searches in the future.

Accordingly, the time to address the constitutional concerns raised by the proposed amendment is now. Speculation that these important issues will be fully dealt with in future case law is unlikely to prove correct, at least in the near future. The significant issues involved counsel caution, and the right course is to reject the proposed amendment and let Congress act.

These problems are exacerbated by the government’s lack of candor about the nature of its remote access searches. The DOJ’s explanations of its remote access search capability in the sample warrant applications,⁹⁹ in warrant applications actually filed in federal court,¹⁰⁰ and in its recent memoranda to this Committee fail to fully describe the nature and invasiveness of its contemplated and completed remote access searches. As described above, one use of the proposed amendment will be to enable searches involving malware or spyware that take advantage of zero-day vulnerabilities and that travel over the open internet. But nothing in the government’s descriptions of its “network investigative techniques”¹⁰¹ or “remote network techniques”¹⁰² would put a magistrate judge (or, for that matter, a member of this Committee) on notice that the government seeks to hack into the computers of targets, exploiting publicly unknown security flaws in the software on those devices using techniques that may create significant cybersecurity collateral damage to the target and to others, and that may fail the reasonableness and particularity requirements of the Fourth Amendment.¹⁰³

access search in the past will not be able to prove a likelihood that they will be subjected to such a search again in the future. *See City of L.A. v. Lyons*, 461 U.S. 95 (1983).

⁹⁹ *See* Advisory Committee Materials at 181–235.

¹⁰⁰ *See, e.g.*, Affidavit of Justin E. Noble in Support of Application for Search Warrant, *In re Search of Network Investigative Technique (“NIT”) for E-mail Address 512SocialMedia@gmail.com*, No. 12-mj-748-ML (W.D. Tex. Dec. 18, 2012); Third Amended Affidavit of William A. Gallegos In Support of Application for Search Warrant, *In re Search of Network Investigative Technique (“NIT”) for Email Address texan.slayer@yahoo.com*, No. 12-sw-05685-KMT (D. Colo. Dec. 11, 2012).

¹⁰¹ *See, e.g.*, Advisory Committee Materials 200–03.

¹⁰² *See, e.g., id.* 216.

¹⁰³ *See* Remarks by Laura Donahue, *supra*, at 21:45–22:17 (“Often [the government’s] applications do not include detailed technology, or technological explanation as to how it is actually going to be executed, enter the computer, exactly what information is going to be obtained, which other devices might be infected, how many devices may be infected, and so on.”).

It is crucial that the government provide full and accurate information to magistrate judges (and to this Committee) when seeking authority to conduct novel and invasive searches.¹⁰⁴ The Advisory Committee should not authorize new search powers without ensuring that the duty of candor has been and will be satisfied. At a minimum, the Advisory Committee Notes accompanying the proposed amendment should speak to this issue.

VI. Recommendations

The ACLU recommends that the Committee reject the proposed amendment to Rule 41. The proposed amendment raises myriad technological, policy, and constitutional concerns. Some of those might be addressed through careful regulation; others are inherent in even the most circumscribed versions of the proposal. The dramatic expansion of investigative power that the government seeks should not be authorized through a change to the Rules of Procedure. Rather, if the government wants this power, it should seek congressional action.

Should Congress decide that remote access searches in the situations covered by the proposed amendment are to be permitted, the ACLU would recommend a set of restrictions to mitigate its concerns, including:

- Require a Title III order for any remote access search that collects information on an ongoing basis or forces a target's device to generate or collect new data (such as by turning on a computer's webcam or microphone);
- Only permit use of malware against specific and particularly described persons. Watering hole attacks, particularly when performed against sites that share computing resources with other innocent websites, present significant public policy and legal issues which make such attacks problematic;
- Require that the government make explicit in warrant applications that it intends to conduct a remote access search using malware and that it will exploit security vulnerabilities in the software on the target's device to do so, and require the government to describe in detail how the malware will work, how many computers it will affect, how long it will remain installed on those computers, what code will remain on those computers indefinitely, the extent to which there may be irreversible changes or damage to devices, the extent to which insertion of the malware requires the assistance of a third party service provider, what impact there will be on the security of computers of targets and non-target third parties, whether it is reasonably foreseeable that government malware could malfunction, target the wrong people, or fall into the wrong hands, what technical experts have

¹⁰⁴ *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1178 (Kozinski, C.J., concurring) (“[O]mitting . . . highly relevant information [about a search of electronic data] is inconsistent with the government's duty of candor in presenting a warrant application. A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.”); cf. Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 *Yale J. L. & Tech.* 134, 162 (2013) (discussing government's lack of candor to judges when seeking authority to use “Stingray” cell phone tracking devices).

been consulted prior to submission of the application, and the basis for the determinations made with regards to the issues above;

- Prohibit the impersonation of third parties by law enforcement agencies in their efforts to deliver malware to targets, unless those third parties provide informed consent in writing;
- Require that any assistance of a service provider in delivering the malware be consensual or explicitly required by the warrant;
- Require law enforcement malware to include identifying markings in the computer code, such that if the code is subsequently discovered by security researchers, they will know who to contact if, for example, the malware malfunctions, spreads, or ends up on the computers of non-suspects;
- Prohibit the use by law enforcement of zero-day exploits in general-use software and hardware; and
- Prohibit the approval of warrants in which there is a reasonable likelihood that execution of the warrant will result in damage to third parties who are not the intended law enforcement target.

Many of these proposed constraints are beyond this Committee's power to enact. The ACLU recommends that the Committee not adopt the proposed amendment and allow the government to seek legislation in Congress.

* * * * *

Thank you for your consideration of these comments.

Respectfully,



Nathan Freed Wessler
Christopher Soghoian
Alex Abdo
American Civil Liberties Union
Speech, Privacy, and Technology Project
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8fbu-46g0
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0015](#)

Testimony of Robert J. Anello, on behalf of the Federal Bar Council

Submitter Information

Name: Robert J. Anello

Organization: Federal Bar Council

General Comment

See attached

Attachments

Testimony for Nov. 5 Hearing



Serving the courts and legal community
of the Second Circuit since 1932

Federal Bar Council

ROBERT J. ANELLO
President, Federal Bar Council

DAVID B. ANDERS
Chair, Federal Criminal Practice Committee

TESTIMONY OF ROBERT J. ANELLO BEFORE THE ADVISORY COMMITTEE ON CRIMINAL RULES
Thurgood Marshall Federal Judiciary Building
One Columbus Circle, N.E., Washington, D.C.
November 5, 2014

Good morning. My thanks to the Advisory Committee on Criminal Rules for the invitation to testify today. I am the president of the Federal Bar Council, an organization of lawyers who practice in federal courts within the Second Circuit¹. The Council was founded in 1932, and currently has approximately 3,800 members. It is dedicated to promoting excellence in federal practice and fellowship among federal practitioners. The Council, together with its several committees, regularly comments on proposed changes to the various rules that affect the practices of our members.

In a letter dated August 27, 2014, the Advisory Committee solicited the views of the Council on several proposed amendments to Federal Rules of Criminal Procedure 4 and 41. The Council provided its views on the proposed amendments in a letter addressed to the Committee on Rules of Practice and Procedure, dated October 27, 2014.

On behalf of the Council, I would like to commend the Advisory Committee on Criminal Rules for its work developing these amendments to the Federal Rules of Criminal Procedure. The Council supports the proposed amendments to Rules 4 and 41 and recommends that the Advisory Committee submit all of the proposed amendments to the Committee on Rules of Practice and Procedure.

Rule 4

In its current form, Rule 4 provides that, for service to be effected on a corporation, a copy of the summons must be delivered to an officer, managing or general agent, or to another agent authorized to receive service. A copy also must be mailed to the organization's last known address within the judicial district, or to its principal place of business elsewhere in the United States.

The mailing requirement poses an undue obstacle to the prosecution of foreign corporations that are suspected of committing offenses in the United States, but that

¹ I am also a principal in Morvillo Abramowitz Grand Iason & Anello P.C., a firm that specializes in litigation and, in particular, white collar criminal defense.

cannot be served because they have no last known address or principal place of business here. This has led the Department of Justice to recommend that Rule 4 be amended to remove the mailing requirement, and to designate the means to serve a summons upon an organization located outside the United States.

In response to the DOJ's recommendation, the Advisory Committee has proposed several amendments to Rule 4. Chief among these are (i) limiting the mailing requirement when delivery is made in the United States, (ii) providing means for service outside the United States, and (iii) specifying that sanctions may be levied against an organizational defendant that fails to appear in response to a summons.

To address the concern that service of process on foreign organizations may not be completed if the organization does not have either (i) an address within the district, or (ii) a principal place of business outside the district, but within the United States, the Advisory Committee has proposed limiting the mailing requirement. Under the proposed amendments, the mailing requirement would apply only to situations where service has been made on a statutorily appointed agent, and the authorizing statute itself requires mailing as well as personal service.

The Advisory Committee also has recommended amending Rule 4 to authorize service on a foreign organization by any "means that gives notice." The proposed amendment sets out three permissible, non-exhaustive methods of service that presumptively satisfy this requirement.

Finally, the Advisory Committee has proposed amending Rule 4 to address the potential consequences for an organization that fails to appear in response to a summons. Rule 4 currently provides that both individual and corporate defendants may be served with a summons, but the rule is silent on the procedure to be followed if an organizational defendant fails to appear. The proposed amendment would fill this gap, by providing that a judge may take any action authorized by United States law if an organizational defendant fails to appear.

In the view of the Federal Bar Council, the proposed amendments fairly address the gaps in the current version of the rule that may prevent the government from being able to prosecute effectively foreign organizations that commit crimes in the United States but have no physical presence here.

In light of the actual delivery required by the rule, the Council believes that the mailing requirement in Rule 4 is largely redundant and unnecessary, and prevents service on foreign organizations without a physical presence in the United States. The amendments would eliminate this requirement, unless a statutory obligation exists to mail a copy of the summons to the organization.

The Council is also of the view that the various methods of service for foreign organizations described in the amendments are reasonably calculated to provide effective notice, while also ensuring that service complies with United States constitutional requirements, the law of the foreign jurisdiction, and any applicable international agreements.

The Council also agrees with the Advisory Committee's decision to give the courts discretion to fashion remedies for a corporation's failure to appear after service, to the extent authorized by United States law. Foreign and domestic corporations have many incentives to appear and resolve criminal charges once service is made. For this reason, cases in which an organizational defendant has defaulted appear to be rare. Nevertheless, to the same extent good reasons exist to permit a court to impose consequences on an individual defendant who fails to appear for a criminal summons, courts should possess such authority as to organizational defendants. The Advisory Committee's language provides a framework for the courts to evaluate the range of actions authorized by law if and when cases arise in which a corporate defendant fails to appear after being served with a summons.

For these reasons, and for the reasons provided by the Advisory Committee, we recommend that the Advisory Committee submit the proposed amendments to Rule 4 to the Committee on Rules of Practice and Procedure.

Rule 41

Rule 41 addresses the circumstances under which a court has authority to issue a warrant to search and seize a person or property. With few exceptions, the court's authority is limited to issuing warrants for search and seizure of person or property located within the district.

The Department of Justice has raised concerns about the rule's territorial venue restrictions in the context of efforts to search and seize electronic information. In particular, the Department of Justice is concerned that the rule may impede investigations when the location of electronic information sought is unknown, or the electronic information sought spans multiple districts, requiring law enforcement to coordinate efforts with local law enforcement, prosecutors, and courts in multiple jurisdictions. At least one court has declined to issue a warrant under such circumstances because of the rule's express territorial limits.

The Advisory Committee has proposed two changes to Rule 41 to address these concerns. A new proposed section, Rule 41(b)(6), sets out two circumstances under which a court may issue a warrant to use remote access to search electronic storage media, and to seize or copy information, even if the information is or may be located outside of the district. Second, Rule 41(f)(1)(c) would be amended to include language indicating the process for providing notice of a remote access search.

The Federal Bar Council believes that, on balance, these amendments are necessary and will be effective in permitting law enforcement to investigate crimes involving computers and electronic information. Rule 41's territorial limits present unique problems for investigations requiring access to electronic information or storage devices. For instance, sophisticated software may be used to mask the location of a computer or electronic storage device. In this situation, law enforcement may be prevented from identifying the district in which electronic information or an electronic device is located in an otherwise sufficiently detailed warrant. Law enforcement efforts may likewise be thwarted or delayed by complex criminal schemes that involve the use of multiple computers in multiple districts simultaneously. Under the current Rule 41, investigating such schemes may require the government to expend extraordinary resources and efforts to coordinate obtaining individual warrants from the various districts involved. Both of these problems have become more common as crimes involving the use of computers have increased in frequency and complexity.

Under the proposed amendments, investigators could obtain a warrant to remotely install software on a target device to determine the true IP address or identifying information for that device, but only if that location of the device or information has been concealed by technological means. The Council understands that the ACLU has submitted comments to the Advisory Committee objecting to this type of remote access. The Council's Federal Criminal Practice Committee has reviewed the ACLU's objections and concluded that the use of remote access techniques is appropriate under the narrow circumstances outlined in the proposed rule.

The proposed amendments leave unanswered a number of constitutional questions, such as the level of specificity required in a warrant seeking authorization to conduct a remote access search or seizure. The Council believes, however, that these questions can and will be addressed by the courts in due course. The Advisory Committee has explicitly recognized this gap—and the need for the courts to fill it—in the comments to the proposed rule.

* * *

In conclusion, the Federal Bar Council supports the proposed amendments to Federal Rules of Criminal Procedure 4 and 41, and believes that they effectively and fairly address the issues presented by the current versions of the rules as discussed above. We recommend that the Advisory Committee solicit the support approval of the proposed amendments from the Committee on Rules of Practice and Procedure.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8fbv-4a8l
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0016](#)

Comment from Nathan Freed Wessler, on behalf of the American Civil Liberties Union (4/04/2014)

Submitter Information

Name: Nathan Freed Wessler

Organization: American Civil Liberties Union

General Comment

See Attached

Attachments

2014-04-04-ACLU Comments re Rule 41



MEMORANDUM

To: Members of the Advisory Committee on Criminal Rules
From: American Civil Liberties Union
Date: April 4, 2014
Re: ACLU Comment on the Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media

The American Civil Liberties Union writes to offer its perspective on the proposed amendment to Rule 41 concerning remote searches of electronic storage media. The Rule 41 Subcommittee approved the proposal (over a dissenting vote) on March 12, 2014, and forwarded it to the Advisory Committee on Criminal Rules (“Advisory Committee”) in a March 17, 2014, memorandum. The proposal is on the agenda for consideration at the Advisory Committee’s April 7–8, 2014, public meeting.

The proposed amendment would significantly expand the government’s authority to conduct remote searches of electronic storage media. Those searches raise serious Fourth Amendment questions. It would also expand the government’s power to engage in computer hacking in the course of criminal investigations, including through the use of malware and other techniques that pose a risk to internet security and that raise Fourth Amendment and policy concerns. In light of these concerns, the ACLU recommends that the Advisory Committee exercise extreme caution before granting the government new authority to remotely search individuals’ electronic data.

Because of the importance of these issues, the ACLU submits these initial comments in advance of the April meeting. Should the proposal be approved by the Advisory Committee and published for public comment, the ACLU expects to submit more detailed comments at that time.

I. Summary of Proposed Amendment to Rule 41

The proposed amendment, approved by the Rule 41 Subcommittee upon the recommendation of the Department of Justice (“DOJ”), would create a new exception to the territoriality requirement of Rule 41. Rule 41 currently provides that “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.**” Fed. R. Crim. P. 41(b)(1) (emphasis added). This territoriality limitation is subject to several narrow exceptions. *See id.* 41(b)(2)–(5).

The proposed amendment would add a new exception to the general rule that magistrate judges may grant warrants for searches only within their district: “(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 electronically stored information located within or outside that district.” Advisory Comm. on Criminal Rules, Materials for April 7–8, 2014 Meeting 165 (“Advisory Committee Materials”).¹ The proposal would also add language to Rule 41’s notice requirement, providing that for remote access searches, law enforcement “must make reasonable efforts to serve a copy [of the warrant] on the person whose property was searched or whose information was seized. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.” *Id.* at 166.

The Department of Justice asserts that it needs this expanded authority for three primary reasons:

- 1) to enable investigators to obtain warrants where the location of the computer to be searched is unknown, including where a suspect is using anonymization tools like Tor or other proxy services to mask his or her internet protocol (“IP”) address and other identifying information;
- 2) to enable investigators to obtain warrants to search Internet-connected computers in many districts simultaneously when those computers are being used as part of “complex criminal schemes.” As an example, DOJ describes crimes involving “the surreptitious infection of multiple computers with malicious software that makes them part of a ‘botnet,’” where investigating and addressing the threat posed by the botnet may involve law enforcement action in many judicial districts simultaneously; and
- 3) to enable investigators who obtain a warrant to search a physical computer in a particular location to also use that same warrant to search information that is accessible from that computer but stored remotely in another district, such as information stored on cloud-based services (e.g., Dropbox or Amazon Cloud Drive) or web-based email (e.g., Gmail or Yahoo! Mail).

Advisory Committee Materials 172–73, 261.

In response to DOJ’s proposal, one member of the Subcommittee, Professor Orin Kerr, offered a more limited amendment, intended to provide authority to search where the location of the target computer is unknown, but not to conduct remote searches of computers or servers whose location is known or can reasonably be ascertained. Professor Kerr’s proposal reads:

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant authorizing remote access of electronic storage media to obtain electronically stored information **if**

¹ Available at <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf>.

the district (if any) in which the electronic storage media is located cannot reasonably be ascertained.

Advisory Committee Materials 241. The Subcommittee did not adopt this language.

II. Remote Searches of Cloud Data Pose Fourth Amendment, Statutory, and Policy Problems

Gone are the days when all or most of a person's electronic files were stored on her own computer. Increasingly, people and businesses store large amounts of data on servers owned by third-party companies that are remotely accessible via the internet.² This is known as "cloud" storage. Under current law, if law enforcement wishes to search data stored on the cloud it must obtain an order or warrant pursuant to the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2703.³ A warrant issued under ECPA and Fed. R. Crim. P. 41 must demonstrate probable cause justifying search of the data held by the third-party company, and must be served on the company so that its employees may produce the requested data to the government. *See Warshak*, 631 F.3d at 288.

The government's proposed amendment would create a new mechanism for accessing cloud-based data, whereby police could obtain a warrant to search a suspect's physical computer, and then use that computer to directly access, search, and copy files stored remotely on cloud-based services. This raises significant and troubling Fourth Amendment and policy concerns, some of which were highlighted by Professor Kerr in his memoranda, and some of which have not yet been presented to the Advisory Committee:

Forum Shopping and Jurisdictional Overreach: Except in limited circumstances, magistrate judges are empowered to issue search warrants for "property located within the district" in which they serve. The proposed amendment would expand the power of magistrate judges to grant search warrants in two ways: it would permit a magistrate judge "in any district where activities related to a crime may have occurred" to issue a remote access search warrant; and it would allow such warrants to authorize searches for data or files stored "within or outside that district." These changes, taken together, create opportunities for forum shopping and raise federal jurisdictional concerns.

The phrase "in any district where activities related to a crime may have occurred" radically expands the fora in which the government can apply for a warrant. Most federal criminal investigations and prosecutions rely for their federal jurisdiction on the crime's effect

² *See, e.g.*, Quentin Hardy, *IBM Plans Big Spending for the Cloud*, N.Y. Times, Jan. 16, 2014, <http://bits.blogs.nytimes.com/2014/01/16/ibm-plans-big-spending-for-the-cloud/>; Tim Bradshaw, *Dropbox Faces Growing Competition in Cloud Storage Wars*, Fin. Times, Aug. 18, 2013, <http://www.ft.com/cms/s/2/88be965e-edd8-11e2-816e-00144feabdc0.html>.

³ Under ECPA, access to certain stored content information requires a warrant. 18 U.S.C. § 2703(a); *see also United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (requiring warrant for all remotely stored email content). Other information about stored electronic communications and records, not including their content, may be obtained with a court order issued on a relevance and materiality standard. 18 U.S.C. § 2703(c)-(d).

on, relation to, or involvement in interstate commerce.⁴ This means that in most federal criminal investigations law enforcement agencies will be able to identify multiple districts where “activities related to the crime may have occurred.” Further, internet-enabled or -connected crimes will frequently involve conduct in multiple districts; in many cases, the government will be able to choose among dozens of districts in which to seek a warrant.

Suppose an internet fraudster sends unsolicited email to people in two dozen districts. Perhaps those emails travel through servers in another dozen districts on their way across the Internet.⁵ And suppose the suspect purchased his computer from a vendor in yet another district, and uses a cloud-based email service to generate the messages, the servers of which are spread across an additional five districts. The government would apparently be able to select among any of those 42 districts in which to apply for a warrant. This raises familiar forum-shopping concerns,⁶ permitting the government to choose the district in which it expects to receive the least skeptical judicial reception.

It also raises jurisdictional issues. There is at least a serious question as to whether a court in a district where a bare minimum of “activities related to a crime” occurred—or especially where activities related to a crime merely “*may* have occurred”—has authority to issue an extraterritorial warrant, especially one that authorizes searches nationwide. *See Weinberg v. United States*, 126 F.2d 1004, 1006 (2d Cir. 1942) (“[E]ven though the statute, 18 U.S.C.A. § 611, authorizing the issuance of search warrants, does not contain an express limitation of the district court’s power to its own district, that seems clearly understood, in view of the constitutional provisions and the general rule of territorial limitation. We, therefore, cannot hold silence to mean that search warrants may be used anywhere in the country.”). The proposed rule would be convenient to the government, but at the cost of allowing a single judge to authorize searches in multiple districts, some at great distance, likely without regard to any differences in binding circuit law at the various sites of those searches.⁷ Unlike terrorism investigations (for which out-of-district search warrants are currently authorized, Fed. R. Crim. P. 41(b)(3)), remote searches of electronic storage media are likely to occur with great frequency. The proposed rule is not a minor procedural update; it is a major reorganization of judicial power.

Circumvention of ECPA: The Electronic Communications Privacy Act provides several important protections that will be evaded under the proposed amendment. First, to obtain a

⁴ *See* 1 Wayne R. LaFare et al., Crim. Proc. § 1.2(c) (3d ed.) (“[T]he dramatic expansion of federal criminal law was based primarily on Congress’ authority under the Commerce Clause . . .”).

⁵ *See* World Science Festival, *There and Back Again: A Packet’s Tale – How Does the Internet Work?*, YouTube (June 6, 2012), <https://www.youtube.com/watch?v=WwyJGzZmBe8>; Glenn Fleishman, *To Sail Data Across the Web, Computers Seek the Best Routes*, N.Y. Times, Dec. 31, 1998, <http://www.nytimes.com/1998/12/31/technology/to-sail-data-across-the-web-computers-seek-the-best-routes.html>.

⁶ *See, e.g., United States v. Bailey*, 193 F. Supp. 2d 1044, 1051 (S.D. Ohio 2002) (“Courts should uniformly discourage forum shopping or judge selection.”); *see also* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 Miss. L.J. 85, 102 (2005).

⁷ For example, the Sixth Circuit is the only court of appeals to have definitively ruled that there is a reasonable expectation of privacy in the contents of email communications stored on an email provider’s servers. *Warshak*, 631 F.3d at 288. The Ninth Circuit has explained the need for particularly robust procedures for regulating computer searches. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1175–77 (9th Cir. 2010). What happens when a magistrate judge in Louisiana authorizes remote searches within the Sixth, Ninth, and other circuits that violate some circuits’ law but not others? When a suppression motion is brought, whose law governs?

warrant for stored content (as opposed to non-content information) under ECPA, the government must demonstrate probable cause as to evidence held by each service provider whose data it seeks to search. The proposed amendment would permit the government to make a single showing of probable cause—that evidence of the crime will be found on a physical computer and any cloud services to which it is connected—and then use that showing to search as many cloud storage accounts as can be accessed from the computer. Thus, a single warrant could result in police searching a suspect’s computer hard drive, and then embarking on a fishing expedition through her work emails stored on her employer’s email server, her personal emails on Gmail or Outlook, her word processing files stored on Dropbox, her vacation photos on Flickr, her private conversations with family members on Facebook, and a log of her personal budget and purchases on Mint.com. Unless police know what cloud-based services a person uses before searching her computer, they will be unlikely to demonstrate probable cause as to each one when applying for a remote access warrant. A warrant granting blanket authority to search any and all of these services—without even knowing which ones a suspect uses or which can be easily accessed from her computer—would raise particularity problems as well.

Second, under ECPA the government must serve a warrant on each service provider, thus providing them with notice that their servers will be searched. This allows the companies to protect both their own legal interests and those of their customers. Service providers are able to subject warrants to scrutiny, and to challenge the government if a warrant seeks information that appears too broad in scope, too vaguely defined, or is otherwise deficient.⁸ Given the vast quantities of data stored on cloud services, much of which will be irrelevant to most investigations, these protections are an important aspect of ensuring compliance with the Fourth Amendment. Most individuals served with a search warrant lack the legal expertise or institutional clout to challenge the terms of the warrant before its execution.⁹ And for delayed notice searches, no challenge is even theoretically possible.

Finally, the government asserts that the proposed amendment is needed to prevent cloud-stored documents from being deleted or encrypted after a physical computer is searched but before the government can obtain an ECPA warrant directed at the cloud storage provider.¹⁰ This problem can be avoided with the simple expedient of a preservation request directed at the provider. 18 U.S.C. § 2703(f). Such requests can be sent immediately and unilaterally by law

⁸ See Google, *Way of a Warrant*, YouTube (Mar. 17, 2014), <https://www.youtube.com/watch?v=MeKKHxcJfh0> (explaining that Google employees scrutinize warrants to catch errors and identify overly vague or broad requests, and that they ask investigators to narrow the scope of warrants when appropriate); Google, Transparency Report, Requests for User Information, Legal Process, http://www.google.com/transparencyreport/userdatarequests/legalprocess/#what_types_of_legal (“If we believe a request is overly broad, we’ll seek to narrow it.”). See also *Permanent Provisions of the Patriot Act: Hearing Before the Subcomm. On Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary* 112th Cong. 69 (2011) (statement of Todd M. Hinnen, Acting Assistant Attorney Gen. for Nat’l Sec.), available at http://judiciary.house.gov/_files/hearings/printers/112th/112-15_65486.PDF (after congressman asks Acting Assistant AG Hinnen “why would [a service provider] . . . have an incentive to hire lawyers to protect [their subscribers’ privacy] rights?,” Mr. Hinnen responded that “telecommunication providers and Internet service providers take the privacy of their customers and subscribers very seriously and I think are often an effective proxy for defending those rights”).

⁹ This is not to say that only service providers should receive notice. Rather, notice to both service providers and users is crucial to protect Fourth Amendment rights.

¹⁰ Advisory Committee Materials 261.

enforcement, without the need to seek judicial approval, and require providers to preserve relevant records and evidence pending issuance of a warrant. The government ignores this power in arguing that ECPA warrants are insufficient.

Use of a Single Warrant to Search Multiple Locations Owned or Controlled by Other Parties: The proposed amendment would allow police to remotely search multiple hard drives, servers, and web-based accounts under a single warrant, without reason to believe that all locations to be searched are under the investigative target’s exclusive control. Courts are particularly skeptical of warrants authorizing searches of multiple locations not owned by the same person.¹¹ This skepticism is partly animated by the concern that the use of multiple-location search warrants could divest one or another occupant of individually held Fourth Amendment rights. In the context of physical searches, “[t]he general rule is that a warrant for a building that has multiple units must specify the individual unit that is the subject of the search to satisfy the particularity requirement.”¹² The same concerns and rules should apply when police search digital “occupancies.”

Remote access searches can raise concerns about joint and divided ownership in several ways. First, physical computers may be shared, but may provide access to remotely stored data that is not. For example, all members of a family might use the same desktop computer. But the cloud storage accounts directly accessible from it might belong exclusively to different people: the Dropbox account might be registered to one family member, the Facebook account to another, the Flickr photo archiving account to a third, and the Yahoo! email account to a fourth. A warrant authorizing a search for evidence of one family member’s crime, but permitting access to any remote data accessible through the suspect’s shared computer, would result in searches of other people’s digital data without probable cause.

Second, remote storage accounts may themselves be shared. A wife and husband may share a joint cloud-based email account; artists or entrepreneurs collaborating on a project may share a cloud storage account to facilitate their joint work. Courts recognize the reasonable expectation of privacy individuals may have in shared places, and doctrines of standing and consent accommodate different interests in the use, possession, and ownership of jointly controlled property.¹³

¹¹ “[I]n the case of multi-location search warrants, the magistrate must be careful to evaluate each location separately. ‘A search warrant designating more than one person or place to be searched must contain sufficient probable cause to justify its issuance as to each person or place named therein.’” *Greenstreet v. Cnty. of San Bernardino*, 41 F.3d 1306, 1309 (9th Cir. 1994) (quoting *People v. Easley*, 671 P.2d 813, 820 (Cal. 1983)).

¹² Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 *Stan. L. Rev.* 1005, 1045 n.173 (2010) (citing *Jacobs v. City of Chicago*, 215 F.3d 758, 767 (7th Cir. 2000)). See also *United States v. Hinton*, 219 F.2d 324, 325–26 (7th Cir. 1955) (“For purposes of satisfying the Fourth Amendment, searching two or more apartments in the same building is no different than searching two or more completely separate houses.”); *United States v. Clark*, 638 F.3d 89, 98 (2d Cir. 2011) (warrant defective where issuing judge was not informed of building’s size or number of residential units and was incapable of making probable cause determination of defendant’s control of entire multi-family building).

¹³ See, e.g., *State v. Lacey*, 204 P.3d 1192, 1205–06 (Mont. 2009) (discussing scope of third-party consent to search shared computer); *United States v. Elliott*, 50 F.3d 180, 186 (2d Cir. 1995) (discussing scope of landlord consent to searches of leased and unleased units).

Third, a service provider will be the owner or lessee of the servers on which a user's data is remotely stored, and may have rights to access accounts and files for some purposes and not others. *See Warshak*, 631 F.3d at 287 (discussing email service provider's limited right to access user's email account). A remote access search not involving notice to the service provider or a specific showing of probable cause may violate the provider's rights.

In order to avoid authorizing searches that violate third parties' Fourth Amendment rights, magistrate judges must determine whether a suspect's linked Gmail, Google Docs, and Google+ accounts are under another person or entity's exclusive or shared use or control. In many circumstances, however, magistrate judges will not be capable of evaluating digital "occupancy" based on the information provided by the government, because the government will not yet have accessed the computer from which it will learn about the existence and nature of remote storage accounts. Authorizing the use of a single search warrant to gain access to multiple computers or online accounts in this circumstance could infringe on individuals' substantive Fourth Amendment rights. As the number of files and locations subject to a single search warrant increases, so too does the probability that privacy rights of people other than the target of the search will be affected.

Particularity Concerns: Although the proposed Committee Note seeks to avoid consideration of the amendment's interaction with the Fourth Amendment's particularity requirement, that issue should be addressed now because the particularity problems likely to be raised by remote access search warrants are entirely predictable. Law enforcement agents may not, and in many cases will not, know ahead of time which cloud services a suspect uses, so warrants will be sought for authority to search any cloud storage service to which the computer is connected. Such authority has little analogue in the context of physical searches. It would be akin to a warrant authorizing the search of a particular house, and also any other building that can be accessed using keys found in the house. Without describing with particularity the places to be searched and demonstrating probable cause as to each one, remote access warrants will violate the Fourth Amendment.

Moreover, some kinds of cloud storage services might be incapable of holding evidence of the crime under investigation. A photo account on Flickr or Picasa is unlikely to contain a spreadsheet proving tax fraud. A remote music storage service will not likely contain evidence of purse snatching. But without knowing ahead of time which cloud services a person uses and which are accessible from their computer, the government cannot describe with particularity the places to be searched, nor can it provide probable cause as to each service. A blanket authority to search "any remote storage services likely to contain evidence of the crime" cannot solve these problems because it would not meaningfully cabin an officer's discretion. A warrant application must describe, and a warrant must specify, the places to be searched. Given the tremendous storage capacity of cloud storage services—more like a warehouse than a filing cabinet or home library¹⁴—the failure to appropriately limit remote access warrants will result in unconstitutional searches of staggering quantities of data.

¹⁴ One gigabyte of data is, on average, the equivalent of 64,782 pages of Microsoft Word documents. LexisNexis Discovery Services, *How Many Pages in a Gigabyte?* (2007), http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitepapers/adi_fs_pagesinagigabyte.pdf. Dropbox currently offers accounts with 100 gigabytes of storage space for \$9.99 per month. Dropbox, *Choose Your Dropbox*

First Amendment: Authorizing a new, expansive power to search through an individual’s private email correspondences, Facebook messages, and Flickr or Dropbox accounts also raises profound First Amendment concerns. Individuals have a right to engage in expressive and associational activities in private, and government intrusions into that privacy trigger heightened scrutiny.

Electronic diaries stored on the cloud, lists of books ordered from Amazon.com, and a multitude of other remotely stored information can reveal an individual’s secret thoughts, hopes, and fears. To access these private, protected records, the government must demonstrate a compelling need to obtain the material, and a substantial relationship between the investigation and the information it seeks.¹⁵

Private social networking information, such as from Facebook and Google+, can also disclose an individual’s most significant private relationships—political, personal, or intimate—and the nature and intensity of those relationships. The First Amendment protects these associations from compelled disclosure, both because they are necessary to other associational and expressive activities and as an end in themselves.¹⁶

Technological improvements will continue to expand the already vast quantities of expressive and associational information that can be stored in the cloud. The proposed amendments will increase the risk of abuses and the chilling of First Amendment-protected activities.

Remote Access Searches Can Implicate the Privacy Rights of Many Innocent Third Parties: Electronic storage media remotely accessible from a physical computer are not limited to cloud storage accounts containing just a suspect’s files. In many cases, remotely accessible servers will contain sensitive data about or belonging to numerous other persons as well. For example, a doctor’s home computer may be connected to her patient files stored electronically on a remote server.¹⁷ Patients have a reasonable expectation of privacy in those files,¹⁸ and in most

Plan, <https://www.dropbox.com/pricing>. At the equivalent of 6,478,200 printed pages, this would fill more than 430 meters of shelf space. See Lynn Neary, *Printing Wikipedia Would Take 1 Million Pages, But That’s Sort of the Point*, Nat’l Pub. Radio, Mar. 30, 2014, <http://www.npr.org/blogs/alltechconsidered/2014/03/27/295262783/printing-wikipedia-would-take-1-million-pages-but-thats-sort-of-the-point>.

¹⁵ See, e.g., *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*, 706 F. Supp. 2d 11, 17 (D.D.C. 2009) (quashing subpoena for company records regarding sexually expressive films because customers’ “right to receive ideas” outweighed prosecutorial interests); see also *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963) (“[I]t is an essential prerequisite to the validity of an investigation which intrudes into the area of constitutionally protected rights of speech, press, association and petition that the State convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest.”).

¹⁶ See *NAACP v. Alabama ex. rel. Patterson*, 357 U.S. 449, 462 (1958) (observing that the “inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs”); *Griswold v. Connecticut*, 381 U.S. 479, 484, 486 (1965).

¹⁷ See, e.g., Press Release, U.S. Dep’t of Health & Human Servs., *Doctors and Hospitals’ Use of Health IT More than Doubles Since 2012* (May 22, 2013), <http://www.hhs.gov/news/press/2013pres/05/20130522a.html> (“HHS has met and exceeded its goal for 50 percent of doctor offices and 80 percent of eligible hospitals to have [electronic health records] by the end of 2013.”).

states they are protected by privilege.¹⁹ Searches of computers owned by lawyers, mental health professionals, and accountants would raise similar concerns. Likewise, a system administrator for a company's cloud-based email and file storage systems may have administrator credentials and login information for the accounts of every employee, including sensitive, private, and perhaps privileged data. Prior to the advent of widespread and large-capacity remote storage, these sensitive files would have been kept at an office or other secure physical storage location, and would have required a separate showing of probable cause and separate warrant to search. The ease with which remote searches can implicate these private third-party files creates new and difficult problems.

III. Zero-Day Exploits and Malware

The proposed amendment would enable the government to use sophisticated remote hacking techniques—malware and so-called “zero-day” exploits—to identify and search computers that are using anonymization tools like the Tor network. Such techniques could also be used to collect private information from computers whose location is known. These techniques are technically complex, and raise significant policy and Fourth Amendment concerns. Their expanded use should not lightly be authorized.

A. Technical Description of Malware and Zero-Day Exploits

Government agencies seeking to “remotely search” a computer or mobile phone are seeking information that is neither published online, nor otherwise available to a member of the public.²⁰ In order to extract such information from a computer that they neither control nor have physical access to, they must deliver specific computer code to the device and cause that code to run.

In some cases, it may be possible to use trickery (a technique that security researchers generally refer to as “social engineering”) in order to get the owner or operator of the computer to take an action that will cause this code to run. For example, law enforcement agents may send an email to a target with an attachment that looks to be an image file, but is in fact a specially designed program (“malware”) that will covertly install itself on the target's computer and then collect data.²¹

¹⁸ *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001); *Or. Prescription Drug Monitoring Program v. U.S. Drug Enforcement Admin.* (“*Oregon PDMP*”), No. 3:12-CV-02023-HA, 2014 WL 562938, at *7 (D. Or. Feb. 11, 2014).

¹⁹ *See, e.g.*, Cal. Evid. Code §§ 900–1007; Fla. Stat. Ann. § 456.057.

²⁰ If the information were available online, or could be obtained by any member of the public without exceeding authorized access to a computer, the government would not need a search warrant.

²¹ “The malware appears on a victim's desktop as ‘exe.Rajab1.jpg’ (for example), along with the default Windows icon for a picture file without thumbnail. But, when the UTF-8 based filename is displayed in ANSI, the name is displayed as ‘gpj.1bajaR.exe’. Believing that they are opening a harmless ‘.jpg’, victims are instead tricked into running an executable ‘.exe’ file. Upon execution these files install a multi-featured trojan on the victim's computer. This malware provides the attacker with clandestine remote access to the victim's machine as well as comprehensive data harvesting and exfiltration capabilities.” Morgan Marquis-Boire, *From Bahrain with Love: FinFisher's Spy Kit Exposed?* 3 (2012), available at <https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/> (describing the method of infection of surveillance software used by the Bahraini government against activists).

U.S. law enforcement agencies are not the only actors seeking to use social engineering to deliver malicious software onto people's computers. This technique is also widely used by criminals and foreign governments, who have used it to hack into the computers of U.S. government agencies, consumers, and major U.S. companies, including Microsoft,²² RSA,²³ Apple, and Amazon.²⁴ It is for this very reason that cyber security education efforts stress the importance of not clicking on unknown email attachments or suspicious-looking links.²⁵

Social engineering will not always work, particularly against targets that are following prudent cyber security warnings about email attachments and suspicious web links. In such cases, law enforcement agencies seeking to install or execute surveillance software on the computers of targets will need to use an alternate delivery technique that does not require the user to install or execute the code.²⁶

It is possible to run code on a computer or mobile device without the knowledge or assistance of the person operating that device. However, this generally requires the exploitation of security vulnerabilities in the software running on that device. For example, by exploiting vulnerabilities in a web browser, it is possible to cause a computer to download and install software when it visits a website,²⁷ without requiring that the target take any additional actions.

²² See Tom Warren, *Microsoft Confirms Syrian Electronic Army Hacked into Employee Email Accounts*, The Verge (Jan. 15, 2009), <http://www.theverge.com/2014/1/15/5312798/microsoft-email-accounts-hacked-syrian-electronic-army> (describing a successful social engineering attack in which the Syrian Electronic Army was able to extract sensitive law enforcement surveillance documents from Microsoft employees).

²³ Riva Richmond, *The RSA Hack: How They Did It*, N.Y. Times (Apr. 2, 2011), <http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/>.

²⁴ Mat Honan, *How Apple and Amazon Security Flaws Led to My Epic Hacking*, Wired (Aug. 6, 2012), <http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>.

²⁵ See Dep't of Homeland Sec., *Cyber Tips for Older Americans*, http://www.dhs.gov/sites/default/files/publications/Cybersecurity%20for%20Older%20Americans_0.pdf; New York Governor's Office of Employee Relations, *Personal Security Responsibilities*, http://www.goer.ny.gov/training_development/resources/hipaa/helpFiles/PersonalSecurityResponsibilities.htm ("Do not open attachments from the Internet or from people you do not know. Do not open any suspicious attachments."); Univ. of Va. at Wise, *Policies & Security: Secure Computing Notices*, <http://www.wise.virginia.edu/oit/SecureComputing/notices> ("Do NOT click on web address links included in email messages unless you are sure they connect to trusted web sites. It is safer to either key a known web site address directly into the address line in your browser or to use the search feature of your browser to find the website.").

²⁶ See *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. On Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary* 112th Cong. (2011) (statement of Valerie Caproni, General Counsel, FBI), available at <http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg64581/html/CHRG-112hhrg64581.htm> ("There will always be criminals, terrorists, and spies who use very sophisticated means of communications that are going to create very specific problems for law enforcement. We understand that there are times when you need to design an individual solution for an individual target, and that is what those targets present.").

²⁷ This website must be under the control of the attacker, or, if the attacker is able to monitor the internet connection of the target, any website that the target visits can be used to initiate a "drive by" installation. See Gamma Group, *Remote Monitoring & Infection Solutions: FINFLY ISP* (Wikileaks.org), https://wikileaks.org/spyfiles/files/0/297_GAMMA-201110-FinFly_ISP.pdf (product brochure for a government-grade surveillance appliance which can "be integrated into an ISP's Access and/or Core Network to remotely install the Remote Monitoring Solution on selected Target Systems. . . . FinFly ISP is able to infect Files that are downloaded by the Target on-the-fly or infect the Target by sending fake Software Updates for popular Software. The new release now integrates Gamma's powerful remote infection application FinFly Web to infect Targets on-the-fly by just visiting any website.").

This technique is known generally as a “drive by download,”²⁸ and is a technique that is used by hackers, criminals, and governments (in the United States and elsewhere) to deliver malware.²⁹

In order to exploit a security vulnerability in the software on a target’s computer, that computer must either be running out-of-date software with a known software vulnerability, or the hacker must know of a vulnerability for which no update exists. As such, targets who regularly patch their software (or use software that automatically updates) may be much harder to compromise with malware. In order to hack into such targets, law enforcement and intelligence agencies are increasingly seeking to purchase or discover so called zero-day (or 0-day) software exploits,³⁰ that is, special software that exploits vulnerabilities in software that are not known to the manufacturer of the software program, and thus, for which no software update exists. Zero-day exploits are extremely valuable, because there is no defense against them.³¹

U.S. law enforcement and intelligence agencies have, in recent years, increasingly turned to zero-day exploits in order to gain access to the computers of high value targets.³² This has in turn fueled a largely unregulated market for zero-day exploits, in which government agencies are active and are often the highest bidder.³³

²⁸ See Long Lu et al., *BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections*, Proceedings of the 17th ACM Conference on Computer and Communications Security (Oct. 2010), available at <http://www.blade-defender.net/BLADE-ACM-CCS-2010.pdf> (“Web-based surreptitious malware infections (i.e., drive-by downloads) have become the primary method used to deliver malicious software onto computers across the Internet.”).

²⁹ See Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired (Sept. 13, 2013, 4:17 PM), <http://www.wired.com/2013/09/freedom-hosting-fbi/>; Dan Goodin, *Attackers Wield Firefox Exploit to Uncloak Anonymous Tor Users*, ArsTechnica (Aug. 5, 2013, 1:02 PM), <http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/> (“A piece of malicious JavaScript was found embedded in webpages delivered by Freedom Hosting, a provider of ‘hidden services’ that are available only to people surfing anonymously through Tor. The attack code exploited a memory-management vulnerability, forcing Firefox to send a unique identifier to a third-party server using a public IP address that can be linked back to the person’s ISP.”).

³⁰ See Leyla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*, Proceedings of the 2012 ACM Conference on Computer and Communications Security (Oct. 2012), available at http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf (“A zero-day attack is a cyber attack exploiting a vulnerability that has not been disclosed publicly. There is almost no defense against a zero-day attack: while the vulnerability remains unknown, the software affected cannot be patched and anti-virus products cannot detect the attack through signature-based scanning.”).

³¹ *The Digital Arms Trade*, Econ., Mar. 30, 2013, <http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade> (“It is a type of software sometimes described as ‘absolute power’ or ‘God’. Small wonder its sales are growing.”).

³² See Craig Timber & Ellen Nakashima, *FBI’s Search for ‘Mo,’ Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post, Dec. 6, 2013, http://www.washingtonpost.com/business/technology/fbi-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html (describing the use of a zero day exploit by the FBI to take over webcams without the indicator light turning on). See also Liam Murchu, *Stuxnet Using Three Additional Zero-Day Vulnerabilities*, Symantec Official Blog (Jan. 23, 2014), <http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities> (describing the use of zero days in Stuxnet, a piece of malware attributed to the US and Israeli governments); David Sanger, *Obama Orders Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times, June 1, 2012, <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all>.

³³ See, e.g., *The Digital Arms Trade*, The Economist, Mar. 30, 2013, <http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems->

Governments spend a lot of money to acquire zero-day exploits. Although there is little verifiable data about the market for such exploits, anecdotal reports suggest that the cost of exploits can be in the hundreds of thousands of dollars, or, in some cases, up to a million dollars.³⁴ These vulnerabilities are their most effective when no one else knows about them, so rather than alerting the companies whose software can be exploited, governments, including the United States, quietly exploit them.³⁵ Quite simply, governments that rely on zero-day exploits have prioritized offense over defense.

B. Concerns Raised by Use of Zero-Day Exploits and Malware

Although zero-days undoubtedly make it easier to deliver malware to targets and to gain access to difficult-to-penetrate systems, there are significant collateral costs associated with the purchase and use of zero-days by governments. That is, by exploiting these vulnerabilities rather than notifying the companies responsible for the software, governments are putting their own citizens at risk.³⁶ Several senior ex-U.S. government officials have acknowledged these risks, including ex-NSA/CIA director Michael Hayden,³⁷ and ex-‘cyber czars’ Howard Schmidt³⁸ and Richard Clarke.³⁹

digital-arms-trade (“Other reputable customers, such as Western intelligence agencies, often pay higher prices. Mr Lindelauf reckons that America’s spies spend the most on exploits. Vupen and other exploit vendors decline to name their clients. However, brisk sales are partly driven by demand from defence contractors that see cyberspace as a “new battle domain”, says Matt Georgy, head of technology at Endgame, a Maryland firm that sells most of its best exploits for between \$100,000 and \$200,000.”); Nicole Perloth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times, July 13, 2013, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=1&_r=1 (“But increasingly the businesses are being outbid by countries with the goal of exploiting the flaws in pursuit of the kind of success. . . that the United States and Israel achieved. . .”); Joseph Menn, *Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback*, Reuters, May 10, 2013, <http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510> (“Even as the U.S. government confronts rival powers over widespread Internet espionage, it has become the biggest buyer in a burgeoning gray market where hackers and security firms sell tools for breaking into computers.”).

³⁴ See Nicole Perloth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times, July 13, 2013, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=1&_r=1 (describing hackers searching for “secret flaws in computer code that governments pay hundreds of thousands of dollars to learn about and exploit”).

³⁵ Joseph Menn, *U.S. Cyberwar Strategy Stokes Fear of Blowback*, Reuters, May 10, 2013, <http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510> (“The core problem: Spy tools and cyber-weapons rely on vulnerabilities in existing software programs, and these hacks would be much less useful to the government if the flaws were exposed through public warnings. So the more the government spends on offensive techniques, the greater its interest in making sure that security holes in widely used software remain unrepaired.”).

³⁶ *Id.* (“The strategy is spurring concern in the technology industry and intelligence community that Washington is in effect encouraging hacking and failing to disclose to software companies and customers the vulnerabilities exploited by the purchased hacks.”).

³⁷ *Id.* (“Acknowledging the strategic trade-offs, former NSA director Michael Hayden said: ‘There has been a traditional calculus between protecting your offensive capability and strengthening your defense. It might be time now to readdress that at an important policy level, given how much we are suffering.’”).

³⁸ *Id.* (“It’s pretty naïve to believe that with a newly discovered zero-day, you are the only one in the world that’s discovered it,” said Schmidt, who retired last year as the White House cybersecurity coordinator. ‘Whether it’s another government, a researcher or someone else who sells exploits, you may have it by yourself for a few hours or for a few days, but you sure are not going to have it alone for long.’”) See also Perloth & Sanger, *supra* note 1

Indeed, at a time when cyberattacks are, according to government officials, one of the biggest threats faced by this country,⁴⁰ the collateral damage associated with exploiting, rather than fixing, security vulnerabilities is the topic of considerable debate. For example, the President’s NSA Review Group recently observed that “[a] vulnerability that can be exploited on the battlefield can also be exploited elsewhere”⁴¹ and recommended that “US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks.”⁴² Moreover, “in almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities—‘patching’ them—strengthens the security of US Government, critical infrastructure, and other computer systems.”⁴³

These issues are complicated and serious, and they raise both policy and constitutional concerns. Under the Fourth Amendment, use of zero-day exploits may constitute an unreasonable search. It is well established that some searches in the physical world are too intrusive, destructive, or dangerous to be reasonable. Surgically removing evidence from a suspect’s body,⁴⁴ using a powerful motorized battering ram to break into a residence,⁴⁵ and

(“Governments are starting to say, ‘In order to best protect my country, I need to find vulnerabilities in other countries,’ ” said Howard Schmidt, a former White House cybersecurity coordinator. “The problem is that we all fundamentally become less secure.”).

³⁹ Menn, *supra* (“Former White House cybersecurity advisors Howard Schmidt and Richard Clarke said in interviews that the government in this way has been putting too much emphasis on offensive capabilities that by their very nature depend on leaving U.S. business and consumers at risk. ‘If the U.S. government knows of a vulnerability that can be exploited, under normal circumstances, its first obligation is to tell U.S. users,’ Clarke said. ‘There is supposed to be some mechanism for deciding how they use the information, for offense or defense. But there isn’t.’”).

⁴⁰ James Clapper, the Director of National Intelligence, and James Comey, the Director of the FBI, have both told Congress that cyber-attacks are the most serious national security threat faced by the United States. See Jim Garamone, *Clapper Places Cyber at Top of Transnational Threat List*, Armed Forces Press Service, March 12, 2013, <http://www.defense.gov/news/newsarticle.aspx?id=119500>. See also Greg Miller, *FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered*, Wash. Post, November 14, 2013, http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html (“FBI Director James B. Comey testified Thursday that the risk of cyberattacks is likely to exceed the danger posed by al-Qaeda and other terrorist networks as the top national security threat to the United States and will become the dominant focus of law enforcement and intelligence services.”).

⁴¹ Review Grp. on Intelligence and Comm’n Techs., *Liberty and Security in a Changing World* 187 (2013), available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

⁴² *Id.* at 37, 219 (“We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called “Zero Day” attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.”).

⁴³ *Id.* at 220.

⁴⁴ *Winston v. Lee*, 470 U.S. 753, 759, 766–67 (1985) (holding that the health risks posed by the “compelled surgical intrusion into an individual’s body for evidence” make that search unreasonable under the Fourth Amendment); see also *Schmerber v. California*, 384 U.S. 757, 771–72 (1966) (requiring that a search involving drawing a suspect’s blood be “performed in a reasonable manner,” including that it be carried out by medical personnel in a medical

“employ[ing] a flashbang device [to enter a house] with full knowledge that it will ‘likely’ ignite accelerants and cause a fire”⁴⁶ have all been ruled unreasonable under the Fourth Amendment. Zero-day exploits may well pose analogous concerns. When the government unleashes zero-day exploits and malware, it will rarely be able to control who can intercept the code in transmission, whether it will reach its intended target, whether it will be copied and reused by others, and whether it will spread virally across the internet and cause damage to innocent persons and businesses.⁴⁷ These factors are relevant to individual warrant applications, but also to the Advisory Committee’s consideration of the proposed Rule amendment.

The issues described above are unavoidably complex. Before courts waded into the constitutional questions that the use of malware and zero-day exploits raise, it would be best for Congress to affirmatively address the wisdom and parameters of their use after informed public discussion. At a minimum, however, this Committee should seek comment from technical experts and from government agencies responsible for domestic cybersecurity, including the Federal Trade Commission and the Department of Homeland Security. The power the government seeks is weighty and risky, and this Committee’s consideration of the proposed amendment should proceed with due deliberation and care.

IV. Botnets

The government seeks authority to obtain warrants authorizing simultaneous remote access searches of hundreds or thousands of computers that have, unbeknownst to their owners, been enlisted into a botnet and used for allegedly criminal purposes. The ACLU is sympathetic to the goal of disabling botnets and strengthening the security of the Internet, but that goal can be accomplished with a far more modest modification of Rule 41. If the government is acting primarily in a cybersecurity capacity (analogous to the government’s public health function⁴⁸), rather than in a primarily law enforcement capacity, then Fourth Amendment concerns are less acute. *See Illinois v. Lidster*, 540 U.S. 419, 423 (2004) (discussing special needs doctrine). But if the government is engaged in searches of computers for “general ‘crime control’ purposes,” *id.*, Fourth Amendment concerns are at their zenith.

Even to the extent the government seeks to use remote access warrants only to disable botnets by identifying the command and control structure of the network and then distributing computer code that disinfects the controlled computers, there are still concerns. The techniques the government uses to disable the botnet matter. If the government wants authority to distribute

environment); *Rochin v. California*, 342 U.S. 165, 172 (1952) (conduct by agents trying to obtain swallowed evidence, including “the forcible extraction of [the defendant’s] stomach’s contents,” violates due process).

⁴⁵ *Langford v. Superior Ct. of L.A. Cnty.*, 729 P.2d 822, 827 (Cal. 1987) (holding that, because a motorized battering ram can cause “potential danger from collapse of building walls and ceilings or through rupture of utility lines,” which could cause fires that “could threaten the safety not only of occupants, but of entire neighborhoods,” “routine deployment of the ram to enter dwellings must be considered presumptively unreasonable unless authorized in advance by a neutral magistrate, and unless exigent circumstances develop at the time of entry”).

⁴⁶ *Bing ex rel. Bing v. City of Whitehall, Ohio*, 456 F.3d 555, 570 (6th Cir. 2006).

⁴⁷ Rachel King, *Stuxnet Infected Chevron’s IT Network*, Wall St. J., Nov. 8, 2012, <http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/>.

⁴⁸ *See* Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity* 10–14 (2011), available at <http://www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf>.

computer code to infected computers via remote access, it needs to specify to the magistrate judge the capabilities of that code, how it will be delivered, the risk of interception en route, and the risks of causing new damage. Only full disclosure of this type of information will enable a judge to accurately assess the likely effect of the technique on the rights of those whose computers will be targeted and others. The government also needs to propose, and judges need to adopt, robust minimization and notice procedures to mitigate the effects on innocent parties' privacy interests.

Other concerns are common to both law enforcement and cybersecurity activities. The government wants to be able to send to many hundreds or thousands of computers "remote network techniques" that will report back those computers' IP addresses, MAC addresses, and other unique identifiers. The government must explain whether it can be sure that the techniques will not target or search computers that are not part of the botnet. It must also explain in more detail the nature of the "unique identifiers" it seeks to collect. A computer may contain numerous pieces of data that constitute "unique identifiers," and the particularity and reasonableness requirements of the Fourth Amendment require that the information collected be precisely described and limited in scope. Further, an authorization to search thousands of computers to collect information from a large number of people may verge on a general warrant. The use of extra-district remote access warrants to investigate and combat botnets raises numerous questions that the government has not yet answered.

V. The Proposed Amendment Weakens Rule 41's Notice Requirement

The proposed amendment modifies Rule 41's notice requirement so that for remote access searches the government "must make reasonable efforts" to serve a copy of the warrant on the person whose property was searched or whose information was seized. This departs from the normal requirement that "[t]he officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person" subject to the search. Fed. R. Crim. P. 41(f)(1)(C). The proposed language clearly contemplates searches for which no notice can be provided. But failure to provide notice "casts strong doubt on [a warrant's] constitutional adequacy." *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (citing *Berger v. New York*, 388 U.S. 41, 60 (1967)). As the Ninth Circuit has explained,

[a] warrant [i]s constitutionally defective [if it] fail[s] to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. . . . We take this position because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed.

Id.; see also *United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) ("[I]f a delay in notice is to be allowed, the court should nonetheless require the officers to give the appropriate person notice of the search within a reasonable time after the covert entry."). Surreptitious entry into a

repository of a person's electronic files, containing digital analogues of her diaries, address books, letters, and photo albums, raises no less important concerns.

A second problem with the proposed amendment is that it will allow the government to provide notice to third-party service providers rather than to the actual target of the search in many cases, which all but defeats the purpose of the notice. Notice should be given to both.⁴⁹ The proposed language provides that “the officer must make reasonable efforts to serve a copy on the person whose property was searched **or** whose information was seized.” (Emphasis added). A reasonable interpretation of this language would allow the government to choose between providing notice to the third-party cloud storage provider (whose physical server was searched) *or* to the person whose information was seized. Service providers may fail to, or be ordered not to, provide their own notice to the target of the search upon receiving notice from the government. Thus, the target might never learn of the search, and therefore never be able to challenge its constitutionality. To avoid this problem, “or” should be replaced with “and.”

Finally, as explained by Professor Kerr, the proposed amendment will likely result in more delayed-notice searches.⁵⁰ Delayed notice may be permissible if it is of short duration and reviewed by a judge, but it has the potential to interfere with substantive Fourth Amendment rights if too heavily, widely, or extensively used.

VI. Professor Kerr's Counter-Proposal Does Not Address All of the ACLU's Concerns

Professor Kerr proposes to allow remote access warrants only when “the district (if any) in which the electronic storage media is located cannot reasonably be ascertained.” Although this narrows the scope of the government's remote search authority in a way that avoids some of the above concerns, it still poses problems. For example, under Professor Kerr's language, the government would still be able to obtain warrants to use malware, zero-day exploits, and other techniques that raise serious constitutional and policy questions.

Additionally, Professor Kerr's proposal can be interpreted to allow remote access searches of data stored on the cloud, even when the identity of the cloud service containing the data is known. This is because for many cloud storage services it is impossible to know where the data is physically located (in other words, on what server it resides). Many cloud storage providers distribute their servers among multiple locations, both within the United States and around the world. A digital file might be stored on any one of those servers, split up between servers, or redundantly stored on multiple servers simultaneously. A file stored on one server in California today might be automatically transferred to another server in North Carolina tomorrow. The storage location will be dictated by features of the provider's network architecture, the usage patterns and comparative loads on its servers, and other factors that are

⁴⁹ Although providing notice to the service provider is important (and compelled by ECPA and Rule 41, *see Application for Warrant for E-mail Account [redacted]@gmail.com Maintained on Computer Servers Operated by Google, Inc., Headquartered at 1600 Amphitheatre Parkway, Mountain View, CA*, No. 10-291-M-01, slip op. (D.D.C. Sept. 20, 2010), *available at* <http://www.crowell.com/files/Lamberth-Opinion.pdf>), it is not sufficient. Notice must be provided to the target of the search as well.

⁵⁰ Advisory Committee Materials 252.

both out of the control of users and unknowable to them. Providers do not typically disclose the physical location of the server on which any given file resides. The location of the server housing the data is likewise unknown, and probably unknowable, to law enforcement. Therefore, the district in which the electronic storage media is located cannot be reasonably ascertained, and a remote access warrant instead of an ECPA warrant could be used to conduct the search, with all of the attendant consequences described above.

VII. The Advisory Committee Should Fully Consider All the Implications of the Proposed Amendment Now, and Should Be Skeptical of its Wide Reach

The Advisory Committee should proceed with extreme caution before expanding the government's authority to conduct remote electronic searches. As explained above, the proposed amendment would significantly expand the government's authority to conduct searches that raise troubling Fourth Amendment, statutory, and policy questions.

A. The Proposed Amendment Expands the Government's Substantive Powers, and the Advisory Committee Should Grapple With Its Fourth Amendment Implications Now

The Federal Rules are limited to "regulat[ing] procedure." *Sibbach v. Wilson & Co.*, 312 U.S. 1, 13 (1941). They may not "abridge, enlarge or modify any substantive right." 28 U.S.C. § 2072(b). Although the proposed Committee Note purports to leave "constitutional questions" to be addressed in future case law,⁵¹ in practice the amendment will enlarge the government's substantive power to conduct searches. By radically expanding the circumstances in which a magistrate judge may approve a warrant to search and seize data on computers and servers located in distant districts, including searches using malware and other hacking techniques, the proposed amendment risks abridging Fourth Amendment rights and frustrating the purposes of ECPA.

But even if the Advisory Committee determines that the proposed amendment will "govern[] only 'the manner and the means' by which the litigants' rights are 'enforced,'" and will not "alter[] 'the rules of decision by which [the] court will adjudicate [those] rights,'"⁵² it should still be reticent to approve the amendment. The "constitutional questions" raised by the amendment include what limitations the particularity, probable cause, and reasonableness requirements of the Fourth Amendment impose on remote access searches. These will likely not be addressed by courts for years, if ever. Moreover, important policy questions involving cybersecurity and government exploitation of internet and software vulnerabilities are implicated, as are conflicts with the text and structure of ECPA. In order to prevent violations of the Fourth Amendment and an untoward expansion of government power, this Committee should grapple with these issues now. Alternatively, the Department of Justice should request the authority it seeks from Congress, so as to permit a public debate about the propriety of the intrusive techniques it proposes to use and about possible alternatives that Congress would be in a unique position to craft.

⁵¹ Advisory Committee Materials 166.

⁵² *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 407 (2010) (second and third alterations in original).

There are several reasons why courts are unlikely to address Fourth Amendment limits on remote access searches in the near future. For one, warrant applications are considered by judges *ex parte* and without adversarial argument. While magistrate judges are experienced in assessing general questions of particularity and probable cause in run-of-the-mill warrant applications, they are likely to be ill-equipped to provide robust review of applications for remote access warrants without adversarial briefing. Full appraisal of these applications requires technical expertise about electronic data storage issues, internet architecture, and cybersecurity. Applications that appear reasonable on their face in light of a magistrate judge’s limited technical understanding may in fact fail the particularity and reasonableness requirement upon closer study. But without detailed technical knowledge—or adversarial briefing explaining the issues—many of these concerns will go unnoticed and unaddressed.

Further, orders granting or denying warrants are rarely published and are usually sealed.⁵³ The likelihood of magistrate judges *sua sponte* publishing detailed opinions analyzing Fourth Amendment issues involved in electronic searches is particularly low when they are unable to independently identify the constitutional infirmities of the warrant application. Indeed, although the government has likely been seeking warrants to authorize remote access searches with some frequency,⁵⁴ there is only one published opinion of a magistrate judge grappling with the Fourth Amendment issues involved. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). There is no telling how long it will be until there is another.

Additionally, notice may be delayed for significant periods of time, thus forestalling the time when the target of a remote access search could challenge its constitutionality. *See* Fed. R. Crim. P. 41(f)(3); 18 U.S.C. § 3103a(b)–(c). And even when notice is given, *ex post* judicial review is limited by doctrines precluding or discouraging a ruling on the constitutionality of the government’s conduct. In criminal prosecutions, defendants may challenge the constitutionality of a search through motions to suppress. In response to such motions, the government is likely to argue that investigating officers were relying in good faith on a facially valid warrant when conducting the search. *See United States v. Leon*, 468 U.S. 897 (1984). Courts frequently address the good-faith exception before—and to the exclusion of—the substantive Fourth Amendment claim when denying motions to suppress.⁵⁵ Thus, even in cases where a remote access warrant fails the particularity, probable cause, or reasonableness requirements of the Fourth Amendment, courts will generally avoid ruling on the issue.

⁵³ *See* Laura Donahue, Professor, Georgetown Univ. Law Ctr., Remarks at Panel on the Legal and Policy Implications of Hacking by Law Enforcement at Yale Law School (“Remarks by Laura Donahue”), at 18:00–21:40 (Feb. 18, 2014), <http://vimeo.com/88165230> (stating knowledge of dozens of cases involving government use of hacking tools, but explaining that most of the relevant magistrate judge orders are sealed).

⁵⁴ *Id.*

⁵⁵ *See, e.g., United States v. Clay*, 646 F.3d 1124, 1128 (8th Cir. 2011) (“[T]he district court properly denied [the defendant’s] motion to suppress based on the *Leon* good-faith exception. In light of this conclusion, we need not reach the underlying question of probable cause.”); *United States v. Woodbury*, 511 F.3d 93, 99 (1st Cir. 2007) (“We need not address [the defendant’s] particularity arguments because we find that the *Leon* good faith exception applies.”); *United States v. Cherna*, 184 F.3d 403, 407 (5th Cir. 1999) (“If [the *Leon* good faith exception applies], we end our analysis and affirm the district court’s decision to deny the motion to suppress. . . . If the good-faith exception applies, we need not reach the question of probable cause.”).

The doctrine of qualified immunity functions in much the same way to preclude substantive adjudication in suits seeking damages for violations of Fourth Amendment rights.⁵⁶ Qualified immunity “protects government officials from ‘liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.’” *Pearson v. Callahan*, 555 U.S. 223, 231 (2009). Courts have discretion to address qualified immunity before determining whether the government has violated a plaintiff’s constitutional rights, *id.* at 236, and they frequently do so. Courts often dispose of cases seeking relief for Fourth Amendment violations by concluding that there was no clearly established law at the time of the search which would have put law enforcement on notice that their conduct was unconstitutional. *See, e.g., Messerschmidt v. Millender*, 132 S. Ct. 1235 (2012) (finding qualified immunity and declining to rule on whether facts stated in a warrant application established probable cause). The issues raised by warrants for remote, extra-district electronic searches are necessarily novel because the Federal Rules have not heretofore authorized them. Therefore, qualified immunity will likely apply. Perversely, the very absence of case law addressing these searches will mean there is likely to be little development of case law addressing the constitutionality of these searches in the future.

Accordingly, the time to address the constitutional concerns raised by the proposed amendment is now. Speculation that these important issues will be fully dealt with in future case law is unlikely to prove correct.

B. The Advisory Committee Should Account for the Government’s Lack of Candor About the Scope and Invasiveness of its Remote Access Searches

These problems are exacerbated by the government’s lack of candor about the nature of its remote access searches. The DOJ’s explanations of its remote access search capability in the sample warrant applications,⁵⁷ in warrant applications actually filed in federal court,⁵⁸ and in its recent memoranda to this Committee fail to fully describe the nature and invasiveness of its contemplated and completed remote access searches. As described above, one use of the proposed amendment will be to enable searches involving malware or spyware that take advantage of zero-day vulnerabilities and that travel over the open internet. But nothing in the government’s descriptions of its “network investigative techniques”⁵⁹ or “remote network techniques”⁶⁰ would put a magistrate judge (or, for that matter, a member of this Committee) on notice that the government seeks to conduct its searches using techniques that pose a serious risk

⁵⁶ *See Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388 (1971). Suits for injunctive and declaratory relief are likely to be barred by standing doctrine, on the basis that a person targeted by a remote access search in the past will not be able to prove a likelihood that they will be subjected to such a search again in the future. *See City of Los Angeles v. Lyons*, 461 U.S. 95 (1983).

⁵⁷ *See* Advisory Committee Materials 181–235.

⁵⁸ *See, e.g.,* Affidavit of Justin E. Noble in Support of Application for Search Warrant, *In re Search of Network Investigative Technique (“NIT”) for E-mail Address 512SocialMedia@gmail.com*, No. 12-mj-748-ML (W.D. Tex. Dec. 18, 2012); Third Amended Affidavit of William A. Gallegos In Support of Application for Search Warrant, *In re Search of Network Investigative Technique (“NIT”) for Email Address texan.slayer@yahoo.com*, No. 12-sw-05685-KMT (D. Colo. Dec. 11, 2012).

⁵⁹ *See, e.g.,* Advisory Committee Materials 200–03.

⁶⁰ *See, e.g., id.* 216.

to cybersecurity, and that may fail the reasonableness and particularity requirements of the Fourth Amendment.⁶¹

The government also does not provide detailed explanation of the remote searches of data stored on cloud-based services that it seeks to conduct using warrants authorizing physical searches of computers connected to the cloud. The government does not describe the almost incomprehensibly large storage capacity of many cloud-based services, the vast amount of personal information now stored on the cloud, or the dizzying array of cloud storage services to which a computer may be connected. This information is crucial to assessing whether a warrant is appropriately limited to permit access only to cloud services as to which there is probable cause, and whether the warrant describes the locations to be searched with particularity.

It is crucial that the government provide full and accurate information to magistrate judges (and to this Committee) when seeking authority to conduct novel and invasive searches.⁶² The Advisory Committee should not authorize new search powers without ensuring that the duty of candor has been and will be satisfied.

C. Expanding the Government’s Remote Access Search Powers Based on Consideration of Current Technology Will Result in Increasingly More Invasive Searches as Technology Advances

If adopted, the proposed amendment will provide authority for the government to conduct remote access electronic searches for years to come. Over the coming decades, electronic storage systems will become ever more interconnected. Interconnectivity of cloud storage will likely increase at a rapid rate, and will proceed in ways that we cannot now accurately predict. This raises the specter of the authority enacted today for one purpose inadvertently enabling future searches that are considerably more invasive than anything the Advisory Committee, or even the government, now envisions.

Ten years ago, few people could have predicted the ubiquity of cloud storage, the widespread reliance on internet-connected mobile devices, or the substantial portion of people’s personal and professional lives that has migrated online. It is similarly difficult to predict technological developments five or ten years from now. We are likely to see new forms of cloud storage and new linkages between cloud storage systems, giving remote access searches increasingly invasive potential. Companies are designing and marketing new types of internet-

⁶¹ See Remarks by Laura Donahue, *supra*, at 21:45–22:17 (“Often [the government’s] applications do not include detailed technology, or technological explanation as to how it is actually going to be executed, enter the computer, exactly what information is going to be obtained, which other devices might be infected, how many devices may be infected, and so on.”).

⁶² *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1178 (Kozinski, C.J., concurring) (“[O]mitting . . . highly relevant information [about a search of electronic data] is inconsistent with the government’s duty of candor in presenting a warrant application. A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.”); cf. Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J. L. & Tech. 134, 162 (2013) (discussing government’s lack of candor to judges when seeking authority to use “Stingray” cell phone tracking devices).

connected devices, from smoke detectors,⁶³ to “nanny cams,”⁶⁴ to televisions and refrigerators.⁶⁵ According to one estimate, “up to 200 billion devices—from games consoles to thermostats—will be hooked up to the Internet by 2020.”⁶⁶ Granting the government the power to hack remotely into these devices, thus gaining a view inside people’s most private spaces, is constitutionally suspect. Any amendment adopted today must account for short- and long-term changes in the nature and magnitude of cloud storage and internet connectivity, and must adequately protect Americans’ rights over the coming years.

* * * * *

Thank you for your consideration of these comments.

Respectfully,



Nathan Freed Wessler
Christopher Soghoian
Alex Abdo
Rita Cant
American Civil Liberties Union
Speech, Privacy, and Technology Project
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

⁶³ See Rory Carroll, *Google Buys Nest Labs for \$3.2bn in Bid for Smart Home-Devices Market*, Guardian, Jan. 14, 2014, <http://www.theguardian.com/technology/2014/jan/13/google-nest-labs-3bn-bid-smart-home-devices-market>.

⁶⁴ E.g., NetGear VueZone, Nanny Cam, <http://www.vuezone.com/use-ideas/nanny-cam>.

⁶⁵ Gary Davis, *Smart TVs, Refrigerators Used in Internet-of-Things Cyberattack*, McAfee Blog Central, Jan. 22, 2014, <https://blogs.mcafee.com/consumer/internet-of-things-cyberattack>.

⁶⁶ David Nield, *Thousands of Smart Gadgets Hacked to Send out Spam Email*, Digital Trends, Jan. 18, 2014, <http://www.digitaltrends.com/computing/thousands-smart-gadgets-hacked-send-spam-email>.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jy-8gbw-o4p1
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0017](#)

Comment from Kyle Druding, NA

Submitter Information

Name: Kyle Druding

Organization: NA

General Comment

This comment discusses the proposed changes to Rule 4 of the Federal Rules of Criminal Procedure. It is also available, as a Note in the Duke Law Journal, 64 Duke L.J. 515, at <http://dlj.law.duke.edu/article/in-search-of-monsters-abroad-druding-vol64-iss3/>. The abstract of the comment is as follows:

Recently, federal prosecutors increased interest in criminally charging foreign organizational defendants has revealed a jurisdictional gap in Rule 4 of the Federal Rules of Criminal Procedure. Rule 4, which has operated largely unchanged since its adoption in 1944, requires that a copy of a compulsory summons be served on an organizational defendant by mailing it either to the defendants last known address in the relevant district or to its principal place of business elsewhere in the United States. The courts have divided over how to confront jurisdictional challenges brought by certain foreign corporations those without domestic principal places of business and addresses that appear to be legally incapable of receiving service. As it stands, the jurisdictional gap threatens to effectively immunize large swaths of illegality over which the United States would otherwise have jurisdiction. The Department of Justice and the Advisory Committee on Rules of Criminal Procedure have responded to this concern with dueling proposals to close Rule 4s jurisdictional gap.

This Note agrees that the jurisdictional gap should be closed, but in a narrowly fashioned manner. Relaxing the service regime for foreign organizational defendants too much may enable, for the first time, prosecutions of wholly extraterritorial conduct that would violate the Fifth Amendments Due Process Clause. This Note sketches the contours of such a case, and concludes that any risk is best cabined by reasonably limited means of service under Rule 4 coupled with the responsible exercise of prosecutorial discretion.

Attachments

In Search of Monsters Abroad- Serving Summonses on Foreign Organi

Notes

IN SEARCH OF MONSTERS ABROAD: SERVING SUMMONSES ON FOREIGN ORGANIZATIONS UNDER RULE 4 AND FIFTH AMENDMENT DUE PROCESS

KYLE M. DRUDING[†]

ABSTRACT

Recently, federal prosecutors' increased interest in criminally charging foreign organizational defendants has revealed a "jurisdictional gap" in Rule 4 of the Federal Rules of Criminal Procedure. Rule 4, which has operated largely unchanged since its adoption in 1944, requires that a copy of a compulsory summons be served on an organizational defendant by mailing it either to the defendant's "last known address" in the relevant district or to its "principal place of business elsewhere in the United States." The courts have divided over how to confront jurisdictional challenges brought by certain foreign corporations—those without domestic principal places of business and addresses—that appear to be legally incapable of receiving service. As it stands, the jurisdictional gap threatens to effectively immunize large swaths of illegality over which the United States would otherwise have jurisdiction. The Department of Justice and the Advisory Committee on Rules of Criminal Procedure have responded to this concern with dueling proposals to close Rule 4's jurisdictional gap.

This Note agrees that the jurisdictional gap should be closed, but in a narrowly fashioned manner. Relaxing the service regime for foreign

Copyright © 2014 Kyle M. Druding.

[†] Duke University School of Law, J.D. expected 2015; Michigan State University, B.A. 2012. This Note would not have been possible without the guidance and support of Elisabeth de Fontenay, who graciously supervised this effort. I am also deeply indebted to Sara Sun Beale, who first introduced me to this topic while I had the great privilege to serve as her research assistant. Working with the staff of the *Duke Law Journal* has been anything but monstrous. Brittany Cassell, Jerry Fang, Haniya Mir, Alison Newman, Bill O'Connell, Jack Pararas, Stevie Pearl, Daniel Rice, Ben Sachs, Christine Turner, and James Waters deserve particular recognition for their collegiality, insight, and patience. All remaining mistakes are, of course, my own.

organizational defendants too much may enable, for the first time, prosecutions of wholly extraterritorial conduct that would violate the Fifth Amendment's Due Process Clause. This Note sketches the contours of such a case, and concludes that any risk is best cabined by reasonably limited means of service under Rule 4 coupled with the responsible exercise of prosecutorial discretion.

INTRODUCTION

*America, in the assembly of nations, since her admission among them, has invariably, though often fruitlessly, held forth to them the hand of honest friendship, of equal freedom, of generous reciprocity. . . . But she goes not abroad, in search of monsters to destroy.*¹

An ongoing contract dispute involving alleged violations of intellectual property and trade secrets against an American corporation by a Chinese state-owned enterprise has evolved into an extraterritorial federal criminal prosecution, garnering serious political attention. AMSC, formerly American Superconductor, has accused the Beijing-based Sinovel Wind Group (Sinovel) of offering an AMSC employee an employment contract worth more than \$1.5 million in exchange for illegally procuring protected source code for the operation of wind turbines.² The pirated software was then reimported for use in four wind turbines located mere miles from AMSC headquarters in Devens, Massachusetts, allegedly costing AMSC more than \$1 billion and forcing it to shrink its worldwide staff by five-hundred employees.³

Four civil suits based on this pirating were filed in China but stalled for years, and Chinese officials declined to prosecute.⁴ The U.S. Department of Justice (DOJ) stepped in to indict Sinovel on charges of conspiracy, trade-secret violations, and wire fraud.⁵ Secretary of State John Kerry, then the senior senator from

1. John Quincy Adams, Sec'y of State, Speech to the U.S. House of Representatives on Foreign Policy (July 4, 1821) (transcript available at <http://millercenter.org/president/speeches/detail/3484>).

2. Press Release, AMSC, China's Sinovel Indicted in the United States for Stealing AMSC Trade Secrets (June 27, 2013), available at <http://ir.amsc.com/releasedetail.cfm?ReleaseID=774372>.

3. *Id.*

4. *Id.*

5. Indictment at 4, 10, United States v. Sinovel Wind Grp. Co., 3:13-cr-84 (W.D. Wis. filed June 27, 2013).

Massachusetts, characterized the controversy as “a mugging in broad daylight and a real test of China’s commitment to the rule of law.”⁶ The Sinovel–AMSC incident, however, is not an isolated case. The U.S. International Trade Commission estimated that in 2009 alone, similar “muggings in broad daylight” by Chinese companies cost the U.S. economy \$50 billion and 900,000 jobs.⁷

Whatever the underlying merits of the DOJ’s charges in this case, an obscure procedural hurdle may prevent it and similar prosecutions from moving forward in federal court. Sinovel specially appeared to quash the government’s efforts to serve it process pursuant to Rule 4 of the Federal Rules of Criminal Procedure (Rule 4).⁸ For organizational defendants, Rule 4 requires the government to personally serve an officer or agent and to mail a copy of the summons to the defendant’s “last known address within the district” or “its principal place of business elsewhere in the United States.”⁹ In essence, Sinovel argued that its status as a foreign corporation, without a sufficient domestic footprint, immunized it from federal criminal proceedings because it was physically impossible for Sinovel to receive a copy of the summons pursuant to Rule 4’s current language.¹⁰ After reviewing the “underdeveloped law” and “facts that point in both directions,” Magistrate Judge Crocker issued a ruling that will allow the case to move forward, but noted that the “court could justify a ruling in either direction.”¹¹ Highlighting its importance and complexity, Judge Crocker openly invited the appellate courts to provide guidance on this issue.¹² Similar arguments in recent cases have likewise troubled other courts and vexed prosecutors’ efforts to vindicate U.S. interests by bringing criminal actions against foreign

6. Keith Johnson, *Chinese Wind Turbine Maker Indicted in U.S.: Sinovel Charged With Stealing Trade-Secrets From American Firm, Copyright Infringement*, WALL ST. J., June 28, 2013, at B2. Vice President Joe Biden, Senator Elizabeth Warren, former Secretary of State Hillary Clinton, former U.S. Trade Representative Ron Kirk, and former Acting Secretary of Commerce Rebecca Blank have also expressed their support for AMSC. Press Release, AMSC, *supra* note 2.

7. Johnson, *supra* note 6, at B2.

8. Brief for Defendant at 1, *Sinovel Wind Grp. Co.*, 3:13-cr-84.

9. FED. R. CRIM. P. 4(c)(3)(C).

10. *See* Brief for Defendant at 13–17, *Sinovel Wind Grp. Co.*, 3:13-cr-84 (arguing that Rule 4 precludes service on Sinovel).

11. *United States v. Sinovel Wind Grp. Co.*, 3:13-cr-84, at 1 (W.D. Wis. May 27, 2014) (order denying motion to quash service of process).

12. *See id.* (“Regardless which way this court rules on Sinovel China’s motion, the loser will appeal, perhaps generating some useful circuit case law on this point.”).

organizations.¹³ In response to the DOJ's experiences, there are efforts currently pending to update Rule 4 to allow service to be made on foreign organizations whose conduct is subject to U.S. jurisdiction.¹⁴

This Note is the first piece of scholarship to address the jurisdictional gap in Rule 4 and to analyze the courts' mixed reactions to nonconforming attempts to effectuate service.¹⁵ It is also the first work to evaluate the recent movement to revise Rule 4. Further, this Note contributes to a developing body of scholarship on Fifth Amendment due-process limits in criminal prosecutions of extraterritorial conduct¹⁶ by assessing the unique challenges of prosecuting nonnatural persons. It also argues that potential due-process concerns are best framed as policy concerns of general prosecutorial overreach, which cannot be adequately cabined by Rule 4.

This Note proceeds in four parts. Part I provides an overview of the jurisdictional gap embodied in the language of Rule 4 and examines the courts' varied responses to defendants challenging the sufficiency of service of process. Part II details the DOJ's and the Advisory Committee on Rules of Criminal Procedure's (Advisory Committee's) proposed revisions to Rule 4 and analyzes their subtle, but critical, differences.¹⁷ Part III explores the extraterritorial application of federal criminal law and its likely, but uncertain, limitations as a matter of Fifth Amendment due process. Part IV concludes that expanding service of process abroad will increase the likelihood that prosecutors will subject foreign organizational defendants to due-process violations; nevertheless, concerns about

13. *See infra* Part I.B.

14. *See infra* Part II.

15. To this author's knowledge, no one has previously examined this aspect of Rule 4, which may be due to its recent provenance. *See infra* note 39. Other analyses of Rule 4's application to foreign defendants generally focus on its warrant provision for individuals. *See, e.g.*, Thomas G. Becker, *Justice on the Far Side of the World: The Continuing Problem of Misconduct by Civilians Accompanying the Armed Forces in Foreign Countries*, 18 HASTINGS INT'L & COMP. L. REV. 227, 292 (1995).

16. *See infra* note 172.

17. As of this Note's publication, the Advisory Committee's proposed changes to Rule 4 have been submitted for public comment. *See* Comm. on Rules of Practice & Procedure of the Judicial Conference of the U.S., *Preliminary Draft of Proposed Amendment to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure* 329 (2014), available at <http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf>. Comments may be submitted until Tuesday, February 17, 2015. *Id.* at 1.

potential prosecutorial overreach should not prevent efforts to update Rule 4 and to eliminate its jurisdictional gap.

I. RULE 4'S JURISDICTIONAL GAP

As courts have repeatedly reminded prosecutors attempting to serve summonses on foreign organizational¹⁸ defendants like Sinovel, there is a jurisdictional gap between the substantive reach of federal criminal law and the procedural means used to enforce it. This Part examines the gap in Rule 4's language and provides an overview of the judicial responses to nonconforming efforts to effectuate service on foreign organizational defendants.

A. *The Current Language of Rule 4*

Service of process in the U.S. legal tradition serves two primary functions: first, to provide notice of a pending action,¹⁹ and second, to establish the court's jurisdiction over the defendant.²⁰ These dual functions are incorporated into Rule 4, which governs arrest warrants and summonses in all federal criminal proceedings.²¹ Organizational defendants cannot be "arrested" in any meaningful sense,²² but are subject to compulsory summonses.²³ Unlike the analogous provision governing civil proceedings,²⁴ the Federal Rules of Criminal

18. Although this Note generally uses "organization" to refer to corporations, federal law defines the term broadly to encompass any "person other than an individual." 18 U.S.C. § 18 (2012).

19. *See, e.g.,* Milliken v. Meyer, 311 U.S. 457, 462–63 (1940) (holding that service must be "reasonably calculated to give [the party] actual notice of the proceedings and an opportunity to be heard" as a matter of due process).

20. *See, e.g.,* Murphy Bros. v. Michetti Pipe Stringing, Inc., 526 U.S. 344, 350 (1999) ("Service of process . . . is fundamental to any procedural imposition on a named defendant.").

21. FED. R. CRIM. P. 4. Similar issues may arise under state law, as well, because approximately half of the states have adopted similar or identical rules governing criminal procedure. Jerold Israel, *Federal Criminal Procedure as a Model for the States*, 543 ANNALS AM. ACAD. POL. & SOC. SCI. 130, 138 n.18 (1996) (identifying these states). However, state-law concerns may be less grave given the practical realities of prosecuting foreign organizations.

22. For a discussion of the fictive nature of corporate personhood encountered when serving foreign organizations and the associated policy concerns, see *infra* Part IV.A–B.

23. FED. R. CRIM. P. 4(c)(3)(C).

24. *See* FED. R. CIV. P. 4(h)(2) (enumerating several authorized methods of serving organizational parties outside a U.S. judicial district, including the use of an international agreement or court order).

Procedure do not specifically address defendants located abroad.²⁵ The relevant portion of Rule 4 is as follows:

A summons is served on an organization by delivering a copy to an officer, to a managing or general agent, or to another agent appointed or legally authorized to return service of process. A copy must also be mailed to the organization's *last known address within the district* or to its *principal place of business elsewhere in the United States*.²⁶

Thus, Rule 4 imposes two distinct requirements for properly serving summonses on organizational defendants: the delivery requirement and the mailing requirement, which are discussed in turn.

1. *The Delivery Requirement.* The requirement that a copy of the summons be delivered to an “officer,” “managing or general agent,” or “another agent appointed or legally authorized”²⁷ is fairly straightforward and does not, on its own, create a jurisdictional gap. The delivery requirement does, however, raise the specter that prosecutors will be unable to serve an organizational defendant whose relevant agents are located abroad and where no federal statute authorizes an arrest to be made.²⁸

The problem of criminal activity committed beyond the reach of authorized U.S. jurisdiction is not limited to organizational defendants.²⁹ What is unique to organizational defendants, however, is their ability to employ creative corporate structures as a shield against criminal liability for the parent company while maintaining a physical domestic presence. The most blatant version of such an attempted shield would be a foreign defendant incorporating a subsidiary in the United States for the sole purpose of engaging in

25. See FED. R. CRIM. P. 4(c)(3)(C). Rule 4 also lacks a provision specifically addressing serving process on an individual abroad, but states that a summons may be served “within the jurisdiction of the United States or anywhere else a federal statute authorizes an arrest.” FED. R. CRIM. P. 4(c)(2).

26. FED. R. CIV. P. 4(c)(3)(C) (emphasis added).

27. *Id.*

28. See FED. R. CIV. P. 4(c)(2) (limiting the scope of service to locations within U.S. jurisdiction and those where federal statutes have authorized service).

29. See, e.g., *United States v. Hijazi*, 845 F. Supp. 2d 874, 878–81, 895 (C.D. Ill. 2011) (finding that a Defense Cooperation Agreement between the United States and Kuwait effectively precluded prosecution of the defendant for inflating bids submitted as a subcontractor to the U.S. government, even though the United States had jurisdiction over his conduct).

domestic criminal activity and insulating its legitimate business interests abroad. Under such circumstances, courts would likely hold the shell company to be the defendant's "alter ego"³⁰ or a "mere conduit for the activities of its parent,"³¹ and find service made on an agent of the shell company to be sufficient to establish jurisdiction over the defendant.³² When the relationship between parent and subsidiary is less stark, however, prosecutors face an onerous and highly fact-dependent burden of proof.³³

When the subsidiary's operations are determined to be sufficiently distinct from its parent's, service on the subsidiary will not be imputed to the parent.³⁴ Therefore, foreign organizational defendants that maintain domestic corporate enterprises with a degree of separation in their activities are unlikely to be subject to service. As a result, although the delivery requirement may exacerbate such evasive measures,³⁵ the service regime it creates for organizational defendants does not differ in kind from that faced by natural persons.

2. *The Mailing Requirement.* The requirement that a copy of the summons be mailed to an organizational defendant at its "last known address in the district" or "its principal place of business elsewhere in the United States"³⁶ clearly contemplates a *domestic* mailing. Therefore, a "jurisdictional gap" exists when the United States has jurisdiction over an organization's criminal conduct, but it is physically impossible to serve a summons on the defendant because the crime took place in a district where the defendant has no mailing address and the defendant maintains its principal place of business

30. *United States v. The Pub. Warehousing Co. K.S.C.*, No. 1:09-cr-490, 2011 WL 1126333, at *5 (N.D. Ga. Mar. 28, 2011).

31. *United States v. Chitron Elecs. Co.*, 668 F. Supp. 2d 298, 305 (D. Mass. 2009).

32. This approach—effectively, to pierce the corporate veil so that service on the subsidiary will bind the parent as well—is consonant with courts' greater willingness to vindicate veil-piercing challenges in statutory contexts to further governmental purposes. *See* 1 JAMES D. COX & THOMAS LEE HAZEN, *COX & HAZEN ON THE LAW OF CORPORATIONS* § 7:17 (3d ed. 2010) (discussing courts' responses to veil-piercing arguments in contractual and statutory contexts).

33. *See United States v. Alfred L. Wolff GMBH*, No. 08-cr-417, 2011 WL 4471383, at *4-8 (N.D. Ill. Sept. 26, 2011) (using a "totality of the circumstances" test to reject the government's argument to "pierce the corporate veil" for purposes of service).

34. *Id.*

35. For discussion of a case that highlights the incentives to adopt similar parent-subsidiary structures as a shield against criminal liability in the United States, see *infra* notes 40-45 and accompanying text.

36. FED. R. CRIM. P. 4(c)(3)(C).

abroad. The jurisdictional gap is especially pernicious for crimes committed remotely via the internet or through a domestic subsidiary,³⁷ as failure to comply with the mailing requirement may stall U.S. prosecutions or even preclude them altogether.³⁸

Nor is this jurisdictional gap purely theoretical. Federal district courts have recently adjudicated several challenges from organizational defendants contesting the efficacy of service as a result of the government's failure to satisfy Rule 4's mailing requirement.³⁹ The DOJ's experience in the first of these challenges highlights the mailing requirement's potential threat as a procedural barrier to otherwise viable prosecutions. In *United States v. Johnson Matthey PLC*,⁴⁰ the government indicted but twice failed to properly serve the defendant, an organization incorporated under the laws of England and Wales and with its principal place of business in London.⁴¹ Service was held to be improper despite the fact that the parties stipulated to an agent capable of receiving service.⁴² Moreover, copies of the summonses had been sent to the company's main London office and to a subsidiary-owned refinery in Salt Lake City, Utah, via the subsidiary's headquarters in Wayne, Pennsylvania.⁴³ Despite having provided "ample notice," prosecutors had failed to mail a copy of the summons in strict adherence to the language of Rule 4.⁴⁴

37. See, e.g., Indictment at 4, 10, *United States v. Sinovel Wind Grp. Co.*, 3:13-cr-00084 (W.D. Wis. filed June 27, 2013) (alleging that a Chinese state-owned enterprise conspired with a Serbian national employed by an Austrian subsidiary to steal protected information from a Massachusetts corporation's internet server located in Middleton, Wisconsin).

38. Prosecutors could still pursue defendants in their individual capacities. However, specific consequences that flow from prosecutions of organizational defendants would be effectively barred by the text of Rule 4's mailing requirement. See *infra* Part IV.B.

39. To date, seven district courts have ruled on Rule 4's mailing requirement. *United States v. Kolon Indus., Inc.*, 926 F. Supp. 2d 794 (E.D. Va. 2013); *United States v. Dotcom*, No. 1:12-cr-3, 2012 WL 4788433 (E.D. Va. Oct. 5, 2012); *United States v. Pangang Grp. Co.*, 879 F. Supp. 2d 1052 (N.D. Cal. 2012); *United States v. Alfred L. Wolff GMBH*, No. 08-cr-417, 2011 WL 4471383 (N.D. Ill. Sept. 26, 2011); *United States v. The Pub. Warehousing Co. K.S.C.*, No. 1:09-cr-490, 2011 WL 1126333 (N.D. Ga. Mar. 28, 2011); *United States v. Chitron Elec. Co.*, 668 F. Supp. 2d 298 (D. Mass. 2009); *United States v. Johnson Matthey PLC*, No. 2:06-cr-169, 2007 WL 2254676 (D. Utah Aug. 2, 2007).

40. *Johnson Matthey PLC*, 2007 WL 2254676, at *1.

41. *Id.* at *1-2.

42. *Id.*

43. *Id.* at *2. *Johnson Matthey PLC*, which was not alleged to have had a presence in Utah, was charged with conspiracy and twenty-eight counts of regulatory offenses concerning effluent discharge at a gold and silver refinery owned by its subsidiary, *Johnson Matthey, Inc.* *Id.* at *1.

44. *Id.* at *2.

The court did suggest, however, that the government could have effectuated proper service through the bilateral Mutual Legal Assistance Treaty to which the United Kingdom and the United States are both signatories.⁴⁵ Even if the court would have actually approved service pursuant to an international agreement—a method of service not apparent from a plain textual reading of Rule 4⁴⁶—defendants located in countries not party to such an agreement would remain effectively immunized from prosecution. Thus, the court’s recognition of this jurisdictional gap would bar prosecution for at least a certain class of organizational defendants.

From the limited available evidence, it appears that Rule 4’s jurisdictional gap is an unintended consequence of efforts to ensure actual notice for organizational defendants. Nothing in the Advisory Committee Notes (ACN) suggests that the jurisdictional gap created by the mailing provision was consciously intended. The only mention of the mailing requirement states that “in all cases in which a summons is being served on an organization, a copy of the summons must be mailed to the organization.”⁴⁷ Although the ACN emphasize the importance of a mailing, they do not explain why the mailing must be a *domestic* one.⁴⁸ Bolstering the view that the jurisdictional gap emerged inadvertently, the ACN explicitly state that Rule 4’s summons provisions were modeled on their counterparts in the Federal Rules of Civil Procedure.⁴⁹ The analogous civil provision does not contain a domestic-mailing requirement and allows for service on organizations abroad in the same manner as for individuals.⁵⁰

If the drafters of Rule 4 had consciously intended to further a policy goal by enacting a domestic-mailing requirement, such as limiting the number of prosecutions brought against foreign organizations, evidence to this effect would be expected. Moreover, it is hard to imagine what policy rationales might have animated Rule

45. *Id.*

46. *Cf. DeJames v. Magnificence Carriers, Inc.*, 654 F.2d 280, 287–90 (3d Cir. 1981) (finding service of process that occurred abroad pursuant to a multilateral treaty, but that was not independently authorized, to be insufficient).

47. FED. R. CRIM. P. 4 advisory committee’s note.

48. *Id.*

49. *See* FED. R. CRIM. P. 4(c)(1) (“Any person authorized to serve a summons in a federal civil action may serve a summons.”); *see also* FED. R. CRIM. P. 4 advisory committee’s note (“Service of summons under the rule is substantially the same as in civil actions.”).

50. *See* FED. R. CIV. P. 4(h) (failing to specify that required mailings be made domestically).

4's current mailing requirement. There is no compelling reason to believe that a domestic mailing could provide adequate notice, but an international one could not.⁵¹ Nor is there good reason to believe that foreign organizations lacking a domestic address or principal place of business should be immune from service, while those with such a domestic footprint are not.⁵² Therefore, the jurisdictional gap is most likely the unhappy oversight of a well-intentioned drafting effort.

B. The Federal Courts' Responses to Nonconforming Attempts at Service

Courts encounter the horns of dilemma in prosecutions where it is impossible to make a domestic mailing on organizational defendants. On the one hand, service is an integral step in ensuring that courts act only within their own jurisdictional authority⁵³—a failure to properly effectuate service will usually preclude a court from exercising its power over that defendant.⁵⁴ On the other hand, courts should be concerned that the sensitive interests protected by federal criminal law may not be vindicated because of a provision that, in all likelihood, did not contemplate systematic underenforcement.⁵⁵

To date, the federal courts have generally hewed closely to the text of Rule 4 by granting motions to quash summonses where a domestic mailing to an organizational defendant could not have been made. The approach taken in *United States v. Pangang Group, Co.*⁵⁶ is particularly instructive. The *Pangang Group* defendants, both foreign and domestic entities, consisted largely of state-owned enterprises of

51. In the civil context, for example, service may be made abroad by “using any form of mail that the clerk addresses and sends . . . that requires a signed receipt,” FED. R. CRIM. P. 4(f)(2)(C)(ii), or pursuant to the Hague Convention, FED. R. CRIM. P. 4(f)(1).

52. Any possible rationale concerning the sufficiency of a U.S. nexus fails to explain why such a strong policy preference would be limited to the provision governing service of process. For a discussion of the due-process limits on U.S. prosecutions of noncitizens, see *infra* Part III.C. Moreover, the relevant portion of the ACN predates, by several years, the earliest case successfully challenging the validity of service as failing to satisfy the mailing requirement.

53. See *Murphy Bros. v. Michetti Pipe Stringing, Inc.*, 526 U.S. 344, 350 (1990) (“Service of process, under longstanding tradition in our system of justice, is fundamental to any procedural imposition on a named defendant.”).

54. See *Omni Capital Int’l, Ltd. v. Rudolf Wolff & Co.*, 484 U.S. 97, 104 (1987) (“Before a federal court may exercise personal jurisdiction over a defendant, the procedural requirement of service of summons must be satisfied.”).

55. See *supra* notes 47–52 and accompanying text.

56. *United States v. Pangang Grp. Co.*, 879 F. Supp. 2d 1052 (N.D. Cal. 2012).

the People's Republic of China.⁵⁷ They were indicted on numerous charges, most prominently conspiracy to commit economic espionage and violation of trade secrets.⁵⁸ The principal defendant held ownership interests in many of its codefendants, including a 75 percent stake in Pan America, a New Jersey corporation.⁵⁹ Over the defendant's and its counsel's objections, the government personally served Pan America's general manager on behalf of the defendant and mailed copies of the summons to Pan America's office in East Brunswick, New Jersey.⁶⁰

In response to the Pangang Group's motion to quash the summons as improperly served, the court began with the "plain language" of Rule 4.⁶¹ The court differentiated Rule 4 from its civil counterpart, holding that a copy of the summons must be mailed to the organization directly—not to its general agent's address—because Rule 4's mailing requirement is "[un]ambiguous."⁶² Next, the court noted that it was "relevant but not dispositive" that the Pangang Group had actual notice of the proceedings, and that effective service required "substantial compliance" with Rule 4's stated requirements.⁶³ Finally, the court concluded that a mailing to Pan America could properly effectuate service on the Pangang Group only if the government proved that Pan America was the "alter-ego" of the Pangang Group.⁶⁴ This approach categorically fails to provide any means to serve foreign organizations if they lack a domestic

57. *Id.* at 1056.

58. *See id.* (describing the charges).

59. *Id.* The other 25 percent of Pan America was held by the Pangang Group's "financing arm." *Id.*

60. *Id.*

61. *Id.* at 1064.

62. *Id.* at 1065.

63. *Id.*

64. *Id.* at 1066. Although the court did not hold that Pan America was the Pangang Group's "alter-ego," *id.* at 1069, there is good reason to believe that service would have been improper even if it had. Unless Pan America had a last known address in the Northern District of California, Rule 4 would require the mailing be sent to the defendant's "principal place of business elsewhere in the United States." FED. R. CRIM. P. 4(c)(3)(C). Because the Pangang Group's principal place of business is in China—not "elsewhere in the United States"—the court would have to determine that the Pangang Group had *two* principal places of business to uphold the mailing to Pan America's New Jersey office, something of a metaphysical conundrum that runs counter to the logic of recent Supreme Court jurisprudence in civil diversity cases. *See Hertz Corp. v. Friend*, 559 U.S. 77, 93 (2010) (adopting a "nerve center" test to determine citizenship under which a party's principal place of business must be located in "a single place").

subsidiary or if the subsidiary operates as a separate, independent entity.

Faced with the unfortunate results generated by strict adherence to the text of Rule 4, at least one court, the Eastern District of Virginia, has begun pushing back.⁶⁵ Ruling on a situation in which a domestic mailing was physically impossible, Judge Liam O’Grady held that compliance with Rule 4’s delivery requirement alone provided effective jurisdiction over a defendant.⁶⁶ The opinion noted that although the mailing requirement was “unambiguous[]” and “mandatory,” it was a statutory requirement, created wholly by Rule 4, which did not preclude jurisdiction.⁶⁷ In dictum, Judge O’Grady strongly suggested that courts could still hear cases where the mailing requirement had not been satisfied by imposing an “appropriate [but unspecified] penalty.”⁶⁸ Reflecting on Rule 4’s jurisdictional gap, Judge O’Grady captured the intractability of a pure textualist reading: “It is doubtful that Congress would stamp with approval a procedural rule permitting a foreign corporate defendant to intentionally violate the laws of this country, yet evade the jurisdiction of United States’ courts by purposefully failing to establish an address here.”⁶⁹ After failing to find to a “legal and factual certainty” that the government could not properly effectuate service, the court denied the defendant’s motion to dismiss.⁷⁰

In *United States v. Kolon Industries, Inc.*,⁷¹ the Eastern District of Virginia took the additional step of carving an exception out of Rule 4’s mailing requirement. The court noted that it was “clear” the

65. It is unsurprising that the Eastern District of Virginia is pushing back, given that its efficiency in hearing complex commercial cases requires it to deal frequently with similar cases. Requiring prosecutors to comply with Rule 4 too strictly would conflict with the desire to dispose of cases in a timely manner and maintain the court’s “fabled rocket docket.” *Eastern District of Virginia: The Rocket Docket*, WILEY REIN LLP, <http://www.wileyrein.com/practices.cfm?sp=overview&id=57> (last visited Nov. 2, 2014). For example, one prominent law firm has dubbed the Eastern District of Virginia the “most efficient court” in the United States and maintains a specialized “Rocket Docket Team” because of the advantages offered by the court’s unique expertise. *Id.*

66. *United States v. Dotcom*, No. 1:12-cr-3, 2012 WL 4788433, at *1 (E.D. Va. Oct. 5, 2012).

67. *Id.* at *1 n.1.

68. *Id.* The court declined to “expound . . . the Rule’s syntax” to suggest what such a penalty might entail, but did hint that it may vary based on “the individual facts and circumstances.” *Id.*

69. *Id.* at *1 (footnote omitted).

70. *Id.*

71. *United States v. Kolon Indus., Inc.*, 926 F. Supp. 2d 794 (E.D. Va. 2013).

prosecution “did not strictly comply with the mailing provision” and that doing so remained “impossible.”⁷² After employing a strict “textual reading” to determine that the mailing requirement was not jurisdictional in nature, the court invoked the “absurd consequences” canon⁷³ to completely invalidate the mailing requirement in such circumstances.⁷⁴ The court “decline[d] to construe [a] procedural rule to thwart the purpose of the substantive criminal statutes themselves,”⁷⁵ denying that Congress could have intended to immunize wholly foreign corporate defendants from prosecution.⁷⁶ *Kolon Industries* remains the strongest indication of the federal courts’ uneasiness with Rule 4’s jurisdictional gap.⁷⁷

The federal courts’ growing dissatisfaction with the jurisdictional gap created by the mailing requirement reflects Rule 4’s underlying drafting problems. Although the courts have expressed at least some willingness to moderate the mailing requirement’s harshest consequences, the responsibility of eliminating the jurisdictional gap ultimately rests with Congress.⁷⁸

II. THE DOJ’S ATTEMPT TO CLOSE THE JURISDICTIONAL GAP AND REVISE RULE 4

More than thirty years ago, V. Rock Grundman observed that “the United States has had three major exports: rock music, blue jeans, and United States law.”⁷⁹ The resonance of this observation has

72. *Id.* at 800.

73. For an overview of how the “absurd consequences” doctrine functions in determining statutory meaning, see generally John F. Manning, *The Absurdity Doctrine*, 116 HARV. L. REV. 2387 (2003).

74. *Kolon Indus., Inc.*, 926 F. Supp. at 801.

75. *Id.* at 802.

76. *Id.*

77. In at least one other situation, a federal court has held that a summons may be delivered through an email to a foreign terrorist group’s website and through publication in several newspapers and magazines, considering such efforts to be “reasonably calculated to notify” the defendant. *United States v. Fuerzas Armadas Revolucionarias de Colombia*, No. 1:04-cr-232 (D.D.C. July 19, 2005). The court did not mention Rule 4’s mailing requirement, however. *See id.*

78. There are several reasons to think that prospective drafting efforts can more appropriately address the current jurisdictional gap, including the legislature’s institutionally superior fact-finding, the benefits of uniformity, and separation-of-powers principles. *See generally* J. HARVIE WILKINSON III, *COSMIC CONSTITUTIONAL THEORY: WHY AMERICANS ARE LOSING THEIR INALIENABLE RIGHT TO SELF-GOVERNANCE* 22–27 (2012).

79. V. Rock Grundman, *The New Imperialism: The Extraterritorial Application of United States Law*, 14 INT’L LAW. 257, 257 (1980).

only intensified in the intervening decades. The overseas application of white-collar criminal law has been a major development.⁸⁰ For example, between 1991 and 1999, the category of foreign firms prosecuted for antitrust violations ballooned from less than 1 percent to roughly 50 percent of all cases brought by the DOJ's Antitrust Division.⁸¹ Tellingly, a defense lawyer, observing the effects on the U.S. Attorney's Manhattan Office, remarked: "It's no longer the Southern District of New York. It should be the Southern District of the World."⁸² Resolving the jurisdictional gap created by Rule 4 will only become more urgent as globalization and economic development continue to extend the reach of foreign organizations.

This Part discusses the DOJ's proposal to reform Rule 4 and the Advisory Committee subcommittee's revised version of the original proposal. Assuming that the government will continue to prosecute foreign organizations engaged in criminal conduct, there are strong arguments for removing the current procedural barriers in Rule 4. Updating Rule 4 in an excessively broad manner may create its own risks, however. Thus, it is important to ensure that the DOJ's effort to eliminate the jurisdictional gap does not prove to be stronger medicine than the disease.

A. *The DOJ's Original Proposal*

On October 25, 2012, the DOJ sent the Advisory Committee a recommendation (the 2012 Recommendation) to revise Rule 4.⁸³ Motivated by the fear that foreign organizations could "avoid liability through the simple expedient[]" of creatively structuring their domestic operations to avoid maintaining a permanent U.S. address, the 2012 Recommendation suggested two specific changes: eliminating the mailing requirement and creating a new mechanism

80. See Brandon L. Garrett, *Globalized Corporate Prosecutions*, 97 VA. L. REV. 1775, 1777 (2011) ("In the past, domestic prosecutions of foreign corporations were not particularly noteworthy. . . . All of this has changed. Federal prosecutors now advertise how they target foreign corporations."); Ellen S. Podgor, *Globalization and the Federal Prosecution of White Collar Crime*, 34 AM. CRIM. L. REV. 325, 326 (1997) (discussing the "international flavor" of the increased growth in U.S. prosecutions for white-collar offenses).

81. Garrett, *supra* note 80, at 1819.

82. Benjamin Weiser, *For Prosecutor in New York, A Global Beat*, N.Y. TIMES, Mar. 28, 2011, at A1.

83. Memorandum from Lanny A. Breuer, Assistant Att'y Gen., Dep't of Justice, to the Hon. Reena Raggi, Chair, Advisory Comm. on the Criminal Rules (Oct. 25, 2012), available at <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2013-04.pdf>.

for serving summonses on organizations abroad.⁸⁴ As the 2012 Recommendation observed, “[t]he environment that influenced the original drafters of the [r]ules . . . no longer exists.”⁸⁵

Increasing economic globalization and the prevalence of electronic communication create a daunting “new reality” for federal prosecutors: more than ever, foreign organizations may “conduct both real and virtual activities” in the United States without maintaining a physical presence there.⁸⁶ Thus, foreign organizations now maintain “an undue advantage” over the government when it attempts to initiate criminal proceedings.⁸⁷ The 2012 Recommendation concluded that as long as the “core objective” of providing “notice of pending criminal proceedings” is fulfilled, the mailing requirement could be safely eliminated.⁸⁸

The 2012 Recommendation used the analogous civil provisions for serving process as a starting point.⁸⁹ The civil rules include separate provisions for service made domestically⁹⁰ and abroad.⁹¹ These two civil provisions contemplate, but do not mandate, mailing copies of the summons to notify a defendant that legal proceedings have been initiated. The former provision requires mailing a copy of the summons when the statute authorizing an agent to receive service so provides.⁹² The latter provision allows service to be made through qualifying mailings, but does not require that a copy of the summons be mailed as a matter of course.⁹³ Neither provision specifies a

84. *Id.* at 1.

85. *Id.* at 2.

86. Memorandum from Sara Sun Beale and Nancy King, Reporters, to the Members, Criminal Rules Advisory Comm., at 1 (Mar. 25, 2013), available at <http://pdfserver.amlaw.com/ca/rules041113.pdf>.

87. *Id.*

88. *Id.*

89. *See id.* at 3 (“Because the original language of Criminal Rule 4 seems to have been based upon the parallel provision of the Federal Rules of Civil Procedure, it may be useful to compare the current civil and criminal provisions.”).

90. FED. R. CIV. P. 4(h)(1).

91. FED. R. CIV. P. 4(h)(2).

92. FED. R. CIV. P. 4(h)(1)(B).

93. Additionally, a copy of the summons may have to be mailed when service is made pursuant to an international agreement or foreign law that imposes a mailing requirement. *See* FED. R. CIV. P. 4(f), (h)(2) (allowing service to be made abroad on an organization in the same manner as an individual, which allows service to be made: (1) by international agreement “reasonably calculated to give notice”; (2) by a method prescribed by foreign law, by a foreign authority in response to a letter rogatory or letter of request, or by “using any form of mail that

particular address to which a mailing must be sent or restricts its destination to within U.S. borders.⁹⁴

The 2012 Recommendation recognized that the “greater public aims of criminal process” may require a “higher burden on the government” for effectuating service.⁹⁵ It therefore rejected “direct incorporation” of the civil provisions.⁹⁶ In order to satisfy this “higher burden,” the DOJ proposed a new subsection⁹⁷ governing service on organizations abroad:

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

(i) 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, in a manner authorized under the laws of the foreign jurisdiction where the officer or agent to be served is located, or

(ii) by other means reasonably calculated to give notice, including

(a) a stipulated means of service;

(b) a means that a foreign authority undertakes in response to a letter rogatory or letter of request;

(c) a means that a foreign authority undertakes in response to a request submitted under an applicable international agreement;

(d) a means otherwise permitted under an applicable international agreement;

the clerk addresses and sends to the individual and that requires a signed receipt;” or (3) “by other means not prohibited by international agreement as the court orders”).

94. See FED. R. CIV. P. 4(h)(1)–(2) (failing to specify an address or restrict mailings to a domestic address).

95. Memorandum from Lanny A. Breuer, *supra* note 83, at 6.

96. *Id.* For example, the Hague Convention allows entry of judgments against parties that fail to appear after being served with a summons. Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, Nov. 15, 1965, 20 U.S.T. 361, 658 U.N.T.S. 163. Directly incorporating this provision (and others like it) into the criminal context would, needless to say, raise serious due-process concerns.

97. Memorandum from Lanny A. Breuer, *supra* note 83, at 6. The new subsection would be titled Rule 4(c)(3)(D). *Id.* at 8. The DOJ’s proposal also includes the following changes: adding “A summons may also be served at a place not within a judicial district of the United States” to Rule 4(c)(2), striking the mailing requirement in Rule 4(c)(3), and adding “at a place within a judicial district of the United States” to Rule 4(c)(3) to create distinct provisions for domestic and foreign service. *Id.* at 7.

(e) *other means upon request of an attorney for the government, as the court orders.*⁹⁸

Proposed Rule (4)(c)(3)(D) creates two discrete mechanisms for serving process on a foreign organization. These methods hinge on whether personal service can be made on an agent of the defendant.

Subsection (D)(i), which allows personal service to be made on an agent of the defendant pursuant to the relevant foreign jurisdiction's law, generally tracks the language of the civil provision but differs in key respects. Most crucially, unlike the civil provision, Subsection (D)(i) contains no explicit requirement that service be made in a manner "reasonably calculated to give notice."⁹⁹ By omitting this requirement, the DOJ implicitly assumed that when personal service on an agent conforms to the laws of the relevant jurisdiction, proper notice is necessarily given. Although adherence to the foreign jurisdiction's law may generally satisfy the "reasonably calculated" standard, employing service mechanisms available solely under a foreign sovereign's law could raise serious concerns.¹⁰⁰ Most notably, prosecutors may undertake foreign-service mechanisms that could not effectuate service domestically and that fail to provide actual notice, such as a law authorizing service to be made on a low-level employee or a copy of the summons to be sent solely to a listed email address.¹⁰¹

In contrast, Subsection (D)(ii), which creates five alternatives to personal service on one of the defendant's agents, explicitly requires that these "other means" be "reasonably calculated to give notice."¹⁰²

98. *Id.* (emphasis added).

99. *Cf.* FED. R. CIV. P. (4)(f)(2). The "reasonably calculated" standard was enumerated in *Mullane v. Century Bank & Trust Co.*, 339 U.S. 306, 314 (1950). *Mullane v. Cent. Bank & Trust Co.*, 339 U.S. 306, 314 (1950) ("An elementary and fundamental requirement of due process in any proceeding which is to be accorded finality is notice *reasonably calculated*, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections." (emphasis added)).

100. Even absent legal barriers to using a service mechanism available only under the laws of a foreign sovereign, foreign-policy concerns may counsel against granting foreign citizens inferior procedural protections. For a discussion, see generally Paul B. Stephan III, *Constitutional Limits on the Struggle Against International Terrorism: Revisiting the Rights of Overseas Aliens*, 19 CONN. L. REV. 831 (1987).

101. *Cf.* Frederick S. Longer, *Service of Process in China*, ABA SECTION OF LITIGATION 2012 SECTION ANNUAL CONFERENCE (2012), http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/19-1_service_of_process_in_china.pdf (noting that requests to provide service on organizations in China must be submitted to the "Chinese Central Authority," which has wide discretion to authorize various service mechanisms).

102. Memorandum from Lanny A. Breuer, *supra* note 83, at 7.

Subsection (D)(ii)'s first four subparts are all premised on notions of consent. Subpart (D)(ii)(a), which allows service to be made by "a stipulated means of service,"¹⁰³ guarantees that the defendant itself has consented to a specified means of receiving service and, by implication, to U.S. jurisdiction. Subparts (D)(ii)(b)–(d), which cover various international-service arrangements,¹⁰⁴ require consensual agreements between the sovereigns with jurisdiction over the defendant and whose laws govern the defendant's conduct. These methods are largely uncontroversial because they directly fulfill the dual purposes of service: providing notice and asserting jurisdiction.¹⁰⁵

Subpart (D)(ii)(e) creates a residual service provision that allows for any "other means . . . as the court orders," if made "upon request of an attorney for the government."¹⁰⁶ This subpart lacks any element of consent; the United States may invoke it unilaterally as long as the prosecution and court act in tandem. This residual provision introduces the serious policy concern that an overzealous prosecutor and a rogue judge will together concoct inappropriate, undemocratic, and ad hoc methods of effectuating service, thereby infringing on other sovereigns' jurisdiction and the defendant's rights.¹⁰⁷ This concern is somewhat less serious than it seems, however, because requests to invoke the residual service provision would likely be funneled through the DOJ's Office of International Affairs, which provides some systemic oversight by working in conjunction with the State Department on matters concerning foreign relations.¹⁰⁸ Still, such internal protections alone may be an insufficient check, and the

103. *Id.*

104. *Id.* The 2012 Recommendation notes that personal service may be provided by foreign governments themselves and is "the Department's preferred method of service." *Id.* at 8.

105. *See supra* notes 19–20 and accompanying text.

106. Memorandum from Lanny A. Breuer, *supra* note 83, at 7.

107. In addition to the noteworthy diplomatic concerns, similar infringements of sovereignty may also violate international law. *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 306 (6th ed. 2003) ("Persons may not be arrested, a summons may not be served, police or tax investigations may not be mounted, orders for production of documents may not be executed, on the territory of another state, except under the terms of a treaty or other consent given.").

108. *Office of International Affairs*, THE UNITED STATES DEP'T OF JUSTICE, <http://www.justice.gov/criminal/about/oia.html> (last visited Nov. 2, 2014). The Office of International Affairs already has mandatory supervision over the process of making formal requests for international extradition and provisional arrests of fugitives. THE UNITED STATES DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL 9-15.210 (1997), available at http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/15mcrn.htm#9-15.210.

residual service provision is the most contentious element of the 2012 Recommendation.

B. The Subcommittee's Revised Version

*Our age will be known as the age of committees.*¹⁰⁹

A subcommittee was appointed by the Advisory Committee to address the DOJ's suggested changes to Rule 4.¹¹⁰ After a series of meetings in which it examined the proposed revisions, the subcommittee unanimously recommended that Rule 4 be amended.¹¹¹ It also recommended three specific changes to the 2012 Recommendation.¹¹² First, the subcommittee suggested eliminating the mailing requirement for all service made on organizational defendants in the United States unless an authorizing statute so requires.¹¹³ Second, the subcommittee proposed expanding the list of available methods to effectuate service on defendants outside a judicial district of the United States.¹¹⁴ Finally, the subcommittee also addressed a question not posed by the 2012 Recommendation: What happens when an organizational defendant has been properly served but fails to appear?¹¹⁵

109. M.P. SINGH, QUOTE UNQUOTE (A HANDBOOK OF QUOTATIONS) 85 (2005) (quoting the late British publisher Ernest Benn).

110. The subcommittee was comprised of prominent experts in the field, including law professors, judges, practitioners, and representatives from the DOJ. For a full list of the subcommittee's members, see Draft Minutes, Advisory Comm. on Rules of Criminal Procedure (Apr. 25, 2013), *available at* <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2013-10.pdf>.

111. Memorandum from Sara Sun Beale & Nancy King, Reporters, Advisory Comm. on Rules of Criminal Procedure, to Members, Criminal Rules Advisory Comm. 1 (Sept. 24, 2013), *available at* <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2013-10.pdf>.

112. The Subcommittee's revisions were ultimately incorporated in the Advisory Committee's proposal that is seeking public comment through February 17, 2015. *See supra* note 17.

113. *Id.* at 2.

114. *Id.*

115. The subcommittee's proposed answer to this question would allow a court to "take any action authorized by law if an organizational defendant fails to appear in response to a summons." *Id.* at 1. The problem of an absentee defendant is not unique to Rule 4, and setting forth a complete solution falls far outside this Note's scope. Courts possess several tools to deal with recalcitrant defendants, most notably the contempt power. *See* 18 U.S.C. § 401(3) (2012) (granting each federal court the "power to punish by fine or imprisonment, or both . . . [d]isobedience or resistance to its lawful writ, process, order, rule, decree, or command"). Courts may even be empowered to appoint counsel for absent defendants. *See, e.g., United States v. Crosby*, 24 F.R.D. 15, 16 (S.D.N.Y. 1959) ("It would be idle to provide for summoning

The most significant difference between the subcommittee's proposed revision and the 2012 Recommendation is the list of options for making service outside a judicial district of the United States. Instead of five enumerated options under Rule 4(c)(3)(D)(ii), the subcommittee shortened the list to three.¹¹⁶ In addition to the change in form, the subcommittee also proposed substantial alterations to Rule 4(c)(3)(D)(ii)'s operative language.

Table 1. Possible Revisions to Rule 4

The DOJ's 2012 Recommendation	The Subcommittee's Proposed Revisions
<p>(D) A summons is served on an organization at a place not within a judicial district of the United States:</p> <p>(i) 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, in a manner authorized under the laws of the foreign jurisdiction where the officer or agent to be served is located, or</p> <p>(ii) by other means reasonably calculated to give notice, including</p> <p>(a) a stipulated means of service;</p> <p>(b) <u>a means that a foreign authority undertakes in response to a letter rogatory or letter of request;</u></p> <p>(c) <u>a means that a foreign authority undertakes in response to a request submitted under an applicable international agreement;</u></p> <p>(d) <u>a means otherwise permitted under an applicable international agreement;</u></p> <p>(e) <i>other means upon request of an attorney for the government, as the court orders.</i></p>	<p>(D) A summons is served on an organization not within a judicial district of the United States:</p> <p>(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 another agent appointed or legally authorized to receive service of process; or</p> <p>(ii) by any other means that gives notice, including one:</p> <p>(a) that the parties stipulate to;</p> <p>(b) <u>that a foreign authority undertakes in response to a letter rogatory, a letter of request, or a request submitted under an applicable international agreement;</u> or</p> <p>(c) <i>that is not prohibited by an applicable international agreement.</i>¹¹⁷</p>

The subcommittee's first three methods of making service, detailed in Subparts 4(c)(3)(D)(i), (ii)(a), and (ii)(b), incorporate and

a corporation if the court, after so doing, could not render judgment against it. The court must, therefore, have power to appoint one of its attorneys and officers to appear for the corporation.”).

116. Memorandum from Sara Sun Beale & Nancy King, *supra* note 111, at 130.

117. *Id.* (emphasis added). This version of the rule also includes purely stylistic changes. *Id.* at 9.

consolidate the provisions in the 2012 Recommendation premised on consent.¹¹⁸ The subcommittee viewed these provisions as “uncontroversial” and unlikely to harm other rights under domestic or international law.¹¹⁹

The subcommittee’s final proposed revision, Rule 4(c)(3)(D)(ii)(c), could raise serious legal and policy issues. This catchall provision was included to “provide[] flexibility” when the other three provisions cannot be met, and operates similarly to the 2012 Recommendation’s residual service provision.¹²⁰ Notably, however, the subcommittee’s revision dropped the 2012 Recommendation’s requirement that a court approve the alternative method of service by issuing a prospective order.¹²¹ Although the subcommittee’s revision generally tracked the language of the civil provision more closely than did the 2012 Recommendation,¹²² its abandonment of ex ante judicial approval for an alternative service mechanism deviates from the civil rules.¹²³ Therefore, if adopted, this catchall provision allowing service to be made without court approval would seem to be unique in federal procedural law.

Detractors could hypothesize a troubling situation in which service of a summons is made in a foreign country in contravention of that country’s laws and without its participation or consent. Further exacerbating the problem, the catchall provision may be invoked even when the government fails to show that it has exhausted Rule 4’s other options.¹²⁴ As a result, prosecutors may freely elect to infringe on foreign sovereigns’ autonomy without prior judicial approval, whether or not less controversial means of effectuating service are available. According to the subcommittee’s survey of the civil

118. *Id.* at 6. For a discussion of the analogous provisions in the 2012 Recommendation, see *supra* notes 99–104 and accompanying text.

119. Memorandum from Sara Sun Beale & Nancy King, *supra* note 111, at 6.

120. *Id.* Compare *id.* at 130 (allowing service to be made “by any other means that gives notice, including one . . . that is not prohibited by an applicable international agreement”), with Memorandum from Lanny A. Breuer, *supra* note 83, at 7 (allowing service to be made “by other means reasonably calculated to give notice, including . . . other means upon request of an attorney for the government, as the court orders”).

121. Memorandum from Sara Sun Beale & Nancy King, *supra* note 111, at 7.

122. See FED. R. CIV. P. 4(f)(3) (allowing service to be made “by other means not prohibited by international agreement, as the court orders”).

123. *Id.*

124. See Memorandum from Sara Sun Beale & Nancy King, *supra* note 111, at 6 n.8 (“The Subcommittee considered and rejected a[n exhaustion] requirement.”).

analogue, this potential consequence “appeared to have generated significant concern.”¹²⁵

The subcommittee omitted an ex ante-approval requirement for use of the catchall provision because it felt that courts should not impinge on the executive branch’s constitutional primacy in foreign relations.¹²⁶ Under a service regime that does not require prior court approval, judges need not condone a violation of international or foreign law to establish U.S. jurisdiction over a given case.¹²⁷ Instead, the “executive alone” will be responsible for determining whether the “public interest” warrants violating international or foreign law in a particular case.¹²⁸ Although the subcommittee believed such cases would arise only “rare[ly],” the catchall provision affords the executive branch “the necessary flexibility” to act “in an efficient and effective manner”¹²⁹—unilaterally, if need be. In contrast to the 2012 Recommendation, the subcommittee placed the responsibility for invoking the catchall provision squarely on the executive’s shoulders.¹³⁰

Although the current jurisdictional gap in Rule 4 was likely created inadvertently,¹³¹ it may have conveniently excused the courts from grappling with the implications of the vast overseas expansion of federal criminal law in hard cases. Revising Rule 4 may force the courts to resolve several difficult questions obviated by the current jurisdictional gap.

III. THE LIMITS OF EXTRATERRITORIAL APPLICATION OF U.S. LAW

Service of process is only one requirement for properly commencing a prosecution against a foreign organization in the United States. Congress must have first passed a law criminalizing the defendant’s conduct pursuant to one of its enumerated powers. A court must also interpret that law to be fairly susceptible of

125. *Id.* at 7.

126. *Id.* at 8.

127. *Id.* at 7.

128. *Id.* at 8.

129. *Id.*

130. Entrusting this power to the executive’s discretion created its own tension. Several members “expressed support” for requiring individual prosecutors to receive prior approval from the Attorney General or the Deputy Attorney General in order to invoke the catchall provision. *Id.* at 9. Although such a requirement “might be desirable,” the Advisory Committee customarily declines to “dictate” internal DOJ policy. *Id.*

131. *See supra* notes 47–52 and accompanying text.

extraterritorial application. Finally, the prosecution may not violate the defendant's due-process rights.¹³² Part III provides an overview of the legal environment upon which a revised Rule 4 would be superimposed. It then highlights potential Fifth Amendment concerns raised by Rule 4's revision.

A. *The Constitution's Structural Limits*

As a matter of first principle, Congress may create federal crimes only if the Constitution expressly or impliedly empowers it to do so and if doing so would not violate another constitutional provision.¹³³ The Constitution does not categorically bar Congress from proscribing criminal conduct outside U.S. geographical boundaries, and several enumerated Article I powers specifically contemplate extraterritorial legislation.¹³⁴ These powers include: the power to "regulate Commerce with foreign Nations,"¹³⁵ the power to "coin Money, regulate the Value thereof, and of foreign Coin,"¹³⁶ and the power to "define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations."¹³⁷ When coupled with the Necessary and Proper Clause,¹³⁸ courts have been willing to construe Congress's authority to enact extraterritorial legislation very broadly.¹³⁹ For example, the Foreign Commerce Clause, although distinct from its domestic counterparts,¹⁴⁰ has been given a similarly expansive breadth.¹⁴¹ In short, the Constitution's structure constrains

132. U.S. CONST. amend. V. This Note expresses no view on what differences, if any, similar state prosecutions would face under a Fourteenth Amendment due-process analysis.

133. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES § 3.1 at 238 (4th ed. 2011).

134. CHARLES DOYLE, CONG. RESEARCH SERV., No. 94-166, EXTRATERRITORIAL APPLICATION OF AMERICAN CRIMINAL LAW 1 (2012).

135. U.S. CONST. art. I, § 8, cl. 3.

136. U.S. CONST. art. I, § 8, cl. 5.

137. U.S. CONST. art. I, § 8, cl. 10.

138. U.S. CONST. art. I, § 8, cl. 18.

139. *See, e.g.*, *United States v. Belfast*, 611 F.3d 783 (11th Cir. 2010) (upholding application of the Torture Act to the defendant's use of torture in Liberia as a valid exercise of the treaty power and the Necessary and Proper Clause).

140. U.S. CONST. art. I, § 8, cl. 3.

141. *See, e.g.*, *United States v. Clark*, 435 F.3d 1100, 1103 (9th Cir. 2006) ("Where, as in this appeal, the defendant travels in foreign commerce to a foreign country and offers to pay a child to engage in sex acts, his conduct falls under the broad umbrella of foreign commerce and consequently within congressional authority under the Foreign Commerce Clause."). *But see* *United States v. Yunis*, 681 F. Supp. 896, 907 n.24 (D.D.C. 1988) ("[Congress] is not empowered to regulate foreign commerce which has no connection to the United States. Unlike the states,

the extraterritorial activity Congress may proscribe, but this constraint's exact limits remain nebulous.¹⁴² Thus, rather than claiming that Congress lacks the power to proscribe extraterritorial conduct, defendants challenging a prosecution will more likely succeed by arguing that their particular actions were not covered as a matter of statutory construction.

B. The Role of International Law in Statutory Construction

The judicial practice of statutory construction limits the reach of U.S. law over foreign defendants by creating a set of interpretive default rules. As a matter of domestic constitutional law, Congress is not bound by international law when it proscribes extraterritorial conduct.¹⁴³ Whether or not international law itself is binding under U.S. law,¹⁴⁴ it does play an important interpretive role. Congress may legislate to “supersede[]” a principle of international law when its intent is “clear” and the resulting conflict cannot be “fairly reconciled.”¹⁴⁵ Congress can demonstrate its intent to proscribe extraterritorial conduct in a number of ways, such as by enacting laws specifically targeting foreign conduct or drafting extraterritoriality provisions that expressly delimit the scope of its legislation.¹⁴⁶ Absent an explicit statement of a statute's geographic scope, courts rely on

foreign nations have never submitted to the sovereignty of the United States government nor ceded their regulatory powers to the United States.”).

142. See Curtis A. Bradley, *Universal Jurisdiction and U.S. Law*, 2001 U. CHI. LEGAL F. 323, 337 (2001) (“[T]he scope of the Define and Punish Clause is unclear, the Foreign Commerce Clause is not limitless, . . . and . . . treaties may not extend to . . . citizens of non-party countries.”).

143. See, e.g., *Barrera-Echavarría v. Rison*, 44 F.3d 1441, 1450–51 (9th Cir. 1995).

144. International law in this context refers to customary international law. Agreements with other nations have the full force of federal law, as long as Congress has properly given them effect. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 111 (1987). The extent to which customary international law is part of the law of the United States, and in what fashion, is a subject of much scholarly debate that this Note does not attempt to address. For a discussion, see generally T. Alexander Aleinikoff, *International Law, Sovereignty, and American Constitutionalism: Reflections on the Customary International Law Debate*, 98 AM. J. INT'L L. 91 (2004); Curtis A. Bradley & Jack L. Goldsmith, *Customary International Law as Federal Common Law: A Critique of the Modern Position*, 110 HARV. L. REV. 815 (1997); Louis Henkin, *International Law as Law in the United States*, 82 MICH. L. REV. 1555 (1984); Harold Hongju Koh, Commentary, *Is International Law Really State Law?*, 111 HARV. L. REV. 1824 (1998).

145. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 115(1)(a) (1987).

146. Podgor, *supra* note 80, at 329–35.

other techniques to resolve this “haziest” situation.¹⁴⁷ Two canons of statutory construction function as default rules to address this potential uncertainty: the presumption against extraterritorial application and the *Charming Betsy* canon.¹⁴⁸

1. *The Presumption Against Extraterritorial Application.* The first relevant canon of statutory construction that limits the reach of U.S. law over foreign defendants is the presumption against extraterritorial application. The Supreme Court has recently restated the presumption: “[W]hen a statute gives no clear indication of an extraterritorial application, it has none.”¹⁴⁹ The presumption “serves to protect against unintended clashes between [U.S.] laws and those of other nations which could result in international discord.”¹⁵⁰ Foreign defendants accused of criminal conduct abroad may be able to invoke the presumption successfully when Congress has failed to address the governing statute’s scope.¹⁵¹

Regardless of other expressions of Congressional intent, the very decision to proscribe certain categories of behavior will overcome the presumption against extraterritorial application because of the inherent nature of that conduct.¹⁵² In *United States v. Bowman*,¹⁵³ the Supreme Court first announced its two-part test to determine whether particular conduct is of such a nature as to overcome the presumption against extraterritorial application. As Chief Justice Taft explained, “The necessary locus, when not specifically defined, depends on the purpose of Congress as evinced by the description and nature of the crime and upon the territorial limitations upon the

147. *Id.* at 335.

148. For a discussion of the inconsistent ways in which these canons have been applied, see generally John H. Knox, *A Presumption Against Extrajurisdictionality*, 104 AM. J. INT’L L. 351 (2001).

149. *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013) (quoting *Morrison v. Nat’l Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010)).

150. *Id.* (quoting *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991)).

151. For a discussion of the likely, but yet uncertain, application of the presumption against extraterritorial application in the criminal context, see generally S. Nathan Williams, Note, *The Sometimes “Craven Watchdog”: The Disparate Criminal–Civil Application of the Presumption Against Extraterritoriality*, 63 DUKE L.J. 1381 (2014).

152. The range of proscribed conduct exempt from the presumption against extraterritorial application has led some commentators to advocate its revision or complete abolition. See Gary B. Born, *A Reappraisal of the Extraterritorial Reach of U.S. Law*, 24 LAW & POL’Y INT’L BUS. 1, 1 (1992) (arguing that the presumption is “obsolete” and “should be abandoned”); Knox, *supra* note 148, at 353 (arguing for a “clarified” version).

153. *United States v. Bowman*, 260 U.S. 94 (1922).

power and jurisdiction of a government to punish crime under the law of nations.”¹⁵⁴ Crimes such as espionage,¹⁵⁵ theft of government property,¹⁵⁶ and treason¹⁵⁷—which are not “logically dependent on their locality for the Government’s jurisdiction”¹⁵⁸—are considered so critical to national security that Congress is presumed to have proscribed qualifying conduct wherever it may occur.

Under the *Bowman* framework, courts must attempt to distill the essential nature of a range of criminal offenses to determine whether the presumption against extraterritorial application is animated. As Professor Ellen Podgor observes, “Since Congress has often failed to focus on extraterritoriality in drafting statutes, courts are frequently left to consider the international ramifications of an extraterritorial application.”¹⁵⁹ The cabining effects of the presumption against extraterritorial application will thus vary from case to case,¹⁶⁰ but the presumption remains a viable shield for foreign defendants seeking to ward off uncertain U.S. jurisdiction.

2. *The Charming Betsy Canon.* The second canon of statutory construction that limits the scope of Congressional jurisdiction over foreign conduct is the *Charming Betsy* canon. This historically well-rooted canon originates from Chief Justice Marshall’s opinion in

154. *Id.* at 97–98 (emphasis omitted). The modern restatement of the *Bowman* test requires that courts (1) “look to the text of the statute for an indication that Congress intended it to apply extraterritorially,” and (2) examine whether “extraterritorial jurisdiction comports with principles of international law.” *United States v. Neil*, 312 F.3d 419, 421 (9th Cir. 2002). Under international law, states possess the jurisdiction to prescribe, adjudicate, and enforce, all of which are subject to various substantive and procedural limits. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 401 (1987).

155. *See United States v. Zehe*, 601 F. Supp. 196, 197–98 (D. Mass. 1985) (“Because espionage is an offense threatening the national security of the United States, regardless of where it occurs, the Court readily concludes [its proscription] was meant to apply extraterritorially to citizens.”).

156. *See United States v. Cotton*, 471 F.2d 744, 750 (9th Cir. 1973) (“It is inconceivable that Congress . . . would proscribe only the theft of government property located within the territorial boundaries of the nation.”).

157. *See Chandler v. United States*, 171 F.2d 921, 930 (1st Cir. 1948) (“The nature of treason, therefore, is such that there is no a priori reason for supposing that the Congress would naturally be inclined to restrict [its] definition . . . within the territorial limits of the United States.”).

158. *Bowman*, 260 U.S. at 98.

159. Podgor, *supra* note 80, at 340.

160. At least one court has suggested that *Bowman* is distinguishable when the defendant is not a citizen of the United States. *United States v. Pizzarusso*, 388 F.2d 8, 9 n.2 (2d Cir. 1968).

Murray v. Schooner Charming Betsy,¹⁶¹ in which the court announced: “[A]n act of Congress ought never to be construed to violate the law of nations if any other possible construction remains”¹⁶² The *Charming Betsy* canon counsels that, absent clear evidence to the contrary, Congress does not intend to disrupt the international legal order through domestic legislation.¹⁶³ The canon operates primarily as a “braking mechanism” to limit the scope of federal law, but as with the presumption against extraterritorial application, its precise interpretative force remains “somewhat uncertain.”¹⁶⁴

The *Charming Betsy* canon may prove an effective shield for defendants whose prosecution would violate norms of customary international law, even when Congress clearly intended to grant extraterritorial application. In *United States v. Ali*,¹⁶⁵ for example, the D.C. Circuit relied on the *Charming Betsy* canon to “check the exercise of U.S. criminal jurisdiction.”¹⁶⁶ The court dismissed the relevant charge after finding that conspiracy to commit piracy was not a cognizable offense under international law.¹⁶⁷ It specifically rejected the government’s argument that the general federal conspiracy statute¹⁶⁸ evinced a sufficiently clear intent to overcome the canon’s protection.¹⁶⁹ As *Ali* demonstrates, the *Charming Betsy* canon imbues U.S. law with the force of international law in the process of statutory interpretation that, like the presumption against extraterritorial application, constrains Congress’s power to proscribe conduct abroad.

161. *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64 (1804).

162. *Id.* at 118. The Supreme Court had actually articulated a similar version of the *Charming Betsy* canon several years earlier. *See Talbot v. Seeman*, 5 U.S. (1 Cranch) 43 (1801) (“[T]he laws of the United States ought not, if it be avoidable, so to be construed as to infract the common principles and usages of nations.”).

163. With slight alteration in language, the *Charming Betsy* canon has been codified in the influential *Restatement (Third) of the Foreign Relations Law of the United States*. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 141 (1987).

164. Curtis A. Bradley, *The Charming Betsy Canon and Separation of Powers: Rethinking the Interpretive Role of International Law*, 86 GEO. L.J. 479, 484 (1998); *see id.* at 490 (arguing that the *Charming Betsy* canon’s main thrust is interpretive, and that the canon “is best thought of today as a device to preserve the proper separation of powers between the three branches of the government”).

165. *United States v. Ali*, 718 F.3d 929 (D.C. Cir. 2013).

166. *Id.* at 935.

167. *Id.* at 936–42. The court did find, however, that aiding and abetting piracy was an offense recognized under international law and so upheld those charges. *Id.*

168. 18 U.S.C. § 371 (2012).

169. *Ali*, 718 F.3d at 942.

C. *Fifth Amendment Due Process*

Even when Congress possesses the enumerated power to proscribe extraterritorial conduct and displaces the interpretive default rules discussed above, defendants' individually enforceable due-process rights may preclude U.S. prosecution. In their seminal article *Federal Extraterritoriality and Fifth Amendment Due Process*, Professors Lea Brilmayer and Charles Norchi set out the first comprehensive treatment of the Constitution's individual-rights protections against federal prosecutions of conduct occurring abroad.¹⁷⁰ Brilmayer and Norchi argued that the "increasingly unilateral and aggressive character" of applying U.S. law extraterritorially could give rise to due-process challenges.¹⁷¹ While acknowledging that this trend raises sensitive policy concerns, they suggested that if courts "are to become involved, they must do so in a manner consistent with the Constitution."¹⁷² Following the publication of their article, foreign defendants have continued to raise due-process challenges frequently,¹⁷³ even though no federal court has yet invalidated a prosecution on due-process grounds.¹⁷⁴ The Supreme Court has not yet definitively ruled on this issue, and the circuits remain split over how to analyze due-process challenges between two divergent frameworks: the sufficient-nexus test and the fundamental-fairness test.

170. Lea Brilmayer & Charles Norchi, *Federal Extraterritoriality and Fifth Amendment Due Process*, 105 HARV. L. REV. 1217, 1261–62 (1992).

171. *Id.* at 1223.

172. *Id.* Brilmayer's and Norchi's work has generated extensive commentary offering competing conceptions of the Fifth Amendment's protections for foreign defendants. See Anthony J. Coangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 HARV. INT'L L.J. 121, 124 (2007) (arguing for a due-process test that incorporates principles of international law); Mark Weisburd, *Due Process Limits on Federal Extraterritorial Legislation?*, 35 COLUM. J. TRANSNAT'L L. 379, 381 (1997) (arguing that the Fifth Amendment, unlike the Fourteenth Amendment, places no territorial limits on Congressional legislative authority); see also Bradley, *supra* note 142, at 338 (observing that "it may be logically awkward for a defendant to rely on what could be characterized as an extraterritorial application of the U.S. Constitution in an effort to block the extraterritorial application of U.S. law"); Stephan, *supra* note 100, at 833 ("Although the Supreme Court has not definitively resolved the matter, it generally has indicated that overseas aliens enjoy no constitutional protection.").

173. See, e.g., *United States v. Reumayr*, 530 F. Supp. 2d 1210, 1223 (D.N.M. 2008) (citing Brilmayer & Norchi, *supra* note 170, at 1221 n.12).

174. *United States v. Ali*, 718 F.3d 929, 944 n.7 (D.C. Cir. 2013); *Reumayr*, 530 F. Supp. 2d at 1223. One district court has found a violation of due process for an "arbitrary and fundamentally unfair" drug-conspiracy prosecution, but its ruling was reversed on appeal. *United States v. Caicedo*, 47 F.3d 370, 371 (9th Cir. 1995).

1. *The Sufficient-Nexus Test.* The sufficient-nexus test requires that there be a *minimum amount of contact* between the defendant and the United States so that application of U.S. law is not “arbitrary or fundamentally unfair.”¹⁷⁵ In applying this test, courts weigh “a wide range of factors” to determine whether a prosecution comports with due process.¹⁷⁶ A sufficient-nexus requirement “serves the same purpose as the minimum contacts test in personal jurisdiction” by guaranteeing the court’s jurisdiction over “a defendant who should reasonably anticipate being haled into court in this country.”¹⁷⁷ Courts have construed this notice requirement very broadly by upholding prosecutions for conduct that put the defendant on notice of prosecution “*somewhere*” in the world, even if the defendant could not reasonably have anticipated being prosecuted in the *United States*.¹⁷⁸ Three circuits have adopted the sufficient-nexus test: the Second,¹⁷⁹ Fourth,¹⁸⁰ and Ninth Circuits.¹⁸¹

The best exposition of the sufficient-nexus test appears in *United States v. Davis*,¹⁸² which involved a prosecution under the Maritime Drug Law Enforcement Act (MDLEA). The defendant, the captain of a ship ostensibly traveling from Hong Kong to the Caribbean via Mexico, was indicted after the Coast Guard discovered seven thousand pounds of marijuana during a maritime raid thirty-five miles from Point Reyes, California.¹⁸³ Davis challenged U.S. jurisdiction

175. *United States v. Davis*, 905 F.2d 245, 248–49 (9th Cir. 1990).

176. *See United States v. Brehm*, No. 1:11-cr-11, 2011 WL 1226088, at *4 (E.D. Va. Mar. 30, 2011) (noting that these factors include “(1) the defendant’s actual contacts with the United States, including his citizenship or residency; (2) the location of the acts allegedly giving rise to the alleged offense; (3) the intended effect a defendant’s conduct has on or within the United States; and (4) the impact on significant United States interests”), *aff’d*, 691 F.3d 547 (4th Cir. 2012).

177. *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1257 (9th Cir. 1998) (quotation marks omitted). *But see United States v. Perez Oviedo*, 281 F.3d 400, 403 (3d Cir. 2002) (finding the use of civil personal-jurisdiction precedents in criminal cases to be “inapposite”).

178. *United States v. Al Kassar*, 660 F.3d 108, 119 (2d Cir. 2011) (emphasis added) (finding that arms trafficking to terrorists in Spain and Central America created sufficient notice); *see also United States v. Brehm*, 691 F.3d 547, 554 (4th Cir. 2012) (finding that the stabbing of a fellow contractor at a military base in Afghanistan created sufficient notice).

179. *United States v. Yousef*, 327 F.3d 56, 111 (2d Cir. 2003).

180. *United States v. Mohammad-Omar*, 323 F. App’x 259, 261 (4th Cir. 2009) (per curiam).

181. *United States v. Davis*, 905 F.2d 245, 248–49 (9th Cir. 1990). The Ninth Circuit has abandoned its nexus requirement for prosecutions involving stateless vessels, however, relying instead on principles of international law. *United States v. Caicedo*, 47 F.3d 370, 372 (9th Cir. 1995).

182. *Davis*, 905 F.2d at 245.

183. *Id.* at 247.

over his conduct as a matter of due process.¹⁸⁴ The Ninth Circuit rejected his claim, finding that the evidence presented to the district court was sufficient to establish jurisdiction under the sufficient-nexus approach.¹⁸⁵ International law played a critical role in the court's due-process analysis.¹⁸⁶ The court cautioned, however, that this inquiry into international law should not cause it to "lose sight of the ultimate question: would application of the statute to the defendant be arbitrary or fundamentally unfair?"¹⁸⁷ Although the court failed to incorporate international law as the test for due process, it did note that international-law principles "may be useful as a rough guide" to determine whether a sufficient nexus exists between the defendant and the United States.¹⁸⁸

International law provides five distinct bases of jurisdiction. The most significant source of jurisdiction is the "territorial principle," which grants a state jurisdiction over its own territory.¹⁸⁹ The territorial principle extends to conduct that has, or is intended to have, substantial domestic effects.¹⁹⁰ Second, the "nationality principle" grants jurisdiction over a state's citizens who commit offenses outside that state's territory.¹⁹¹ Third, the "passive personality" principle grants jurisdiction over extraterritorial actions that affect a state's nationals abroad.¹⁹² Fourth, the "protective principle" grants jurisdiction over conduct that threatens a state's own security or the integrity of its governmental functioning, such as espionage or counterfeiting.¹⁹³ Finally, a narrow band of crimes may be so widely condemned among the community of nations as to warrant "universal jurisdiction," under which any state has the jurisdiction to prosecute perpetrators of these offenses.¹⁹⁴ Offenses conferring universal jurisdiction include piracy; genocide; war crimes;

184. *Id.*

185. *Id.* at 249.

186. In a footnote, the court mentioned that its previous decisions had discussed constitutional requirements "simultaneously" with principles of international law. *Id.* at 249 n.2.

187. *Id.*

188. *Id.*

189. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402(1) cmt. c (1987).

190. *Id.* § 402(1)(c) cmt. b.

191. *Id.* § 402(2) cmt. e.

192. *Id.* § 402(2) cmt. g.

193. *Id.* § 402(3) cmt. f.

194. *Id.* § 404.

and, in certain instances, terrorism.¹⁹⁵ These five bases of jurisdiction under international law implicate most potential U.S. interests in prosecuting extraterritorial conduct. Courts employing the “rough guide” of international law to define the limits of due process under the sufficient-nexus test will therefore find that the vast majority of factual scenarios fit under one or more of these jurisdictional bases (and thus satisfy due process).¹⁹⁶

2. *The Fundamental-Fairness Test.* Some courts have adopted another standard to assess due-process challenges to prosecutions of extraterritorial conduct: the fundamental-fairness test. The fundamental-fairness test turns entirely on the “ultimate question” of the sufficient-nexus test—whether “application of the statute to the defendant [would] be arbitrary or fundamentally unfair.”¹⁹⁷ The fundamental-fairness test’s rationale resembles the principle that “no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed.”¹⁹⁸ Courts have construed this notice principle quite loosely, suggesting that some criminal conduct may be so self-evidently illegal that its commission provides sufficient notice for defendants to be tried in the United States, no matter where the underlying conduct occurred.¹⁹⁹ As with the sufficient-nexus test, courts often invoke principles of international law for guidance in assessing the fairness of a particular prosecution.²⁰⁰ Given the similarity of these two standards, perhaps the “difference [between them] is less real than apparent.”²⁰¹ So far,

195. *Id.* § 404 cmt. b; *id.* § 404 Reporters’ Note 1.

196. *See* Brilmayer & Norchi, *supra* note 170, at 1263 (predicting that “Fifth Amendment due process problems of federal extraterritoriality will be rare”).

197. *United States v. Ali*, 718 F.3d 929, 944 (D.C. Cir. 2013) (quoting *United States v. Davis*, 905 F.2d 245, 248–49 (9th Cir. 1990)).

198. *Bouie v. City of Columbia*, 378 U.S. 347, 351 (1964) (quoting *United States v. Harriss*, 347 U.S. 612, 617 (1954)).

199. *See United States v. Al Kassar*, 660 F.3d 108, 119 (2d Cir. 2011) (terrorism); *United States v. Martinez-Hidalgo*, 993 F.2d 1052, 1052 (3d Cir. 1993) (drug trafficking).

200. *See, e.g., United States v. Suerte*, 291 F.3d 366, 375–76 (5th Cir. 2002) (relying on the “law of the flag” to uphold jurisdiction over a Maltese ship stopped in Venezuela); *United States v. Cardales*, 168 F.3d 548, 553 (1st Cir. 1999) (upholding U.S. jurisdiction of drug-trafficking offense under the “protective principle” because “all drug trafficking aboard vessels threatens our nation’s security”).

201. *See United States v. Shahani-Jahromi*, 286 F. Supp. 2d 723, 728–29 n.9 (E.D. Va. 2003) (“[T]he existence of a nexus is what makes the prosecution neither arbitrary nor fundamentally unfair.”).

five circuits have, at least implicitly, adopted the fundamental-fairness approach: the First,²⁰² Third,²⁰³ Fifth,²⁰⁴ Eleventh,²⁰⁵ and D.C. Circuits.²⁰⁶

Like the sufficient-nexus approach, the fundamental-fairness test is unlikely to give rise to successful due-process challenges, as exemplified by the *Ali* case discussed above.²⁰⁷ *Ali* involved a Somali national who acted as a negotiator and interpreter in a hostage-taking incident in the Gulf of Aden.²⁰⁸ The victim of the hostage plot, the *CEC Future*, was a Danish-owned ship flying a Bahamian flag, carrying the cargo of a U.S. company.²⁰⁹ Only a “brief period of ‘minutes’” occurred on the “high seas,” as the great bulk of the incident occurred in foreign territorial water.²¹⁰ The defendant, also the “Director General of the Ministry of Education for the Republic of Somaliland” (a semiautonomous region of Somali), was indicted after flying into Washington, D.C., to attend an education conference in Raleigh, North Carolina, set up as a “ruse” by the government.²¹¹ *Ali*’s extraordinary factual record underscores the occasionally tenuous connection between prosecutors’ charges and defendants’ connection to the United States.²¹²

202. *Cardales*, 168 F.3d at 553. Judge Torruella, dissenting from a decision to not readdress the appropriate due-process standard en banc, found the lack of a sufficient-nexus requirement “suspect” because a federal prosecution lacking such a nexus would exceed the scope of Congress’s enumerated powers. *United States v. Angulo-Hernandez*, 576 F.3d 59, 60–62 (1st Cir. 2009) (Torruella, J., dissenting). Judge Torruella would have found “compliance with international law [to be] necessary but not sufficient” to satisfy due process. *Id.*

203. *Martinez-Hidalgo*, 993 F.2d at 1053.

204. *United States v. Alvarez-Mena*, 765 F.2d 1259, 1266–67 (5th Cir. 1985).

205. *United States v. Ibarquen-Mosquera*, 634 F.3d 1370, 1376 (11th Cir. 2011).

206. *See United States v. Ali*, 718 F.3d 929, 943–46 (D.C. Cir. 2013) (considering any nexus requirement to be a proxy for determining whether a prosecution would be “arbitrary or fundamentally unfair,” though not explicitly adopting the fundamental-fairness approach).

207. *See supra* notes 165–69 and accompanying text.

208. *Ali*, 718 F.3d at 933.

209. *Id.*

210. *Id.*

211. *Id.* *Ali* was originally arrested by Somaliland security forces after appearing in a documentary, *STOLEN SEAS: TALES OF SOMALI PIRACY* (Brainstorm Media 2012), before his invitation to and subsequent arrest in the United States. Shashank Bengali, *U.S. ‘Overreaching’ in Piracy Case Against Somali, Judge Says*, L.A. TIMES, Nov. 6, 2013, <http://www.latimes.com/nation/la-na-pirate-negotiator-20131106,0,3540136.story#axzz2ju6RC8r2>. The *Ali* prosecution was not the first time federal prosecutors have generated serious due-process concerns by luring defendants to the United States. *See United States v. Ayes*, 702 F.3d 162, 165 (4th Cir. 2012) (describing how prosecutors used the “pretext of attending a training seminar” to ensnare a Jordanian citizen suspected of stealing funds from the U.S. Embassy in Baghdad).

212. In similar cases in which a defendant is only in the country “transitorily,” the *Restatement* suggests that courts would lack jurisdiction to adjudicate earlier conduct occurring

Despite this uncommonly weak connection to the United States, the *Ali* court ruled that the prosecution did not violate due process.²¹³ The court found that the International Convention Against the Taking of Hostages,²¹⁴ whose implementing legislation formed the basis of the charges against the defendant, provided “global notice” sufficient to satisfy the demands of the Fifth Amendment, even though Somalia is not a signatory to the Convention.²¹⁵ The court strongly suggested that, as long as the law is determined to apply extraterritorially as a matter of statutory construction, the Fifth Amendment does not impose additional limits on the extraterritorial application of federal criminal law.²¹⁶ Under the *Ali* court’s logic, it is hard to imagine a prosecution of a natural person that would violate due process under either the sufficient-nexus test or the fundamental-fairness test. If the relevant conduct fails to create jurisdiction, prosecutors are unlikely to spend their limited time and resources pursuing wholly foreign conduct that would not confer a jurisdictional basis under the “rough guide”²¹⁷ of international law.²¹⁸

In contrast to prosecutions of natural persons, the aggressive pursuit of foreign organizational defendants may be more likely to run afoul of due process because the proscribed conduct will likely be limited to large-scale market offenses—*mala prohibita* rather than

abroad. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 421(2)(a) (1987). Federal courts’ jurisdiction to adjudicate may actually be broader than the *Restatement* suggests, however, given developments since the publication of its latest edition in 1987. In a plurality opinion authored by Justice Scalia, the Supreme Court held transient jurisdiction to be permissible, regardless of its reasonableness, because it was in line with “traditional notions of fair play and substantial justice” as understood (perhaps mistakenly) at the time of the Fourteenth Amendment’s adoption. See *Burnham v. Super. Ct. of Cal.*, 495 U.S. 604, 610–22 (1991).

At least one circuit has extended *Burnham* to apply to foreign persons in the same fashion as to U.S. nationals. *First Am. Corp. v. Price Waterhouse LLP*, 154 F.3d 16, 20–21 (2d Cir. 1998). *But see Connecticut v. Zakharov*, 667 F.3d 705, 715–16 (6th Cir. 2012) (declining to extend *Burnham* to foreign defendants); Peter Hay, Comment, *Transient Jurisdiction, Especially Over International Defendants: Critical Comments on Burnham v. Superior Court of California*, 1990 U. ILL. L. REV. 593, 602–03 (1990) (“In an international context, an unqualified, unremitting rule of transient jurisdiction seems quite intolerable and is unfitting.”).

213. *Ali*, 718 F.3d at 946.

214. International Convention Against the Taking of Hostages, *opened for signature* 17 Dec. 1979, 1316 U.N.T.S. 205.

215. *Id.* at 944–45.

216. *Id.* at 946.

217. *United States v. Davis*, 905 F.2d 245, 249 n.2 (9th Cir. 1990).

218. See *supra* notes 189–96 and accompanying text.

*mala in se*²¹⁹—which may fail to satisfy the notice requirement at the heart of Fifth Amendment due process.²²⁰ Part IV considers this possibility and its importance in the ongoing effort to revise Rule 4 to allow greater flexibility in serving summonses on foreign organizational defendants.

IV. ASSESSING THE IMPACT OF REVISING RULE 4

Revising Rule 4 to eliminate its jurisdictional gap may give rise to new Fifth Amendment challenges, as cases that would have stalled or would have been dismissed for failure to properly effectuate service²²¹ will come squarely before the federal courts. In addition to eliminating Rule 4's jurisdictional gap, the 2012 Recommendation and the subcommittee's proposed changes afford the government expanded powers to serve foreign organizational defendants. This expanded power itself may raise due-process concerns, in addition to facilitating prosecutorial overreach and threatening international comity. The efforts to revise Rule 4 also strike a new equilibrium between the judicial and executive branches in foreign affairs.

This Note argues that, despite these concerns, the jurisdictional gap should be eliminated and Rule 4 revised accordingly because the application of federal criminal law should not turn on whether a domestic mailing could be made to organizational defendants. Although expanding the United States' reach over foreign organizational defendants may increase the likelihood of due-process violations, the revision also implicates a logically prior concern—prosecutorial overreach—that must be confronted directly in order to avoid potential abuses.

A. *The Exacerbation of Due-Process Concerns*

No court has yet addressed a foreign organizational defendant's Fifth Amendment challenge to prosecution in the United States. The prospects for such a challenge remain unclear. The unique treatment

219. See Michael L. Tavers, Comment, *Mistake of Law in Mala Prohibita Crimes*, 62 U. CHI. L. REV. 1301, 1321 (1995) (“Unlike sanctions for violations of *mala in se* statutes, punishment for a *malum prohibitum* crime cannot be justified on the grounds that the defendant's failure to know the law is in itself blameworthy.”).

220. Cf. *Ratzlaf v. United States*, 410 U.S. 135, 144, 149 (1994) (imposing an actual-knowledge requirement because currency structuring is not “inevitably nefarious” (footnote omitted)).

221. *United States v. Johnson Matthey PLC*, No. 2:06-cr-169, 2007 WL 2254676, at *1 (D. Utah, Aug. 2, 2007).

of organizational entities under U.S. law may render the above due-process analysis²²² entirely inapposite. In the civil context, the Supreme Court has failed to generate a majority approach for determining the proper test for personal jurisdiction over organizational parties that enter the stream of international commerce.²²³ The Court has remained deadlocked, unable to strike a majority position that balances the sovereign “authority” over foreign organizations against the due-process protections parties enjoy as “a matter of individual liberty.”²²⁴ Given the sensitive public interests implicated in the criminal context, organizational defendants may simply lack many, if not all, due-process protections.²²⁵

There is good reason to believe, however, that nonnatural defendants will be granted some level of due-process rights in this context, even if such rights are not coterminous with those of natural persons. In the wake of *Citizens United v. FEC*,²²⁶ the continued expansion of organizational entities’ constitutional rights beyond political spending seems likely.²²⁷ Prosecutions of organizational defendants can be analyzed similarly to those of natural defendants for purposes of jurisdiction and fairness because the question is ultimately one of federal authority vis-à-vis the defendant, not of the defendant’s organizational nature.²²⁸ Thus, these prosecutions do not raise many of the theoretical difficulties faced in other areas.

Assuming that the courts will adopt organizational due-process standards similar to those for natural persons, this Note argues that aggressive extraterritorial application of federal criminal law to foreign organizational defendants could violate the Fifth Amendment under certain circumstances. At the outset, it is important to highlight

222. See *supra* Part III.C.

223. See *J. McIntyre Mach., Ltd. v. Nicastro*, 131 S. Ct. 2780 (2011) (failing to garner a majority approach); *Asahi Metal Indus. Co. v. Super. Ct. of Cal.*, 580 U.S. 102 (1987) (same).

224. *Nicastro*, 131 S. Ct. at 2789 (Kennedy, J., plurality opinion).

225. Moreover, whether and to what extent foreign defendants are permitted to exercise these constitutional rights remains an open question. For a discussion, see generally Stephan, *supra* note 100.

226. *Citizens United v. Fed. Election Comm’n*, 130 S. Ct. 876 (2010).

227. See, e.g., Michael S. Kang, *After Citizens United*, 44 IND. L. REV. 243, 243 (2010) (“Although much of the immediate reaction to *Citizens United* focused on the decision’s short-term impact on political spending, the doctrinal impact of the decision is likely to be more significant.”).

228. See *Nicastro*, 131 S. Ct. at 2789 (“This Court’s precedents make clear that it is the defendant’s actions, not his expectations, that empower a State’s courts to subject him to judgment.”).

these circumstances in order to understand the vision of U.S. law enforcement they imply. Regularly undertaking aggressive prosecutions that do not implicate substantial domestic interests would threaten to transform the U.S. Attorneys into the world's beat cops. This vision of U.S. law enforcement is best imagined by slightly altering the facts of *United States v. Nippon Paper Industries*.²²⁹ In *Nippon Paper*, the First Circuit held that § 1 of the Sherman Act applied to a Japanese fax-paper manufacturer's conspiracy with trading houses to artificially inflate the price of paper shipped to North America because of this extraterritorial trading scheme's substantial and intended anticompetitive effects on U.S. markets.²³⁰

Now imagine, instead, a prosecution in which the paper had remained exclusively in Japanese markets. Prosecuting this hypothetical antitrust violation, one consisting of wholly foreign conduct, would likely violate the manufacturer's due-process rights under the framework for analyzing the extraterritorial application of federal criminal law.²³¹ First, under conventional readings of the Foreign Commerce Clause,²³² Congress has broad power to proscribe conduct that may affect global markets.²³³ Given the current realities of a globalized and interconnected world economy, inflated prices for fax paper purchased by Japanese companies could add to the costs of business in sundry international markets. Second, as a matter of statutory construction,²³⁴ the Sherman Act's criminal provisions may overcome the presumption against extraterritorial application because they might not be "logically dependent on their locality" under the *Bowman* framework.²³⁵ Indeed, this is the result the First Circuit reached in *Nippon Paper*.²³⁶ Unless prosecuting the anticompetitive behavior would run afoul of international-law principles, the *Charming Betsy* canon would not be implicated.

Under a sufficient-nexus analysis,²³⁷ prosecuting a foreign defendant whose only connection to the United States is an

229. *United States v. Nippon Paper Indus. Co.*, 109 F.3d 1 (1st Cir. 1997).

230. *Id.* at 2–3, 9.

231. *See supra* Part III.

232. *See supra* Part III.A.

233. *See supra* notes 140–41 and accompanying text.

234. *See supra* Part III.B.

235. *United States v. Bowman*, 260 U.S. 94, 98 (1922).

236. *United States v. Nippon Paper Indus. Co.*, 109 F.3d 1, 9 (1st Cir. 1997).

237. *See supra* Part III.C.1.

attenuated chain of economic effects²³⁸ would likely violate due process unless there is a relevant jurisdictional basis under the “rough guide” of international law.²³⁹ The best candidate is the territoriality principle, which would apply if the potential Sherman Act violations had or were intended to have “substantial” domestic effects.²⁴⁰ However, in the case of solely domestic activity with limited international impact, the United States would lack jurisdiction under the theory of “substantial effects.”²⁴¹ The United States would lack universal jurisdiction²⁴² and jurisdiction under the protective principle²⁴³ for a pure market offense. Without more evidence linking the putative criminal conduct to the United States, the prosecution would also lack a sufficient nexus. Moreover, the highly fact-dependent and context-specific nature of a Sherman Act violation is insufficient to grant the “global notice” that acts of terrorism²⁴⁴ or large-scale drug smuggling²⁴⁵ inherently do. Notice would be particularly problematic if the foreign sovereign’s law lacked American-style antitrust prohibitions or if foreign regulators had previously approved the conduct in question.²⁴⁶ With this lack of meaningful notice, it would likely be “arbitrary” and “fundamentally

238. In this hypothetical prosecution, the costs of inflated paper purchases in Japan would only indirectly affect the United States through an aggregation of the steps of multiple international transactions originating from wholly foreign conduct. *Cf.* *United States v. Lopez*, 514 U.S. 549, 564 (1995) (noting that the Court would be “hard pressed to posit any activity . . . that Congress is without power to regulate” under a chain of inferences that would grant regulatory power over any behavior that would have cascading economic effects when all instances of that behavior are considered).

239. *United States v. Davis*, 905 F.2d 245, 249 n.2 (9th Cir. 1990).

240. *See supra* notes 189–90 and accompanying text.

241. The *Nippon Paper* court’s reliance on the involvement of North American markets suggests that a higher quantum of conduct specifically targeting the United States is required to confer territorial jurisdiction over conduct occurring abroad. *See Nippon Paper*, 109 F.3d at 3–9 (recognizing that although “civil antitrust actions predicated on wholly foreign conduct which has an intended and substantial effect in the United States come within Section One’s jurisdictional reach,” there may be reason to interpret the applicable language uniformly in criminal cases).

242. *See supra* notes 194–95 and accompanying text.

243. *See supra* note 193 and accompanying text.

244. *United States v. Al Kassar*, 660 F.3d 108, 119 (2d Cir. 2011).

245. *United States v. Martinez-Hidalgo*, 993 F.2d 1052, 1056 (3d Cir. 1993).

246. In reality, the conduct in *Nippon Paper* violated both Japanese and U.S. law. *Nippon Paper*, 109 F.3d at 8. The specter that prosecutors may seek to apply criminal laws unique to the United States against foreign defendants engaged in conduct abroad that does not directly implicate U.S. interests is a stark reminder of the need to directly address the limits of prosecutorial discretion in the first instance, regardless of the potential due-process concerns.

unfair” to subject the company to prosecution. Accordingly, this prosecution would also fail a fundamental-fairness analysis.²⁴⁷

Eliminating the jurisdictional gap to allow summonses to be served in situations where prosecutions would likely run afoul of foreign defendants’ due-process rights would exacerbate these concerns. This possibility should not stand in the way of revising Rule 4, however. As a general matter, federal prosecutors can be expected to act judiciously when deciding to prosecute defendants who lack a physical domestic footprint.²⁴⁸ They are unlikely to expend valuable time and resources pursuing cases within the bailiwick of federal criminal law that do not substantially threaten domestic interests or may be better addressed by foreign sovereigns. It is possible that expanding prosecutors’ power would further enable, and perhaps even incent, the use of innovative tactics against foreign defendants.²⁴⁹ To the extent that these due-process violations may occur, it is not the manner of service that is worrisome, but the underlying prosecution’s merits. The adoption of policies to rein in potential abuses of prosecutorial overreach should be engaged directly, not enforced furtively through procedural rules.

B. Prosecutorial Overreach and International Comity

The unique role that entity liability plays in the U.S. legal system provides prosecutors with powerful tools for dealing with foreign organizations. Although commentators have debated the merits of entity liability for decades,²⁵⁰ the modern practice of prosecuting

247. See *supra* Part III.C.2.

248. Although prosecutors have wide discretion to initiate or decline a prosecution, they should not bring charges if “no substantial Federal interest” would be served. THE UNITED STATES DEP’T OF JUSTICE, *supra* note 108, 9-27.220, 9-27.230. The *United States Attorneys’ Manual* makes clear that federal law-enforcement priorities are designed to be “effective nationwide” (not worldwide) and that these priorities are “national” (not global). *Id.* 9-27.230 cmt. 1.

249. A powerful example is the so-called “Al Capone strategy,” whereby prosecutors successfully target savvy defendants by charging offenses that are easier to prove but do not fully vindicate the government’s underlying interests. Al Capone was eventually convicted on tax-evasion and Prohibition charges, not for the violent crimes (such as the St. Valentine’s Day Massacre) widely attributed to him. *Famous Cases & Criminals: Al Capone*, FED. BUREAU OF INVESTIGATION, <http://www.fbi.gov/about-us/history/famous-cases/al-capone> (last visited Nov. 2, 2014).

250. There is a voluminous scholarly debate about the purposes of corporate criminal liability; this Note does not advocate any particular resolution. See, e.g., V.S. Khanna, *Corporate Criminal Liability: What Purpose Does it Serve?*, 109 HARV. L. REV. 1477, 1532 (1996) (“[T]he circumstances in which substantially all of the traits of corporate criminal liability are socially

nonnatural persons has remained firmly rooted in the legal landscape for more than a century.²⁵¹ The threat of criminal action will continue to remain a staple of the federal prosecutor's playbook because of the many advantages it offers over the remedies available in civil suits, such as the threat of debarment from government contracting,²⁵² and because of its uniquely expressive blaming function.²⁵³ In short, entity criminal liability offers a major stick for the United States to carry in its relations abroad. As the importance of post-Westphalian state borders continues to wane, the adoption of more aggressive enforcement strategies to harmonize international economic policy seems inevitable.²⁵⁴ The United States may have legitimate interests in using its criminal law as an element of foreign policy, rather than passively abiding future "mugging[s] in broad daylight."²⁵⁵ One particularly fruitful strategy for prosecutors is the use of deferred prosecution agreements and non-prosecution agreements as de facto regulations of extraterritorial conduct.²⁵⁶ Yet, the use of these agreements may be susceptible to serious abuse. This concern is particularly acute when the targeted defendants are state-owned

desirable are nearly nonexistent."); see generally, e.g., John C. Coffee, Jr., "No Soul To Damn: No Body To Kick": An Unscandalized Inquiry Into the Problem of Corporate Punishment, 79 MICH. L. REV. 386 (1980) (describing the theoretical and practical difficulties with subjecting nonnatural persons to criminal liability).

251. See *N.Y. Cent. & Hudson River R.R. Co. v. United States*, 212 U.S. 481, 486 (1909) (affirming Congress's power to "enact laws which subject corporations to criminal prosecution and punishment").

252. See Sara Sun Beale, *A Response to the Critics of Corporate Criminal Liability*, 46 AM. CRIM. L. REV. 1481, 1500-03 (2009) (arguing that the "critical real world importance" of collateral consequences "should not play a central role in debates concerning the proper scope of criminal liability").

253. Samuel W. Buell, *The Blaming Function of Entity Criminal Liability*, 81 IND. L.J. 473, 514 (2006) (describing the unique costs and "social meaning" of criminal sanctions).

254. See Ethan A. Nademann, *The Role of the United States in the International Enforcement of Criminal Law*, 31 HARV. INT'L L.J. 37, 37 (1990) ("Law enforcement, traditionally a domestic function of government, has become more internationalized. . . . These developments do not mark a passing phenomenon but rather the emergence of new and important dimensions to criminal justice, United States foreign policy, and international politics.").

255. See Johnson, *supra* note 6, at B2.

256. See generally Benjamin M. Greenblum, Note, *What Happens to a Prosecution Deferred? Judicial Oversight of Corporate Deferred Prosecution Agreements*, 105 COLUM. L. REV. 1863 (2005); F. Joseph Warin & Andrew S. Boutros, *Deferred Prosecution Agreements: A View from the Trenches and a Proposal for Reform*, 93 VA. L. REV. IN BRIEF 121 (2007), available at <http://www.virginialawreview.org/sites/virginialawreview.org/files/warin.pdf>. But see Garrett, *supra* note 80, at 1778-79 (demonstrating that foreign corporations are more likely than their domestic counterparts to plead guilty rather than enter into pre-indictment agreements with U.S. prosecutors).

enterprises. Subjecting organizations that are essentially extensions of foreign sovereigns to prosecution in U.S. courts is a heavy-handed approach, akin to a war power.²⁵⁷

To the extent prosecutions of organizational defendants remain a practical reality, the fate of these prosecutions should not turn on the defendants' nationality. Eliminating criminal liability for all foreign organizations would be a dramatic and unwarranted response to potential prosecutorial overreach, no less extreme than eliminating liability for all foreign natural persons. A regime maintaining criminal liability for domestic organizations, but not for their foreign counterparts, "would create perverse incentives for those who would use nefarious means to influence markets in the United States, rewarding them for erecting as many territorial firewalls as possible between cause and effect."²⁵⁸ Rather, prosecutors must temper their reach abroad.

The inherently fictive nature of nonnatural defendants poses several additional challenges in this context. Organizational defendants cannot be "arrested" in any meaningful sense, nor can they be "extradited."²⁵⁹ Moreover, there is no criminal analogue to the Hague Convention, and extant bilateral and multilateral agreements do not specify mechanisms to compel a foreign organization's presence in the United States in order to be prosecuted.²⁶⁰ Without the cooperation of a foreign sovereign, it remains unclear how prosecutors might outmaneuver recalcitrant defendants.²⁶¹ Such unassisted prosecutions of foreign organizations may therefore prove unavailing.

257. In an analogous situation during the Founding period, the nascent U.S. government decided to deal with the Barbary pirates' threats to global trade routes through military action, specifically rejecting an alternative crime bill. FREDERICK C. LEINER, *THE END OF BARBARY TERROR: AMERICA'S 1815 WAR AGAINST THE PIRATES OF NORTH AFRICA* 50-51 (2006).

258. *United States v. Nippon Paper Indus. Co.*, 109 F.3d 1, 8 (1st Cir. 1997).

259. Although individual officials may be arrested or extradited, doing so would not necessarily allow an organization to be prosecuted domestically. One barrier is the inability of an individual official to plead to the indictment at arraignment. *See* FED. R. CRIM. P. 10(a)(3) advisory committee's note ("Read together, Rules 10 and 43 require the defendant to be physically present in court for the arraignment.").

260. *See generally* Thomas G. Snow, *The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available To Address Them*, 11 WM. & MARY BILL RTS. J. 209 (2002) (describing the limited and uneven procedural mechanisms used in international agreements to facilitate the prosecution of foreign defendants).

261. *But see supra* note 115 and accompanying text.

This practical need for international cooperation bolsters the importance of tempered prosecutorial behavior underlying the doctrine of international comity. This doctrine suggests circumstances in which the laws of foreign sovereigns should be given deference, “having due regard both to international duty and convenience, and to the rights of [their] own citizens or of other persons who are under the protection of [their] laws.”²⁶² In the sensitive realm of foreign relations, international comity may “counsel[] voluntary forbearance” when another sovereign has a “legitimate claim to jurisdiction” over the conduct.²⁶³ International comity is a nebulous doctrine whose legal force cannot cabin concerns of prosecutorial overreach on its own.²⁶⁴ However, it remains a forceful reminder that the United States should sometimes defer to the autonomy of foreign sovereigns and the international legal order, in accordance with the concept of tempered prosecutorial discretion detailed above.

C. Revision of Rule 4 and the Role of the Courts

Rule 4 should be revised to eliminate the jurisdictional gap, but not all potential revisions are equally advisable. Successful efforts at revision must carefully balance the capacities and interests of the judicial and executive branches. The subcommittee’s proposed means of achieving this balance is its major point of departure from the 2012 Recommendation.²⁶⁵ The 2012 Recommendation would require judicial authorization of an alternative means of service under the residual service provision,²⁶⁶ whereas the subcommittee’s version would not.²⁶⁷ At first blush, requiring court approval appears to serve as an ex ante check on unilateral prosecutorial actions dangerous to defendants’ due-process rights.

This Note argues, however, that a regime of ex post review would better serve the institutional capacities of both prosecutors and courts, as well as decrease the likelihood of violating due process. There are four reasons to believe this is the case. First, a regime that

262. *Hilton v. Guyot*, 159 U.S. 113, 163–64 (1895).

263. *Nippon Paper*, 109 F.3d at 8.

264. *See id.* (“Comity is more an aspiration than a fixed rule, more a matter of grace than a matter of obligation.”); *see also* Michael D. Ramsey, *Escaping “International Comity”*, 83 IOWA L. REV. 893, 896–97 (1998) (“[T]he phrase ‘comity’ leads not only to confusion but to disguise . . .”).

265. *See supra* Part II.A–B.

266. *See supra* notes 106–08 and accompanying text.

267. *See supra* notes 120–23 and accompanying text.

does not require prior court approval discourages the strategic behavior of locating an outlier judge who may be more amenable to expansive service proposals.²⁶⁸ Second, without judicial preapproval, prosecutors must internalize the full costs of deciding to bring suit in the first place, knowing that their actions will be subject to judicial review. Prosecutors would have to evaluate for themselves the likelihood of violating defendants' due-process rights, rather than rely on a court's preliminary, insufficiently informed decision to order service.²⁶⁹ A third benefit of granting prosecutors the exclusive power to select their preferred means of service as an initial matter is the method's regard for the separation of powers—affording the executive flexibility when it engages in foreign relations, while retaining judicial oversight. Finally, organizational defendants may prefer *ex post* review because a judge would handle service as “a question of first impression,” rather than be forced to overrule her earlier decision.²⁷⁰ The subcommittee's proposed revisions, which embrace these advantages of *ex post* judicial review,²⁷¹ are therefore superior to the 2012 Recommendation.

CONCLUSION

There is no compelling theoretical or practical reason to allow the United States to serve summonses on foreign organizational defendants in criminal cases only if they maintain a domestic mailing address or principal place of business. Rule 4 should be revised to eliminate this jurisdictional gap. Revising Rule 4, however, may spawn potential due-process violations. Moreover, expanding the government's ability to make service abroad may itself exacerbate due-process violations.

This Note concludes that such concerns, while valid, are properly levied against the underlying decisions to bring extraterritorial

268. This would help curb our “national legal pastime” of forum-shopping in a category of prosecutions that, given the foreign defendants, could see its fair share of strategic behavior. J. Skelly Wright, *The Federal Courts and the Nature and Quality of State Law*, 13 WAYNE L. REV. 317, 333 (1967).

269. This benefit is lessened to some degree by the fact that prosecutors may strategically serve defendants in an effort to induce settlements or other arrangements, regardless of any due-process concerns in later stages of a prosecution. *See supra* note 256 and accompanying text.

270. Memorandum from Sara Sun Beale & Nancy King, Reporters, Advisory Comm. on Rules of Criminal Procedure, to Members, Criminal Rules Advisory Comm., *supra* note 111, at 9.

271. *See supra* notes 120–23 and accompanying text.

prosecutions in the first place, not at the procedural mechanisms that govern them. As the United States continues to expand the application of its criminal laws abroad, it is critical for the DOJ to adopt a procedural framework that forces prosecutors to bear the full costs of their decisions when pursuing foreign organizational defendants. Undoubtedly, foreign organizational defendants will continue to act extraterritorially in ways that substantially affect domestic interests; such offending conduct may often justify a criminal response. But this class of offenses must be prudently culled to conserve American institutional legitimacy. Like their country, U.S. prosecutors must not go abroad “in search of monsters to destroy.”²⁷²

272. Adams, *supra* note 1.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8gra-jglm
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0018](#)

Comment from Anonymous anonymous, NA

Submitter Information

Name: Anonymous anonymous

Organization: NA

General Comment

Hi. I just found out about the changes to Federal Rule 41(b), basically allowing law officials to search private computers using a VPN or whatever simply because they're using it and without a warrant. This is asinine. It's the logical equivalent of allowing law enforcement agencies to search your house without a warrant because you're using blinds, curtains, and a door. You don't want citizens living in glass houses, and there is no reason why we should have "glass" computers, either. Keep the warrants; ditch the glass.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8grz-ris8
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0019](#)

Comment from Karen Strombom, Federal Magistrate Judges Association

Submitter Information

Name: Karen Strombom

Organization: Federal Magistrate Judges Association

General Comment

The Federal Magistrate Judges Association respectfully submits the attached comments regarding the proposed amendments to the Federal Rules of Criminal Procedure. The comments were first considered by the Standing Rules Committee of the FMJA, co-chaired by Judge Geraldine Soat Brown of the Northern District of Illinois and Judge David E. Peebles of the Northern District of New York. The committee members come from districts across the country, and their collective experiences encompass varying types of duties. The committee's comments were reviewed and unanimously approved by the Officers and Directors of the FMJA.

We are pleased to have this opportunity to present written comments representing the view of the FMJA.

Sincerely, Karen L. Stromobm, President, FMJA

Attachments

comments on criminal rules amendments class of 2016 (revised jan 2015)

COMMENTS OF
THE FEDERAL MAGISTRATE JUDGES ASSOCIATION
ON PROPOSED AMENDMENTS TO
THE FEDERAL RULES OF CRIMINAL PROCEDURE
(February 2015)

The Committee on Rules of Practice and Procedure of the Judicial Conference of the United States has published for comment proposed amendments to the Federal Rules of Appellate Procedure, the Rules of Bankruptcy Procedure, the Federal Rules of Civil Procedure, and the Federal Rules of Criminal Procedure. Unlike the amendments proposed last year, which included significant changes to the Federal Rules of Civil Procedure governing discovery, the amendments now being proposed for the Rules of Civil Procedure are relatively modest while some significant changes are proposed for the Rules of Criminal Procedure.

The following represent the comments of the FMJA concerning the proposed amendments to the Rules of Criminal Procedure.

PROPOSED REVISION TO FED. R. CRIM. P. 4

This proposal would amend the Rule as it relates to service of summons upon an organization that is named as a defendant in a criminal case. The proposed amendment to Rule 4(a) provides that upon the failure of an organization to appear in response to a summons, a judge may take

any action authorized by United States law. The FMJA endorses that provision.

The proposed amendments to Rule 4(c) would create separate sections relating to service of a summons on an organization, depending on whether that organization is located at a place within or outside a United States judicial district.

First, Rule 4(c)(2) would allow a summons to an organization to be served in a place outside a United States judicial district. Second, Rule 4(c)(3) clarifies service of a summons on an organization in a United States judicial district. Third, Rule 4(c)(3)(D) creates a new subsection setting out the means for service of a summons on an organization that is not in a United States judicial district. Notably, Rule 4(c)(3)(D)(ii) would permit service “by any other means that gives notice,” followed by a non-exhaustive list of examples. Therefore, the proposed rule would permit service by three specified means or by “any other means that gives notice.”

The FMJA endorses the proposed amendments to Rule 4, which address an interstitial gap in the rule, respond to a growing need in our increasingly global economy, and provide a comprehensive approach to service of process upon foreign corporations that are charged in connection

with federal criminal cases. We believe that the options for service of a summons provide an appropriate flexibility that will adapt to changes in the world economy and communications technology. We express a concern, however, about the breadth of subsection 4(c)(3)(D)(ii). We recommend that the Committee comments expressly state: “The use of any other means of service beyond those specified in the rule must satisfy constitutional due process requirements.”

PROPOSED REVISION TO FED. R. CRIM. P. 41

This proposal would modify Rule 41(b) to add a new subsection (6) providing the court authority in two identified circumstances to issue a warrant permitting the government to use remote access to search and seize electronically stored information located inside or outside that district. Rule 41(f)(1)(C) would be modified to require “reasonable efforts” to serve a copy of a warrant for a remote access search.

The FMJA is concerned that the term “remote access” (meaning, presumably, searching by remote means) is not defined and will require explication by the government in each particular situation. We recognize, however, that attempting to be more specific in the Rule risks falling behind

the progress of technology. Likewise, what constitutes “reasonable efforts” to serve will be developed in particular situations. The FMJA nonetheless endorses this proposal as filling a significant gap in authority.

PROPOSED REVISION TO FED. R. CRIM. P. 45(c)

Like the proposed revision to Federal Rule of Civil Procedure 6(d), this proposal would eliminate the three-day extension to act when service is accomplished by electronic means, as authorized through a 2001 amendment to Fed. R. Civ. P. 5(b)(2). The FMJA generally endorses this change, agreeing with the Advisory Committee’s recognition that, with “advances in technology and widespread skill in using electronic transmission,” service by electronic means generally occurs instantaneously, and thus the rationale for adding three days to respond, to account for delays occasioned when service is accomplished through traditional means such as by mail, is no longer relevant.

The proposal mirrors the proposed change in Rule 6(d), and, accordingly, the FMJA has the same concerns about potential confusion that we have expressed concerning that proposal. Specifically, the FMJA believes that the interplay between the proposed amended Criminal Rule

45(c) and existing Civil Rule 5(b)(2)(E) which permits service by electronic means upon written consent, and Civil Rule 5(b)(2)(F) which governs other means of service based upon written consent, has the potential to engender confusion. The proposed amended Rule will include three new parentheticals that refer to “(mail),” “(leaving with the clerk),” and “(other means consented to).” When the Rule appears in final form, the deletion of Rule 5(b)(2)(E) will not be apparent. The proposed new parenthetical “(other means consented to)” may lead some litigants to believe they are entitled to the additional three days if they consent to electronic service. While the Committee Note makes clear that this is not the intention of the amendment, the language of the proposed Rule is not that clear. The FMJA suggests that the confusion could be eliminated or minimized by either leaving out the proposed parentheticals in Rule 45(d), so that the reader would refer back to Rule 5(b)(2) and its subsections (C) (D) and (F), or by clarifying the new parenthetical following (F) so that it reads: “(F) other means consented to except electronic service.”

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8gu2-p9pf
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0020](#)

Comment from Anonymous Anonymous, NA

Submitter Information

Name: Anonymous Anonymous

Organization: NA

General Comment

Proposal to Rule #41. I find this is bad because United States can get to my computer even if I done nothing wrong with them. Stay out of other peoples business and mind your own business. USA police want to spy on everyone in the world and spy on their own peoples too you know. These peoples have done nothing wrong too. If FBI want into a computer, they ask police in other country to ask judge to let them do that. This proposal to rule law #41 is meaning that FBI is being lazy and dont want to work like everyone else.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8gui-ngl9
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0021](#)

Comment from dan teshima, NA

Submitter Information

Name: dan teshima

Organization: NA

General Comment

I agree entirely with what Mr. Wessler said. The proposed "tweaks" to rule 41 would be a mistake that only serves to weaken the 4th amendment. There's not much else I can say that hasn't already been said.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8gp8-cjkd
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0022](#)

Comment from George Orwell, NA

Submitter Information

Name: George Orwell

Organization: NA

General Comment

Dude seriously??? You're going to hack into our computers for practicing internet privacy? Exercising privacy is going to have federal agents reign down upon my porn machine??? That's fucked up man. I need to build a new and improved tinfoil hat now. Bastards.

Perhaps all FBI agents shall also be allowed into all homes that are not entirely made out of glass. Privacy is evil after all right? Government must know all, must see all. If you have something to hide then you are a terrorist against the state.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8gzt-zka9
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0023](#)

Comment from Cheryl Siler, Aderant

Submitter Information

Name: Cheryl Siler

Organization: Aderant

General Comment

I am writing to comment on the proposed amendment to Federal Rule of Criminal Procedure 45(c). In order to promote consistency among the Federal Rules for computation of time after service, I suggest that the language of Criminal Rule 45(c) be revised to match that used in Federal Rule of Civil Procedure 6(d), Federal Rule of Appellate Procedure 26(c) and Federal Rule of Bankruptcy Procedure 9006(f).

Specifically, Criminal Rule 45(c) reads, in part, Whenever a party must or may act within a specified time after service and service is made under...

In contrast, Civil Rule 6(d), Appellate Rule 26(c) and Bankruptcy Rule 9006(f) use the language "within a specified time after being served" or "within a prescribed period after being served."

The language used in Civil Rule 6(d), Appellate Rule 26(c) and Bankruptcy Rule 9006(f) makes it clear that the 3 extra days are not accorded to the party serving the document and that only the party upon whom a document is served is entitled to the extra time.

By keeping the "old" language in the Criminal Rule, it creates confusion and ambiguity. Practitioners may interpret the rule to mean that in criminal proceedings all parties are entitled to the benefit of the 3 extra days after service, regardless of whether they are the party serving a document or the party being served with a document.

In order to avoid confusion and to make the Federal Rules consistent with one another, I propose that Criminal Rule 45(c) be further revised to read, "Whenever a party must or may act within a specified time after being served and service is made under..."

Thank you for your time and consideration.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h10-fvcx
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0024](#)

Comment from Ladar Levison, NA

Submitter Information

Name: Ladar Levison

Organization: NA

General Comment

I oppose this amendment because it:

- a) Moves a substantive question of law to a procedural hearing, where a defendant, or respondent third party has even fewer protections.
- b) Makes the use of encryption legally equivalent to evidence of a crime, thus making everyone subject to a search and seizure warrant (including the person reading this), as every modern communications system uses some form of VPN... including the cellular phone we carry around in our pockets. Cell phones use a rudimentary encryption scheme to protect calls between the handset and the telecom provider.
- c) Makes it easier for a judge to issue an unconstitutional search warrant, creating an even larger burden for the public which must then go to court to defend its rights, at great cost, which should be guaranteed already and which you are sworn to defend.
- d) Expands the FBI's powers to a point where they border on a blanket writ. Allowing for the search of someone's electronic property because they are using a technological tool that not only isn't considered illegal, but is actually considered a best practice.
- e) Makes compliance with industry standards, such as the Payment Card Industry Data Security Standards (PCI DSS) grounds for issuing a search and seizure warrant.
- f) Could 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.

Overall I find this amendment to be driven by law enforcement, with little consideration for the realities of law, and technology. Please reconsider. There are a number of reforms that could be enacted which would improve the protection of our rights, while ensuring LEOs have the, albeit, needed tools to protect us. This amendment is not that reform. If your interested in true reform, please let me know.

There are a number of technologists who deal with these issues in the field. People who understand how an imprecise law gets applied in applied by a court. I would encourage you to hear testimony from them before expanding the powers of our courts.

L~

P.S. I submitted this comment several days ago but haven't seen it show up on the public website yet. So I'm resubmitting.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h6m-jhrq
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0027](#)

Comment from Bruce Moyer, National Association of Assistant United States Attorneys

Submitter Information

Name: Bruce Moyer

Organization: National Association of Assistant United States Attorneys

General Comment

See attached file(s)

Attachments

NAAUSA Comments re Rule 41 FINAL - 0204-2015



National Association of Assistant United States Attorneys

12427 Hedges Run Dr. • Suite 104

Lake Ridge • VA • 22192-1715

Phone: 800-455-5661 • Fax: 800-528-3492 • Email: staff@naausa.org

www.naausa.org

February 4, 2015

The Honorable Reena Raggi
Chair, Advisory Committee on the Criminal Rules
704S United States Courthouse
225 Cadman Plaza East
Brooklyn, NY 11201-1818

Re: Proposed Amendment of Rule 41

Dear Judge Raggi:

The National Association of Assistant United States Attorneys supports the proposed amendment of Rule 41 to revise the territorial limits of search warrants for remote access to electronic information contained in another judicial district. This would ensure the establishment of a court-supervised framework through which law enforcement may successfully investigate and prosecute crimes involving botnets and internet anonymizing technologies. That would be achieved by the conferral of authority to a magistrate judge, in a district where activities related to a crime have occurred, to issue a warrant to use remote access to search electronic storage media and seize or copy electronically stored information located outside of the district.

The Advisory Committee's proposal would change Rule 41 in two ways. The first change is an amendment to Rule 41(b), which generally limits warrant authority to searches within a district, but permits out-of-district searches in specified circumstances. The amendment would add specified remote access searches for electronic information to the list of other extraterritorial searches permitted under Rule 41(b). 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. The National Association of Assistant United States Attorneys supports both of these changes because of their responsiveness to the challenges created by sophisticated technologies in the hands of criminals intent on causing harm to specific persons and the public at large.

The National Association of Assistant United States Attorneys represents the interests of the 5,400 Assistant United States Attorneys (AUSAs) employed by the Department of Justice and responsible for the prosecution of federal crimes and the handling of civil litigation involving the United States. United States Attorneys and Assistant United States Attorneys are the gatekeepers of our system of justice. Their primary responsibility is to protect the innocent and prosecute the guilty.

President	Vice President for Policy	Vice President for Operations	Treasurer	Secretary
Robert G. Guthrie ED of Oklahoma	John E. Nordin II CD of California	and Membership Lawrence J. Leiser ED of Virginia	Daniel A. Brown SD of Ohio	Leah Bynon Farrell New Jersey

Increasingly Sophisticated Technologies Pose Challenges to Law Enforcement

Mindful of the above responsibilities, we appreciate the Advisory Committee's sensitivities to the concerns first raised by the Department of Justice about the need to improve Rule 41's territorial venue limitations and to respond to the increasing need arising within law enforcement investigations of sophisticated internet crimes to locate electronic information when the location of the electronic information being sought is unknown or the electronic information spans multiple districts.

Law enforcement investigations of financial fraud, child pornography, terrorism and other threats to the public often require a remote search of the suspect's computer. But criminal suspects are increasingly using sophisticated anonymizing technologies and proxy services designed to hide their true IP addresses. This creates significant difficulties for law enforcement to identify the district in which the electronic information or an electronic device is located, even though other details may be sufficiently detailed in the warrant. In response, law enforcement authorities seek to use computer software that enables remote searching of a computer to determine the true IP address or other identifying information associated with the suspect's computer.

In addition, the use of multiple computers in many districts simultaneously as part of a sophisticated criminal scheme, commonly known as a botnet, is increasingly requiring law enforcement to pursue remote access to those computers, which may be located in different districts. Botnets represent increasing threats to the public, through their use in massive denial of service attacks, the theft of personal and financial data, and the distribution of malware designed to cause havoc and harm to the users of host computers.

The Amendment's Rationale Coincides with Permissible Extra-Territorial Searches

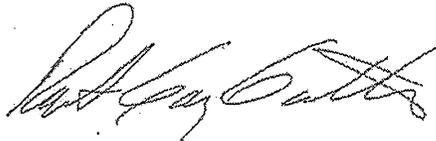
The investigation of botnet schemes can require significant resources and efforts involved in the coordination of warrants and searches spanning numerous districts. Investigative searches of numerous computers in numerous districts in a large botnet investigation requires law enforcement, under the current Rule 41, to obtain warrants in potentially all 94 districts. The number of occasions like this are only growing. The coordination of that many requests and their review by significant numbers of magistrate judges not only wastes judicial and investigative resources, but also may cause delay that impedes the investigation. The solution lies in amending Rule 41, along the lines devised by the Advisory Committee, to authorize a court in a district where activities related to a crime have occurred to issue a warrant for electronic storage media within or outside the district. Such an amendment, and its underlying rationale, would coincide with the justification underlying the extra-territorial searches contained in Rule 41, involving investigations of domestic or international terrorism, as well as the use of tracking devices outside the jurisdiction of the court.

Under the proposed amendment, investigators could obtain a warrant to remotely install software on a target device to determine the true IP address or identifying information for that device, but only if that location of the device or information has been concealed by technological means. We believe the use of remote access techniques with these safeguards is appropriate as outlined in the proposed rule. We expect that collateral issues, such as the level of specificity required in a warrant seeking authorization to conduct a remote access search or seizure, will be sufficiently addressed by the courts in due course. We are pleased that the Advisory Committee has embraced the same view.

Conclusion

The National Association of Assistant United States Attorneys believes that the proposed amendment of Rule 41 is necessary, strikes the right balance and will permit law enforcement to investigate and prosecute crimes involving computers and electronic information. We recommend that the Advisory Committee solicit the support approval of the proposed amendments from the Committee on Rules of Practice and Procedure.

Sincerely,

A handwritten signature in cursive script, appearing to read "Robert Gay Guthrie".

Robert Gay Guthrie
President

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h6o-767h
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0028](#)

Comment from Robert Feldman, Quinn Emanuel Urquhart & Sullivan, LLP

Submitter Information

Name: Robert Feldman

Organization: Quinn Emanuel Urquhart & Sullivan, LLP

General Comment

See attached.

Attachments

QE Comment re Rule 4

February 13, 2015

The Honorable Reena Raggi
United States Court of Appeals
704S United States Courthouse
225 Cadman Plaza East
Brooklyn, New York 11201-1818

Professor Sara Sun Beale
Charles L.B. Lowndes Professor
Duke Law School
210 Science Drive
Durham, North Carolina 27708-0360

Professor Nancy J. King
Lee S. and Charles A. Speir Professor of Law
Vanderbilt University Law School
131 – 21st Avenue South, Room 248
Nashville, Tennessee 37203-1181

Re: *Proposed Amendment to Federal Rule of Criminal Procedure 4*

Your Honor and Professors Beale and King:

We are practicing lawyers and former federal prosecutors. Among our clients are the Pangang Group Company and affiliated entities. We write with several observations on the Proposed Amendment to Federal Rule of Criminal Procedure 4.

The current proposal allows for service on an organizational defendant “not within a judicial district of the United States” in two ways: first, by “delivering a copy” to an officer or agent of the organization; or second, and seemingly more broadly, “by any other means that gives notice.” While the proposed rule lists three ways that service by notice may be accomplished, the plain text of the rule and the advisory committee notes may be construed in the future such that these enumerated methods are examples only with the potential means of service unbounded so long as it purportedly “gives notice.”

There is a fundamental problem with this “notice only” approach: though apparently not the drafters’ intent, the proposed rule may be argued to insulate service from judicial review. The proposed advisory committee notes state that “although it is presumed that the enumerated means will provide notice, whether actual notice has been provided may be challenged in an

Hon. Reena Raggi
Professor Sara Sun Beale
Professor Nancy J. King
February 13, 2015

individual case.” Practically speaking, however, this could be impossible under the proposed regime: the very act of challenging service might be said to conclusively establish the notice that would make service complete.

The inability of a criminal defendant to challenge purported service of process after the fact is exacerbated by the current proposal, which does not require prior judicial review for the method of service chosen by the Department of Justice. The combination of these features results in a system that could foreclose judicial review at any stage in the process, leaving the supposed validity of service entirely in the hands of the executive. This would be a radical departure from the current system, where the judicial branch provides an important check and balance with a meaningful role in ensuring that proper service of process is achieved.

Denying an organizational defendant any means to challenge the procedural propriety of its prosecution would be a particularly harsh result given that the “notice only” regime set up by the proposed rule is vulnerable to arguments by the government that no procedures at all are required for service and that it has effected service, for example, simply by sending a letter or an email telling a foreign organization of an indictment or even through a newspaper article or television appearance describing the prosecution. Indeed, under the proposed rule, a manner of service that is prohibited by international agreement might be argued to pass muster, so long as it appears to have provided notice to the accused. In effect, “any other means that gives notice” might be said to trump and render superfluous the limitations imposed in the other subsections—*e.g.*, the requirement in (D)(i) that the delivery be made “in a manner authorized by the foreign jurisdiction’s law” to a narrow category of persons.

While a court may—and, indeed, should—be loathe to accept such arguments, the language of the proposed rule is troubling. Making notice the sole criterion for service, as the proposed rule could be argued to do, would eliminate a historical function of service, *e.g.*, *Omni Capital Int’l v. Wolf & Co.*, 484 U.S. 97, 104 (1987) (“[B]efore a court may exercise personal jurisdiction over a defendant, there must be more than notice to the defendant and a constitutionally sufficient relationship between the defendant and the forum. There also must be a basis for the defendant’s amenability to service of summons.”), and open the door to various questionable mechanisms of bringing a criminal defendant within the jurisdiction of our courts.

Another proposed addition to Rule 4 expressly authorizing a judge to “take any action authorized by law” in response to “an organizational defendant [that] fails to appear in response to a summons” highlights the difficulty with the “notice only” regime. Assuming that the defendant has in fact received notice, in a framework where “special appearances”—a longstanding feature of our jurisprudence to which the government consented in the Pangang case and that other courts have approved—may be effectively eviscerated, a responsible foreign organization that wishes to contest service is faced with a Hobson’s choice. Worse still for an organization that has not actually received notice, under the proposed rule it is possible that a Court might accept

Hon. Reena Raggi
Professor Sara Sun Beale
Professor Nancy J. King
February 13, 2015

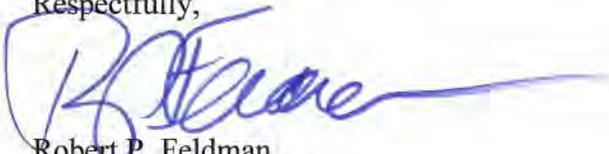
the government's claims that the chosen method of service provided ample notice and impose sanctions on the unwitting defendant, potentially including appointment of counsel and trial effectively *in absentia*.

As with other aspects of the proposed rules, we urge that extreme care be taken. On the theory that "turnabout is fair play" it can be expected that other governments may reciprocate by adopting a similar regime (that "any form of notice is sufficient") that could equally ensnare U.S. corporations in criminal prosecutions around the globe without adequate service of process.

The Department of Justice recognizes that, in comparison to civil service of process, "[t]he greater public aims of criminal process . . . justifies a higher burden on the government for serving a criminal defendant." Letter from Lanny A. Breuer, Assistant Attorney General, to the Hon. Reena Raggi, Chair, Advisory Committee on the Criminal Rules (Oct. 25, 2012), at 6. The proposed rule does precisely the opposite, lowering the requirements for service of process in criminal cases well below the standards in the civil context.

For these reasons, we respectfully urge the Committee to decline to approve the proposed amendments to Federal Rule of Criminal Procedure 4.

Respectfully,

A handwritten signature in blue ink, appearing to be "R. Feldman", written over a circular stamp.

Robert P. Feldman
John M. Potter

04675.51961/6495570.4

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h7v-rzp5
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0029](#)

Comment from Richard Salgado, Google Inc.

Submitter Information

Name: Richard Salgado

Organization: Google Inc.

General Comment

See attached.

Attachments

13Feb2015 Google Inc. Comments on the Proposed Amendment to Federal Rule of Criminal Procedure 41



February 13, 2015

TO: The Judicial Conference Advisory Committee on Criminal Rules

FROM: Richard Salgado, Google Inc.
Director, Law Enforcement and Information Security

RE: **Google Inc. Comments on the Proposed Amendment to Federal Rule of Criminal Procedure 41**

Google Inc. (“Google”) writes in opposition to the proposed amendment to Federal Rule of Criminal Procedure 41. Google makes available a variety of Internet-related products and services for people and businesses around the world, including webmail, search, maps, news, and image storage and organization. Google’s mission is to organize the world’s information and make it universally accessible and useful. Google has a significant interest in protecting its users and securing its infrastructure. The proposed amendment substantively expands the government’s current authority under Rule 41 and raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns. Google urges the Committee to reject the proposed amendment and leave the expansion of the government’s investigative and technological tools, if any are necessary or appropriate, to Congress.

I. The Proposed Amendment Is a Substantive Expansion of the Government’s Search Capabilities That Should Be Left to Congress

A. The government cannot seize evidence outside the United States pursuant to a search warrant that permits remote access of servers abroad.

Under current Rule 41, federal prosecutors must generally seek a warrant in the judicial district to search for and seize a person or property located within the district.¹ This territorial limitation is subject to limited exceptions.² Yet, the proposed amendment to Rule 41 would permit a court

¹ Fed. R. Crim. P. 41(b)(1).

² See Fed. R. Crim. P. 41(b)(2)–(5).

within any district where activities related to a crime may have occurred to issue a warrant authorizing remote access searches of electronic information located within or outside the district in two circumstances: first, where the location of “the media or information . . . has been concealed through technological means,” and second, where the search involves “an investigation of a violation of 18 U.S.C. § 1030(a)(5)” and “the media are protected computers that have been damaged without authorization and are located in five or more districts.”³

Remote searches of media or information that have been “concealed through technological means” may take place anywhere in the world. This concern is not theoretical. A magistrate judge in the Southern District of Texas recently denied an application for a Rule 41 warrant to permit U.S. law enforcement agents to hack a computer whose location was unknown, but whose IP address was most recently associated with a country in Southeast Asia.⁴ Such searches clearly violate the extraterritorial limitations of Rule 41. The Department of Justice (“DOJ”) urges that “[i]n light of the presumption against international extraterritorial application, . . . [the proposed] amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries.”⁵ But despite this weak assurance that the amendment does “not purport” to expand the current scope of Rule 41, in reality it will: the nature of today’s technology is such that warrants issued under the proposed

³ The proposed change in Rule 41 that permits extraterritorial reach of a Rule 41 search warrant is a different issue than the matter currently before the Second Circuit, which deals with whether a search warrant authorized under the Stored Communications Act (“SCA”) and properly served upon a U.S.-based electronic communications service provider is valid where that service provider has custody or control of communications it stores on servers outside the United States. *In re Warrant*, No. 14-2985 (2d Cir. 2014). Here the Committee is seeking by rule to grant extraterritorial reach to Rule 41 warrants and authorize surreptitious searches of remote computers, potentially circumventing both Mutual Legal Assistance Treaties, and SCA procedures in some cases.

⁴ *In re Warrant*, 958 F. Supp. 2d 753, 758 (S.D. Tex. 2013) (“But the Government’s application would fail nevertheless, because there is no showing that the installation of the ‘tracking device’ (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet.”).

⁵ Letter from Mythili Raman, Acting Assistant Att’y Gen., U.S. Dep’t of Justice, to Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 4 (Sept. 18, 2013), available at <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2013-10.pdf>.

amendment will in many cases end up authorizing the government to conduct searches outside the United States.

The government has previously offered the theory that a search or seizure does not occur pursuant to a Rule 41 warrant until the government examines the data.⁶ Under this rationale, a remote search by the government of media or information located in another country would not violate Rule 41's extraterritoriality limitations because no search would occur outside U.S. borders. But this logic must be, and has been, rejected.⁷ A search or seizure occurs at the moment when the government secures the data.⁸ Therefore, where the government accesses servers located abroad to obtain information pursuant to a Rule 41 warrant, there is no doubt that a seizure of such data will occur outside U.S. territorial limits.

Accordingly, while the proposed amendment "purports" not to substantively expand the government's search powers under Rule 41, it in effect does so anyway. Such a change is for Congress to effect, not the Committee.

Moreover, as the Committee must understand, the United States has long recognized the sovereignty of nations.⁹ To this end, it is well established that "[a]bsent a treaty or other agreement between nations, the jurisdiction of law enforcement agents does not extend beyond a nation's borders."¹⁰ Stated differently, "[a] state's law enforcement officers may exercise their

⁶ *In re Warrant*, 958 F. Supp. 2d at 756 ("Even though the Government readily admits that the current location of the Target Computer is unknown, it asserts that this subsection authorizes the warrant because information obtained from the Target Computer will first be *examined* in this judicial district.") (emphasis added) (internal quotation marks and citation omitted).

⁷ *Id.* at 757 ("By the Government's logic, a Rule 41 warrant would permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district.")

⁸ *See, e.g., United States v. Ganas*, 755 F.3d 125, 135–36 (2d Cir. 2014) (copying electronic data constitutes a seizure).

⁹ *See, e.g., The Schooner Exchange v. McFaddon*, 11 U.S. (7 Cranch) 116, 136 (1812) ("The jurisdiction of the nation within its own territory is necessarily exclusive and absolute. It is susceptible of no limitation not imposed by itself."), *superseded by statute as stated in Siderman de Blake v. Republic of Argentina*, 965 F.2d 699 (9th Cir. 1992).

¹⁰ L. Song Richardson, *Convicting the Innocent in Transnational Criminal Cases: A Comparative Institutional Analysis Approach to the Problem*, 26 Berkeley J. Int'l L. 62, 80 (2008); *see also United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990) (seven justices endorsing the view that U.S. courts may not issue search warrants for foreign searches); *cf.*

functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.”¹¹ The U.S. has many diplomatic arrangements in place with other countries to cooperate in investigations that cross national borders, including Mutual Legal Assistance Treaties (MLATs).¹² Generally, these arrangements allow “for the exchange of evidence and information in criminal and related matters.”¹³ Google, and many other service providers, have long encouraged and supported the efforts of the Administration and Congress to improve these processes, but the proposed amendment undermines those efforts.¹⁴

B. The proposed amendment alters constitutional rights and violates the Rules Enabling Act.

The proposed amendment is a substantive change that imposes upon the constitutional rights of targets in violation of the Rules Enabling Act, which provides that rules of practice, procedure, and evidence may be adopted so long as they do not “abridge, enlarge, or modify any substantive right.” 28 U.S.C. § 2072(b). Although the proposed amendment disclaims association with any constitutional questions,¹⁵ it invariably expands the scope of law enforcement searches, weakens

Weinberg v. United States, 126 F.2d 1004, 1006 (2d Cir. 1942) (“With very few exceptions, United States district judges possess no extraterritorial jurisdiction.”).

¹¹ Restatement (Third) of Foreign Relations Law § 432(2); *see also id.* § 433(1) (“Law enforcement officers of the United States may exercise their functions in the territory of another state only (a) with the consent of the other state and if duly authorized by the United States; and (b) in compliance with the laws both of the United States and of the other state.”).

¹² *See, e.g.*, Bureau of Int’l Narcotics & Law Enforcement Affairs, U.S. Dep’t of State, 2012 International Narcotics Control Strategy Report (INCSR) (Mar. 7, 2012), <http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm>.

¹³ *Id.*

¹⁴ *See, e.g.*, Reform Government Surveillance, *Global Government Surveillance Reform*, Principle 5, <https://www.reformgovernmentsurveillance.com/> (“In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved mutual legal assistance treaty — or “MLAT” — processes.”); Exec. Office of the President, Office of Mgmt. & Budget, *Statement of Administration Policy on H.R. 4660 — Commerce, Justice, Science, and Related Agencies Appropriations Act, 2015* (May 28, 2014), available at http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr4660h_20140528.pdf (MLAT improvement “is critical to investigating crimes, working with foreign partners, and prosecuting terrorists and other criminals. This funding will provide for an updated, improved, and accelerated process to handle foreign governments’ requests for evidence as well as enhance mutual relationships.”).

¹⁵ *See* Fed. R. Crim. P. 41 committee note (proposed Apr. 21, 2014), available at <http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf>.

the Fourth Amendment's particularity and notice requirements, opens the door to potentially unreasonable searches and seizures, and expands the practice of covert entry warrants. The Committee asserts that "the proposed amendment's language speaks directly only to venue, and . . . the proposed commentary makes clear that the government must satisfy constitutional requirements with respect to any warrant."¹⁶ But the two provisions of current Rule 41 that authorize the commencement of searches outside the issuing district were both the result of congressional action under the USA PATRIOT Act, and were not, as here, the unilateral work of the Committee.¹⁷

The substantive changes offered by the proposed amendment, if they are to occur, should be the work of congressional lawmaking. Such was the case with a slew of legislation providing law enforcement with the ability to use technological means to conduct invasive searches on targets, including the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1804, which provides law enforcement with the ability to legally surveil and collect foreign intelligence information; Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. § 2518, which provides law enforcement with the ability to legally intercept wire, oral, and electronic communications; the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*, which provides law enforcement with the ability to legally access electronically stored communications; and the Pen Registers and Trap and Trace Act, 18 U.S.C. § 3123, and USA PATRIOT Act, 50 U.S.C. § 1842, both of which provide law enforcement with the ability to legally intercept real time telephony metadata. In passing this legislation, Congress was able to openly debate and weigh the various constitutional issues at play.

¹⁶ See Memorandum from Sara Beale & Nancy King to Criminal Rules Advisory Committee 1 (Mar. 17, 2014) ("Beale Memorandum"), available at <http://www.uscourts.gov/uscourts/rulesandpolicies/rules/agenda%20books/criminal/cr2014-04.pdf>.

¹⁷ See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. Law 107-56, 107th Cong. § 219 (amending Rule 41 to include the power to issue a search warrant for a person or property outside the district in a terrorism investigation); Fed. R. Crim. P. 41, advisory committee notes (2008) (noting that subsection (b)(5) is intended to authorize the issuance of a search warrant "in any of the locations for which 18 U.S.C. § 7(9) provides jurisdiction"); see also USA PATRIOT Act of 2001 § 804.

Legislation, not rule-making, is the proper way to balance legitimate law enforcement needs with serious constitutional and policy considerations.

II. The Proposed Amendment Is Vague and Fails to Specify How Searches May Be Conducted and What May Be Searched

It is unclear what types of searches are being authorized by the proposed amendment. The proposed amendment provides that the government may use “remote access” to search and seize or copy electronically stored data. The term “remote access” is not defined. Sample search warrants submitted by the DOJ to the Committee indicate that “remote access” may involve network investigative techniques, or NITs, which include, for example, the installation of software onto a target device to extract and make available to law enforcement certain information from the device, including IP address, MAC address, and other identifying information.¹⁸ One sample warrant describes the deployment of an NIT onto a website to redirect certain information entered into the website to the government.¹⁹ None of the sample warrants provide any details regarding the nature of the NIT being deployed, technical details specifying how the NIT will extract the specified information, or details regarding how the NIT will avoid collecting information belonging to non-targets who may innocently access the targeted website or share the targeted device or account. In short, “remote access” seems to authorize government hacking of any facility wherever located.

There are a myriad of serious concerns accompanying the government’s use of NITs. These are outlined in detail in other comments submitted to the Committee and include, among other things, the creation of vulnerabilities in the target device thereby increasing the target’s risk of

¹⁸ See Memorandum from Jonathan Wroblewski, Office of Policy & Legislation, to Judge John F. Keenan regarding Proposed Amendment to Rule 41 of the Federal Rules of Criminal Procedure (Jan. 17, 2014) (“Wroblewski Memorandum”), available at

<http://www.uscourts.gov/uscourts/rulesandpolicies/rules/agenda%20books/criminal/cr2014-04.pdf>.

¹⁹ *Id.*

exposure to compromise by other parties, actual damage to the target device, the creation of a market for zero-day exploits, and unintended targets' exposure to malware.²⁰ Additionally, the remote facilities accessed by the government may in fact identify and disclose the “hack” or take action to prevent it or retaliate against its use. These are serious concerns that are more appropriately considered and balanced by Congress than by the Committee.

In addition to failing to specify or limit how searches may be conducted, the proposed amendment also fails to specify or limit what, precisely, may be searched once the media or information is accessed. The proposed amendment would allow the government to “use remote access to search electronic storage media and to seize or copy electronically stored information” where “the district where the media or information is located has been concealed through technological means.” The phrase “concealed through technological means” is not defined and, as written, can be used to justify searches of widespread and legitimate Internet use. For example, this language extends to those who use Virtual Private Networks (VPNs) (as do businesses across the country), which provide a secure connection to sensitive data but also obscure a user's actual network location.²¹ Therefore, routine use of lawful encryption technology would appear to satisfy the standard.²² Moreover, the proposed amendment contains no “intent” element to the concealment, which would require probable cause to believe that the

²⁰ See ACLU Memorandum to the Advisory Comm. on Criminal Rules (Oct. 31, 2014) (“ACLU Memorandum”), available at https://www.aclu.org/files/assets/aclu_comment_on_remote_access_proposal.pdf.

²¹ See, e.g., Written Statement of the Center for Democracy & Technology Before the Judicial Conference Advisory Comm. on Criminal Rules (Oct. 24, 2014) (“CDT Memorandum”), available at <https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/10/CDT-Rule41-Written-Statement-final-20141024.pdf>.

²² A number of news outlets have reported that Attorney General Eric Holder has authorized the National Security Agency to collect and indefinitely retain encrypted data, regardless of its U.S. or foreign origin, “for a period sufficient to allow thorough exploitation” of that data. Andy Greenberg, *Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It*, Forbes (June 20, 2013, 6:21 PM), <http://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/>; see also Declan McCullagh, *NSA 'secret backdoor' paved way to U.S. phone, e-mail snooping*, CNET (Aug. 9, 2013, 11:16 AM), <http://www.cnet.com/news/nsa-secret-backdoor-paved-way-to-u-s-phone-e-mail-snooping/>. The government therefore considers the mere use of encryption as a red flag that raises the suspicion of criminal misconduct. Law enforcement's suspicion of perfectly lawful activity indicates that the amendment as drafted may be fertile grounds for abuse.

target was purposefully concealing its location. Title III, for example, authorizes roving wiretaps only when the government can show that a target is switching facilities to avoid interception.²³

Likewise, the phrase “media” is not defined. This opens the door to law enforcement’s unfettered access to whatever information is accessible on the device being searched—whether that information is stored locally, on a network drive, or in the cloud. Devices such as computers and cell phones locally store or provide access to vast amounts of information that the Supreme Court has recognized amount to “the privacies of life.”²⁴

III. The Proposed Amendment Raises Serious Constitutional Concerns, and Case Law Addressing the Same Will Be Slow to Develop

The serious and complex constitutional concerns implicated by the proposed amendment are numerous and, because of the nature of Fourth Amendment case law development, are unlikely to be addressed by courts in a timely fashion.

First, the proposed amendment raises serious questions as to how the Fourth Amendment particularity requirement will be satisfied in applications submitted under Rule 41. The Fourth Amendment provides 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.”²⁵ In what ways will warrant applications specify what “storage media” will be searched? And how will law enforcement maintain certainty that only specified media is accessed? Will warrants issued under the proposed amendment provide any detailed assurances that non-targets will not be affected by the search? The sample warrant applications submitted

²³ 18 U.S.C. § 2518(11)(b)(ii) (requiring “probable cause to believe that the person’s actions could have the effect of thwarting interception from a specified facility”).

²⁴ *Riley v. California*, 134 S. Ct. 2473, 2494–95 (2014).

²⁵ U.S. Const. amend. IV.

by the DOJ, and case law addressing a similar warrant application, show that warrants issued under the new rules are not likely to satisfy the Fourth Amendment.²⁶

Second, there are legitimate concerns that the use of NITs to conduct remote access searches may constitute an unreasonable search because of their destructive and unpredictable nature. As noted by the ACLU in its comments to the Committee, the use of various forms of NITs, including malware and zero-day exploits, are more invasive than other searches because they often have unknown, widespread, and sometimes destructive consequences.²⁷

Third, the types of searches authorized by the proposed amendment may circumvent the “super warrant” requirements of Title III.²⁸ Title III applies to any government interception of wire, oral, or electronic communications.²⁹ Wiretap orders issued under Title III require protections absent from traditional warrants, including that the applicant show that it has exhausted other investigative techniques and that interception of non-necessary communications will be minimized.³⁰ Additionally, the DOJ Office of Enforcement Operations reviews each wiretap application before it is submitted to a court.³¹

The NITs deployed on target devices could in many instances have wide-ranging capabilities for accessing and engaging various features of the device, including the device’s camera and microphone.³² To the extent that a remote access search engages in techniques such as activating

²⁶ See Wroblewski Memorandum, *supra* note 17; *In re Warrant*, 958 F. Supp. at 759 (“The Government’s application offers nothing but indirect and conclusory assurance that its search technique will avoid affecting innocent computers or devices,” and the application fails to “explain how [the Government] will ensure that only those committing the illegal activity will be subject to the technology.”) (internal quotations omitted).

²⁷ ACLU Memorandum, *supra* note 19, at 17–18.

²⁸ 18 U.S.C. § 2518.

²⁹ *Id.*

³⁰ *Id.*

³¹ See *U.S. Attorneys Criminal Resource Manual* § 89, available at http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00089.htm.

³² See, e.g., *In re Warrant*, 958 F. Supp. 2d at 755–56 (warrant application to install NIT software that would enable the government to take photographs using the target computer’s built-in camera).

built-in cameras or microphones or collecting real-time ingoing or outgoing electronic communications, the heightened protections of Title III would be implicated.³³ It does not appear that the government has, to date, acknowledged the Title III implications of NITs with the Committee or offered a proposal for how it plans to address the issue. This raises the concern that the government will be reluctant to describe techniques to courts that may not always be sensitive to the possibility that Title III is implicated.

Fourth, the proposed amendment weakens Rule 41's notice requirement. Under current Rule 41, law enforcement must provide "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."³⁴ Under the proposed amendment, law enforcement need only "make reasonable efforts to serve a copy of the warrant on the person whose property was searched or whose information was seized or copied."³⁵ If the person whose property is seized is different from the person whose information was copied, only one person need be notified. The relaxed notice standard clearly indicates that warrants issued under the proposed amendment will in many instances be targeted at those to whom no notice can feasibly be given, such as when law enforcement is unsuccessful in ascertaining the target's physical location.

A search without notice is tantamount to a covert entry. Covert searches must be "closely circumscribed,"³⁶ and "the absence of any notice requirement in [a] warrant casts strong doubt on its constitutional adequacy."³⁷ The Ninth Circuit has held that a warrant is constitutionally

³³ 18 U.S.C. § 2518; *see also United States v. Torres*, 751 F.2d 875, 885 (7th Cir. 1984) (surveillance that "is identical in its indiscriminate character to wiretapping and bugging" requires Title III protections); *see also United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987) (requiring Title III protections for video surveillance).

³⁴ Fed. R. Crim. P. 41(f)(1)(C).

³⁵ Proposed Amendment to Rule 41 revised draft – April 21, 2014, *available at* <http://www.uscourts.gov/uscourts/rules/preliminary-draft-proposed-amendments.pdf>.

³⁶ *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986).

³⁷ *Id.* (citing *Berger v. New York*, 388 U.S. 41, 60 (1967)).

defective where it fails “to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry.”³⁸

The nature of Fourth Amendment case law development will make it difficult for courts to address these constitutional concerns any time in the near future, casting serious doubt on the Committee’s reliance on courts to address the numerous and significant constitutional issues raised by the proposed amendment. These issues are likely to evade review for a number of reasons.

First, warrant applications are considered *ex parte* and without the benefit of adversarial perspective by magistrate judges who may lack technical expertise or resources to comprehend the nature or the risks of the search proposed. This is especially true if the warrant applications do not provide the necessary description for the judge to understand the technique being used or to appreciate the constitutional consequences of that technique. This makes it unlikely that the issues will be caught in the warrant application phase.

Second, courts will often apply the good faith exception to the exclusionary rule prior to addressing the underlying constitutional issues implicated by the search, leaving any discussion of the Fourth Amendment challenge as *dicta* or, worse, foregoing any constitutional discussion at all.³⁹ Worse yet, law-abiding citizens who were the target of an unconstitutional search but are not charged with a crime will almost certainly never learn of the search and therefore will not be able to challenge the search.⁴⁰

³⁸ *Id.*

³⁹ *See, e.g., United States v. Clay*, 646 F.3d 1124, 1128 (8th Cir. 2011) (denying a motion to suppress on the basis of the good faith exception and declining to “reach the underlying question of probable cause”).

⁴⁰ *Cf. Stephen W. Smith, Gagged, Sealed & Delivered: Reforming ECPA’s Secret Docket*, 6 Harv. L. & Pol’y Rev. 313, 328 (2012) (discussing a target’s ability to challenge an electronic surveillance order issued under the Electronic Communications Privacy Act (“ECPA”).

Likewise, in those cases where the doctrine of qualified immunity applies, courts will often apply the doctrine first and forego a constitutional discussion altogether.⁴¹ Qualified immunity “protects government officials from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.”⁴² In other words, the doctrine “protects all but the plainly incompetent or those who knowingly violate the law.”⁴³ Under the doctrine, where the government relies on a warrant issued by a magistrate judge, courts have held that the government generally “cannot be expected to” question the magistrate judge’s determination that the warrant was proper.⁴⁴

Therefore, without previously established precedent or statutory law on the constitutionality of the searches permitted under the proposed amendment, case law discussing the constitutionality of such searches will develop slowly at best.⁴⁵ The Committee acknowledges that “there have not yet been many published opinions dealing with the various scenarios that would be covered by the proposed amendment,” but reasons that “these situations are likely to arise more frequently.”⁴⁶ Because this is in fact not likely to be the case, leaving constitutional questions to the courts will be an ineffective means of addressing the serious constitutional issues raised by the proposed amendment.

Additionally, the Committee should not reject the opinion of the at least one court that *has* addressed the extraterritorial effects of Rule 41 warrants that purport to authorize searches of computers outside the U.S.⁴⁷ That court denied a warrant application to remotely search a target

⁴¹ See, e.g., *Messerschmidt v. Millender*, 132 S. Ct. 1235, 1249 (2012) (foregoing a constitutional analysis after holding that qualified immunity applies).

⁴² *Id.* at 1244 (internal quotation marks and citation omitted).

⁴³ *Id.* (internal quotation marks and citation omitted).

⁴⁴ *Id.* at 1245.

⁴⁵ Cf. Smith, *supra* note 39, at 326–31 (discussing the dearth of appellate case law addressing ECPA in the 25 years since its enactment, and citing the lack of incentive to appeal ECPA orders as a cause: “The inevitable result is that appellate courts are rarely presented with the opportunity to interpret and apply ECPA’s complex provisions”).

⁴⁶ See Beale Memorandum, *supra* note 15, at 1.

⁴⁷ *In re Warrant*, 958 F. Supp. 2d 753, 758 (S.D. Tex. 2013).

computer whose location was unknown, citing many of the same constitutional infirmities Google raises today.⁴⁸

IV. The Proposed Amendment Would Authorize Remote Searches of Millions of Computers

The proposed amendment authorizes searches for investigations under § 1030(a)(5) of the Computer Fraud and Abuse Act (“CFAA”).⁴⁹ As the Committee notes, “[t]he proposal would enable investigators to obtain warrants to search computers in many districts simultaneously.”⁵⁰ Such search capabilities would enable law enforcement to investigate robot networks, or botnets, which are “automated malware program[s] that scan[] blocks of network addresses and infect[] vulnerable computers.”⁵¹ According to the FBI, a network of botnets can number “in the hundreds of thousands or even millions.”⁵² The implications of such searches should be left to Congress to weigh and to craft a statute that balances the privacy rights of affected network owners or operators with the investigative needs of law enforcement.

Subpart (B) of the proposed amendment extends beyond botnet searches, however. The definition of “damaged computer” under the CFAA is broad, encompassing “any impairment to the integrity or availability of data, a program, a system, or information.”⁵³ “Damage” may encompass, for example, software infected with unwelcome code,⁵⁴ malware, or viruses. As

⁴⁸ *Id.*

⁴⁹ This provision makes it a crime to “(A) knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer; (B) intentionally access[] a protected computer without authorization, and as a result of such conduct, recklessly cause[] damage; or (C) intentionally access[] a protected computer without authorization, and as a result of such conduct, cause[] damage and loss.” 18 U.S.C. § 1030(a)(5).

⁵⁰ Beale Memorandum, *supra* note 15, at 3.

⁵¹ Fed. Bureau of Investigation, *Botnets 101* (June 5, 2013, 7:00 AM), http://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them.

⁵² *Id.*

⁵³ 18 U.S.C. § 1030(e)(8).

⁵⁴ *See, e.g., United States v. Sullivan*, 40 F. App’x 740 (4th Cir. 2002).

noted by another commentator, it is estimated that nearly thirty percent of computers in the United States are infected with some form of malware.⁵⁵

Computers that have suffered “damage”, therefore, encompass computers belonging to millions of average Americans, many of whom are the victims of cybercrime, and the proposed amendment would permit remote searches into those computers.

V. Conclusion

Google urges the Committee to reject the proposed amendment to Rule 41. As Google has explained above, the proposed amendment substantively expands the government’s current authority under Rule 41 and raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns that should be left to Congress to decide.

⁵⁵ See CDT Memorandum, *supra* note 20, at 8 (citing Panda Security, Annual Report, PandaLabs (2013), available at <http://www.pandasecurity.com/mediacenter/wp-content/uploads/2010/05/Annual-Report-PandaLabs-2013.pdf>).

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h8g-jbl0
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0030](#)

Comment from Pennsylvania Bar Association, Pennsylvania Bar Association

Submitter Information

Name: Pennsylvania Bar Association

Organization: Pennsylvania Bar Association

General Comment

The Pennsylvania Bar Association, upon the recommendation of its Federal Practice Committee, respectfully submits the attached comments in response to the proposed amendments to the Federal Rules of Criminal Procedure.

Attachments

Comments-Criminal-FedRules-submit



February 16, 2015

Committee on Rules of Practice and Procedure
Administrative Office of the United States Courts
Thurgood Marshall Federal Judiciary Building
One Columbus Circle, N.E., Suite 7-240
Washington, D.C. 20544

Re: Proposed Amendments to the Federal Rules of Criminal Procedure

Dear Sir or Madam:

The Pennsylvania Bar Association, upon the recommendation of its Federal Practice Committee, respectfully submits the following comments in response to the proposed amendments to the Federal Rules of Criminal Procedure.

Respectfully,
Francis X. O'Connor, President
Pennsylvania Bar Association



COMMENTS OF THE PENNSYLVANIA BAR ASSOCIATION ON PROPOSED AMENDMENTS TO THE FEDERAL RULES OF CRIMINAL PROCEDURE

The Pennsylvania Bar Association makes the following recommendations with respect to some of the proposed Criminal Rule changes:

Criminal Rules 41, and 45.

- The PBA opposes and submits the following comment in opposition to the proposed amendments to Rule 41, governing search warrants. The proposed amendments to Rule 41 substantively expand the government's investigative powers, which should be addressed by Congress in the first instance. Specifically, the proposed amendment confers authority upon a magistrate judge to authorize a category of searches that the government is currently barred from conducting. Congress has provided a legislative solution when necessary, and congressional action lends itself to substantive limits on questionable search practices in a way that rulemaking does not.
- The PBA opposes the proposed amendments to Rule 45 that would change the three-day enlargement of time for a response to an electronically-served filing.

PBA FEDERAL PRACTICE COMMITTEE
COMMENTING ON THE
PROPOSED AMENDMENTS TO THE FEDERAL RULES OF
APPELLATE, BANKRUPTCY, CIVIL, AND CRIMINAL PROCEDURE

HON. D. MICHAEL FISHER
CHAIR

SUSAN E. ETTER, ESQUIRE
PROJECT COORDINATOR

KATHLEEN WILKINSON
BOG LIAISON

MEMBERS OF THE SUB-COMMITTEE

ROBERT L. BYER, ESQUIRE

PHILIP GELSO, ESQUIRE

MELINDA GHILARDI, ESQUIRE

MATTHEW M. HAAR, ESQUIRE

HENRY W. VAN ECK, ESQUIRE

MEMORANDUM

TO: Susan E. Etter, Esquire
Project Coordinator

FROM: Philip Gelso, Esquire, & Melinda Ghilardi, Esquire
Subcommittee on Criminal Rules

DATE: January 13, 2015

RE: Report of the Subcommittee on Proposed Amendments to Criminal Rules

I. Introduction

The proposed changes to the Criminal Rules contain three amendments. The proposed amendments to Rule 4, governing time limits for service of criminal process, are discussed first. The proposed amendments to Rule 41, governing search warrants, are discussed second. And the proposed amendments to Rule 45, governing an enlargement of time to respond to a filing that is served electronically, are discussed last.

II. Report and Comment

Rule 4

Proposed Amendments

Rule 4 governs service of criminal process on defendants. Due to the current Rule's lack of focus on foreign corporations as criminal defendants, the Rules Advisory Committee decided to amend the Rule to authorize coercive sanctions should foreign corporate defendants fail to appear, limited the obligation to mail process to foreign corporate defendants, and authorized other methods to effect service on foreign corporate defendants, such as by agreed upon methods, diplomatic channels, channels authorized by international agreements, and an option of any method that gives notice should alternative methods appear insufficient.

Comments

These amendments did not generate comments, and the Committee recommends that the PBA make no comment on these amendments.

Rule 41

Proposed Amendments

Rule 41 governs how search warrants are to be authorized and conducted. The proposed amendments to Rule 41 seek to add a new subsection (b)(6) and a corresponding change to subsection (f)(1)(C). Proposed new subsection (b)(6) confers authority upon a magistrate judge "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." The proposed additional language to subsection (f)(1)(C) provides the notice requirement when a warrant is executed pursuant to the proposed subsection (b)(6).

Comments

The Committee recommends that the Rules Advisory Committee reject the proposed amendments to Rule 41. The proposed amendments substantively expand the government's investigative powers, which should be addressed by Congress in the first instance. Specifically, the proposed amendments confer authority upon a magistrate judge to authorize a category of searches that the government is currently barred from conducting. While the rapid change of technology and government's need to counter these technological advancements when investigating and prosecuting criminal activity is understandable, the proper way to address this situation is for the government to seek congressional action as has been done in the past in similar circumstances. In those circumstances, Congress has provided a legislative solution. See, e.g., 18 U.S.C. § 3123 (Stored Communications Act); 18 U.S.C. § 2518 (Title III of the Omnibus

Crime Control and Safe Streets Act of 1968 (“Title III” or “the Wiretap Act”)); 50 U.S.C. § 1804 (the Foreign Intelligence Surveillance Act); 18 U.S.C. § 3123 & 50 U.S.C. § 1842 (regarding metadata collection in criminal and national security investigations in pen registers). As has been done in the past, congressional action is preferable to address the government’s concerns because it lends itself to setting substantive limits on questionable search practices in a way that procedural rulemaking does not. As a result, the proposed amendments to Rule 41 should be rejected.

Rule 45

Proposed Amendments

As currently worded, Rule 45 allows a party who must respond to a filing that has been electronically served three more days in addition to the response time prescribed by the Rules. Under the current version of Rule 45, a person who is served by mail, by leaving the document with the clerk, by delivery by any other agreed means, or by electronic delivery, has three additional days to respond. The proposed amendments will remove the additional three days when a person has been electronically served. The Rules Advisory Committee suggests that the original wording of Rule 45 was due to fears that electronic service would be delayed, and that those concerns have abated. Additionally, the Rules Advisory Committee suggests that removing the three-day additional period will simplify calculating response times.

Comments

The Committee recommends that this amendment be opposed. The Committee is concerned that electronic service may happen at any time of day or any day of the week. Therefore, 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.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h8n-jn3u
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0031](#)

Comment from Peter Goldberger, National Ass'n of Criminal Defense Lawyers

Submitter Information

Name: Peter Goldberger

Organization: National Ass'n of Criminal Defense Lawyers

General Comment

The comments of the National Association of Criminal Defense Lawyers on the proposed amendments to Fed.R.Crim.P. 4 and 45 are attached. Our comments on the proposed Rule 41 amendment will be submitted separately, on the 17th.

Attachments

NACDL Comments - Crim 4&45 021615

NACDL
1660 L St., NW, 12th Fl.
Washington, DC 20036

February 16, 2015

To the Members of the Advisory Committee:

The National Association of Criminal Defense Lawyers is pleased to submit our comments on the proposed changes to Rule 4 and 45 of the Federal Rules of Criminal Procedure. Our comments on the proposed amendment to Rule 41 will be submitted separately.

Our organization has approximately 10,000 members; in addition, NACDL's 94 state and local affiliates, in all 50 states, comprise a combined membership of over 30,000 private and public criminal defense attorneys and interested academics. NACDL, which celebrated its 50th Anniversary in 2008, is the preeminent organization in the United States representing the views, rights and interests of the criminal defense bar and its clients. As you know, we are regular observers at Committee meetings and have a long record of submitting comments. On the basis of that history, we appreciate the close and respectful attention that our comments have always received.

CRIMINAL RULE 4 – SERVICE OF WARRANT OR SUMMONS

NACDL understands that it is possible for a foreign organization (or individual) to commit an offense against United States criminal law without setting foot, so to speak, in this country. We agree that it should be clear under the Rule how a summons is to be served on such an organization. We note that although the amendment is of Rule 4 (governing summonses issued upon a complaint) only, this rule is adopted by reference in Rule 9. The latter context is of far greater significance, since most criminal prosecutions of organizations by far are by information or indictment, for which service is governed by Rule 9, not by Rule 4 directly.

NACDL supports adding language to section (a) addressing the possibility that an organizational defendant (particularly one that has no U.S. presence) may fail to appear in response to a summons, but only with the inclusion of a clarifying caveat: that proceeding with a prosecution *in absentia* is not authorized, as should perhaps already be clear from Rule 43(a). This necessary qualification could be addressed in the Advisory Committee Note, or by adding to the end of new section (a) the words “, and consistent with Rule 43(a).”

NACDL supports the proposed amendment to section (c) with two related changes. Under proposed new Rule 4(c)(3)(D), a summons could be served on a defendant that is “not within a judicial district of the United States” in either of two ways.

However, the proposal not make clear what exactly it means by “not within the United States” as applied to an organization. We suggest a clarification by adopting words from the proposed Advisory Committee Note (that the accused has “no place of business or mailing address within the United States”). We suggest that the amendment be further revised to reflect explicitly what we infer to be its intended meaning. First, that service within the United States under Rule 4(c)(3)(C) is preferred over use of the new paragraph (3)(D) if service under (3)(C) is likely to give actual notice, and that service under subparagraph (3)(D)(i) is preferred over service under subparagraph (3)(D)(ii). Thus, the amended subsection (c)(2) should read:

“(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 may be served under Rule 4(c)(3)(D) at a place not within a judicial district of the United States only if 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.**”

Our suggestion effectuates the suggested clarification by deleting “also” and adding a condition that also serves to define the key concept. (It also moves the phrase “under Rule 4(c)(3)(D)” to its proper location in the sentence; it is the *service*, not the *organization*, that would be “under” the stated provision.)

Relatedly, new paragraph (c)(3)(D)(i) should be amended to add, following the “or” after the final semicolon, “if service under this subparagraph does not apply, then”.

NACDL also strongly supports adherence to the rule, which is implicit in the proposed amendment, that a summons or warrant can only be served effectively on an *individual* by personal service, even if that individual is not within the United States, regardless of the reason for his or her absence. That is, to reiterate the point made above with respect to section (a), prosecution *in absentia* is not allowed.

Finally, we would be remiss if we did not mention that NACDL supports a return to the regime, long supported by this Committee and the Supreme Court (as reflected in the amendment history for 1974-75¹), under which discretion under Rule 4 whether a summons should be issued to a defendant in lieu of a warrant would rest with the Magistrate Judge rather than with the prosecutor. Far too many non-violent and otherwise compliant persons accused of federal crimes are brought to court today by arrest rather than by summons, only to be promptly and properly released on unsecured bond. Yet as a matter of caution and self-protection law enforcement officers execute nearly all arrest warrants forcibly and by surprise,

¹ Only by a very close vote in the House was this salutary reform proposal defeated; *see* 1 Chas. A. Wright, Fed. Prac. & Proc.: Criminal § 51.

causing entirely unnecessary fear, trauma and even injury to the accused and third parties alike (including innocent family members), among other detrimental effects. The wording of Rule 4(a) should be revised to confer discretion on the Magistrate Judge and to express a preference for issuance of a summons, rather than a warrant, unless “good cause” for the latter is shown by the government, placing the rule in harmony with the corresponding policy of the 1984 Bail Reform Act.

CRIMINAL RULE 45 – COMPUTATION OF TIME AFTER ELECTRONIC SERVICE

NACDL opposes the proposed package of amendments – including the proposed amendment to Criminal Rule 45 – to remove from the list of circumstances in which three days are added to otherwise stated time limits those (many) occasions when a document is due under a Rule or court order to be filed a certain number of days “after service” of another paper, and service has been made by electronic filing. Regardless of the arid logic behind the proposal, the fact is that the amendment would reduce by three days the time available to counsel to respond to an adversary’s motions (or to file objections to a Magistrate Judge’s Report and Recommendation, which is also measured from “service”). This small increase in the speediness of proceedings would provide little if any benefit to the court or the public, while placing additional burdens on busy practitioners.

The three day rule has no application, and no impact, in those instances where by local rule filings must be made within a specified number of days in advance of a hearing date. Thus, there is no need to abandon the three day provision in order to insure courts receive filings sufficiently in advance of a hearing, as that concern can be better addressed by changing the date that determines when a filing is due.

It may be that the original justification for adding three days – to take into account that the date of service was not the date of receiving actual notice – no longer obtains. *Cf.* Fed. R. App. R. 26(c) (adding three days “unless the paper is delivered on the date of service stated in the proof of service.”) There are other reasons, however, that justify the additional time. While it used to be that one needed three days to receive a filing due to the mail, nowadays one often needs a day or two to have time to review an electronic filing.

This is particularly so as to criminal defense lawyers, whose clients may be incarcerated but who may have to be consulted before responses can be prepared. Many defense lawyers practice solo or in very small firms. Many are in court for much or all of normal working hours on most days. Many have little if any clerical or paralegal support, particularly in the digital age with its decreased demand for secretaries. For this reason, many defense lawyers do not see their ECF notices – much less open and study the linked documents – immediately or even on the same

day the are “received” by the attorney’s email address. The burdens thus placed on defense counsel (and thus indirectly on defendants) by the proposal – as well as the increased burden on trial courts, which will be confronted with many more motions for short extensions of time, or for leave to file documents out of time – far outweigh any perceived benefit in simplicity or abstract elegance in the rules.

Finally, we do not understand the why the proposed amendment would add the words “; Time for Motion Papers,” to the name or title of the Rule. There is no discussion as to why this change is being proposed. It is likely to add confusion, as the Rule does not directly determine the time for the filing of motions papers, but only provides a mechanism for doing so.

We thank the Committee for its excellent work and for this opportunity to contribute our thoughts.

Respectfully submitted,
THE NATIONAL ASSOCIATION
OF CRIMINAL DEFENSE LAWYERS

By: Peter Goldberger
Ardmore, PA

William J. Genego
Santa Monica, CA

*Co-Chairs, Committee on
Rules of Procedure*

Please respond to:
Peter Goldberger, Esq.
50 Rittenhouse Place
Ardmore, PA 19003
E: peter.goldberger@verizon.net

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h92-i5q2
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0032](#)

Comment from Edward Mulcahy, NA

Submitter Information

Name: Edward Mulcahy

Organization: NA

General Comment

Ummm... wow. Let me say this clearly: Every government degenerates to petty tyranny. Ours is no exception. I am firmly against this. The government's power is already too vast and secret. Leave the internet and encryption alone.

Ladar Levison stated it best: The US Courts are considering an amendment to the rules of criminal procedure which, if passed, would make using a VPN or TOR sufficient evidence of wrongdoing to justify a search warrant. Under the new rules, this search warrant would allow, amongst other things, the FBI to remotely push spyware onto your computer...

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h93-rpfa
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0033](#)

Comment from Kati Anonymous, NA

Submitter Information

Name: Kati Anonymous

Organization: NA

General Comment

I am opposing your rule 41 for remote electronic searches. Private still means private. 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.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h93-co6h
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0034](#)

Comment from Jeff Cantwell, NA

Submitter Information

Name: Jeff Cantwell

Organization: NA

General Comment

NO, you may not spy on my communications just from the fact that I try to enforce my right to privacy. This would be the same as saying the government has a right to read my mail just because I've sealed the envelope. This is nothing more than an excuse to strip away the last of our right to privacy.

The abundance of information you require just to file a comment shows just how little the government values it's citizens privacy.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h93-8tzk
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0035](#)

Comment from Benoit Clement, NA

Submitter Information

Name: Benoit Clement

Organization: NA

General Comment

This is yet again another move to infringe upon the privacy and freedoms of citizens.

If there is to be so much transparency for the people, why does the government repeatedly hide all of its corruption, spying and war profiteering agendas?

This is an unfair practice.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h94-z4tl
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0036](#)

Comment from Yani Yancey, NA

Submitter Information

Name: Yani Yancey

Organization: NA

General Comment

I am writing to firmly oppose this regulation. The Federal government has funded development of TOR and encourages people to use both it and VPN for legitimate security reasons. Now it seeks to paint their use as criminals and strip away the 4th amendment rights of people without any real suspicion of wrongdoing. It's quite clear federal agencies are addicted to conducting unjustified fishing expeditions on a massive scale, but this is a bridge too far. Attempting to safeguard your personal information and online activity is not a criminal or suspicious act. Reject this preposterous amendment.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h95-1g36
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0037](#)

Comment from Jeffrey Adzima, NA

Submitter Information

Name: Jeffrey Adzima

Organization: NA

General Comment

I'm writing as a concerned citizen against this proposal which appears to be in direct conflict with our current Constitutional protections, specifically, amendment 4 against unwarranted search and seizure of private property. Specifically as stated in the US Constitution - Amendment 4 states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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."

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h98-3lem
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0038](#)

Comment from Peter Goldberger, National Ass'n of Criminal Defense Lawyers

Submitter Information

Name: Peter Goldberger

Organization: National Ass'n of Criminal Defense Lawyers

General Comment

The attached document contains the comments of the National Association of Criminal Defense Lawyers on the proposed amendment to Rule 41. Our comments on the proposals to amend Rules 4 and 45 were submitted separately, yesterday.

Attachments

NACDL comment CrimR41 021715

NACDL
1660 L St., NW, 12th Fl.
Washington, DC 20036

February 17, 2015

To the Members of the Advisory Committee:

The National Association of Criminal Defense Lawyers is pleased to submit our comments on the proposed changes to Rule 41 of the Federal Rules of Criminal Procedure. Our comments on the proposed amendments to Rule 4 and 45 will be submitted separately.

Our organization has approximately 10,000 members; in addition, NACDL's 94 state and local affiliates, in all 50 states, comprise a combined membership of over 30,000 private and public criminal defense attorneys and interested academics. NACDL, which celebrated its 50th Anniversary in 2008, is the preeminent organization in the United States representing the views, rights and interests of the criminal defense bar and its clients. As you know, we are regular observers at Committee meetings and have a long record of submitting comments. On the basis of that history, we appreciate the close and respectful attention that our comments have always received.

CRIMINAL RULE 41 – WARRANTS AUTHORIZING REMOTE ACCESS TO COMPUTERS

The proposed amendment to Rule 41(b) would add to the Rule a third circumstance in which a Magistrate Judge may issue a warrant to search for and seize property located outside the judicial district. One of the existing circumstances is uncontroversial and deals with a purely practical problem – a warrant to search in U.S. territory outside the boundaries of any District. *See* Rule 41(b)(5). The other such existing authority, found in subsection (b)(3), was inserted into the Rule by legislative action, the USA PATRIOT Act of 2001, and applies only to investigations of domestic or international terrorism. *See also* 18 U.S.C. § 2703(a); *In re Search Warrant*, 2005 WL 3844032 (M.D.Fla. 2006) (Stored Communications Act, as amended by PATRIOT Act, adopting procedures of Rule 41), *rev'g* 362 F.Supp. 2d 1298 (M.J.-M.D.Fla. 2003). The broad and remarkably vague wording of subsection (b)(3) has yet to be authoritatively construed and has been the subject of only a few lower-level opinions. Yet the proposed amendment, without legislative support, would go even further, and codify a broad new authority to issue warrants for out-of-district searches for (and of) computers in relation to the investigation of any federal crime and – in certain computer crime cases – simply for the convenience of law enforcement agents even if the location of the computers is known.

While presented as addressing a venue problem, the proposal would instead essentially eliminate any venue requirement for digital searches of this kind by making the Rule's limitations so expansive and unbounded as to be meaningless. NACDL opposes this amendment, both 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.

For nearly 50 years, ever since the landmark opinion of the Supreme Court in *Berger v. New York*, 388 U.S. 41 (1967), the Supreme Court has recognized that the Fourth Amendment is not impotent to control new forms of law enforcement intrusion upon the privacy and security of “the People in their persons, houses, papers, and effects” that are made possible by advances in technology. But ordinary search warrants, governed by ordinary standards, often will not suffice to meet the demands of particularity and reasonableness of execution in new technological contexts, as *Berger* explained. For this reason, in response to that decision, Congress in 1968 enacted a detailed statutory scheme for the authorization and regulation of wiretapping, 18 U.S.C. §§ 2510-2521 (“Title III”), which has since stood the test of time and judicial scrutiny. Congress acted upon the same lesson when it adopted – and on later occasions amended – the Stored Communications Act, 18 U.S.C. §§ 2701-2708, 2711, as well as less complex but nonetheless carefully crafted legislative provisions to govern other kinds of searches. *See* 18 U.S.C. § 3117 (mobile tracking devices); 18 U.S.C. §§ 3121-3127 (trap-and-trace devices).

No current law or rule attempts to address the Fourth Amendment issues implicit in any use of “remote access to search electronic storage media and to seize or copy electronically stored information,” to quote the current proposal. The principal flaw in the proposed change in Rule 41 is that it suggests a view that such searches may properly be authorized by ordinary warrants. NACDL very much doubts this is so. By attempting to bring such searches within the conventional framework of Rule 41, the proposal disrupts fundamental balances of jurisdiction and traditional warrant requirements based upon an analysis of what is most expeditious for law enforcement, while turning a blind eye to the inescapable conclusion that these aggressive digital interventions, which both exploit vulnerabilities in the Internet and deliberately create new ones, have technological, political and constitutional implications far beyond the simple mechanics of their application to a specific law enforcement goal.

Changes with such far-reaching potential consequences, even when procedural in form, are not merely procedural. (The line between substance

and procedure is particularly fraught in the context of search warrant regulation, even in its least controversial provisions. See, e.g., Rule 41(c) (listing items subject to search or seizure, which is arguably not “procedural” at all.) Expansion of search authority in response to new technological challenges is political in the purest sense, and requires a political process to justify enactment. No matter how sage and responsible in fulfilling its mission the Committee may be, it is not the forum for resolving the merits of such dramatic change against the demerits of its many unintended but inevitable consequences.

The Advisory Committee Note assures us that “the amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require.” Given the disruptive constitutional and commercial potential inherent in the aggressive tactics to be authorized under the jurisdictional liberality of the amended Rule, and in light of the dearth of precedent guiding the procedural innovation of countering hackers with hacks and the obscure horizons of the permissible scope of authorized seizures, the deferring of such questions is unsatisfactory. This is particularly so where the first case to discuss an application for a “network investigative techniques” warrant concluded that the request had to be denied on constitutional grounds. See *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 758-61 (S.D.Tex. 2013). The fact that there is almost no case law under subsection (b)(3), the terrorism clause, after more than a decade further suggests that reliance on later litigation is not a solution in this context. Motions to suppress are no answer, when the “good faith” exception to the exclusionary rule validates nearly any search conducted under a facially valid warrant. (Moreover, as described below, many of the resulting invasions of privacy will involve searches of computers belonging to bystanders; no person who is later accused will necessarily even have standing to challenge the search.) The proposed amendment thus constitutes a *de facto* grant of power unaccompanied by any framework of restraint. Only a Title III-like statutory regime, not a Rule amendment, can provide what is needed to render such searches reasonable in the context of the often unfamiliar and always transforming digital domain.

The NACDL respects the need for evolution in our criminal procedural rules designed to preserve their traditional purpose and function in changing times. In the face of evolving demands, it is certainly within the reach of this committee to make incremental, graduated and moderate changes in Rule 41 that pull up short of a constitutional, technological and diplomatic cliff. In this instance, however, the fact that the Rule presently does not always authorize a Magistrate Judge to issue a warrant to search the whole of the Internet to locate a computer that is being surreptitiously used to commit some federal offense is not a flaw or weakness in the Rule; rather, it is a

reflection of the fact that such searches by their nature pose threats to the protected privacy interests of an unknown number of innocent persons, require special regulation as to scope, and pose special problems with respect to the constitutional requirement of particularity that cannot be addressed with a simple Rules amendment.

Other submissions and letters to the Committee have identified many of these inherent dangers. Some have set out proposals for additional language that would establish additional limits upon the scope and impact of the proposed Rule change. Technologists have identified and explained why so radical a change in the scope of network search and seizure urgently demands extensive legal controls – defined legislatively and enforced judicially – over the use of “network intervention techniques.” This is especially so where all the effects of deploying these search methods cannot be anticipated and in some respects are not even fully understood.¹ Internet privacy advocates have sounded alarms that place the present problem in the larger context of how the Fourth Amendment applies in the digital realm.²

The proposed restrictive clauses – which would be codified as Rules 41(b)-(6)(A) and (B) – do not serve to limit the scope or cabin the danger nearly enough.

To begin with, the introductory language would permit a warrant authorizing remote access to search and seize electronic storage media and information outside a district to be issued by a Magistrate Judge “in any district where activities related to a crime may have occurred.” This, of course, is essentially no restriction at all. First, the speculative phrase “activities related to a crime may have occurred,” which is derived from the PATRIOT Act provision, has yet to be judicially limited in any way. What is “activity” that is “related to” a crime? It is not even clearly limited to “criminal activity.” Does it require that the warrant application include a showing upon which the Magistrate Judge could find reason to believe that venue for prosecution of the suspected offense might later properly be found in that District? Does it include victim impact that would not support venue? See *United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (extravagant government theory of

¹ See “Comments on Proposed Search Rules” submitted by Steven M. Bellovin, Matt Blaze, and Susan Landau and “Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning ‘Remote Access’ Searches of Electronic Media” for elaborate detailing of government experience and practices deploying surveillance software.

² See Electronic Privacy Information Center, “Testimony and Statement for the Record,” presented for the hearing held November 5, 2014; “Written Statement of The Center for Democracy & Technology,” submitted October 24, 2014.

venue over computer crimes rejected). Does it mean a District through which an electronic communication may have traveled? If so, then not one of the 94 federal districts is ineligible for warrant-issuing jurisdiction over a crime alleged to have been committed through use the use of an anonymized device, or if the offense being investigated is a CAFAA violation and several target computers in various localities have been “damaged” in the trivial sense defined at 18 U.S.C. § 1030(e)(8). Since no single Internet-connected location in any District can be excluded as one that “may” have experienced activities related to the crime, a diligent Magistrate Judge assessing her jurisdictional authority could hardly come to any conclusion other than that jurisdiction resides with her. The fruits of the Internet, bitter or sweet, are accessible in every part of our Nation and across the world wherever an IP address is to be found, and any device can be linked, even unknowingly with any other (so long as even one user among many shares access to that device). The incentive that is created for zealous law enforcement officials to forum-shop for the most pliant Magistrate Judge is also apparent.

Unlike more measured and carefully considered legislative solutions to the inaccessibility of telephonic aural communications, which are equally opaque to investigators without intrusion into the technology of the device network, the proposed Rule change would not discriminate as to the gravity of the offense. Instead, a paragraph inserted into a procedural rule invokes the most invasive technological dragnet of digital information and communication ever granted by a non-FISA warrant and applies it across the entire range of federal crimes. Rule 41 as amended would offer federal agents the power to hack their way into any number of computers, servers, storage accounts, laptops, and flash drives once an anonymous address had been exposed, whether the offense under investigation is commercial production and distribution of child pornography or a hit-and-run collision in the Veterans Administration hospital parking lot.

We respectfully disagree with the premise of the proposed amendment that all crimes under federal investigation associated with any concealed location or content on the Internet, or which may involve minor even if inadvertent damage to five disparately located computers, can justify the same disregard of traditional jurisdictional concerns as do terrorism investigations. A procedural rule change that applies to all federal criminal investigations is far inferior to the Title III model of legislation that limits extreme network intrusion to a defined subset of serious offenses. *Cf.* 18 U.S.C. § 2516(1)(a)-(t).

By removing the district-specific jurisdictional standard the rule dismisses the foundational principle that due process has a “place” dimension. The responsibilities of U.S. Magistrate Judges bring them into the closest contact with the broadest spectrum of individuals in their communities. There is a

deeply rooted history in Anglo-American jurisprudence as to why we are judged by a jury of our peers, *see* U.S. Const., Art. III, § 2, cl. 3; Amend. VI; for the same reason, the seizure of our persons and property is only authorized by a judge who is a member of our own community. Local jurisdiction is local accountability and deference to the diversity of regions and communities of which each Federal District is comprised is not to be lightly dismissed. The digital world is no less immediate and no less geographical than the physical communities in which it resides. The Internet may be accessible anywhere, but everything on the Internet is also most certainly somewhere. As much as we hear about “the Cloud,” every digital cloud sleeps on the ground. Digital systems and the content within them cannot escape local jurisdiction. The question is only whether we build upon or ignore the virtues of local jurisdiction as Rule 41 and our Constitution currently define it.

It is estimated that almost 85% of TOR (anonymized router) users are in countries other than the United States.³ To the government’s credit, it does not rely on this fact (which would arguably place most searches for unknown computers on the Internet outside of *any* Fourth Amendment and Rule 41 regulation; *see United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990); *In re Terrorist Bombings of U.S. Embassies*, 553 F.3d 150 (2d Cir. 2008, as amended 2009)) to eschew warrants entirely. The conferring of search jurisdiction based upon the technological concealment of location guarantees that invasive and potentially destructive actions will be taken against computer systems and storage media located outside the United States, as well as within. Other commentators have articulated how ill-advised such violations of other nations’ sovereignty may be.⁴ The range of application for the “network investigative techniques” – a polite term for court-authorized government hacks – extends well beyond the clear-cut “worst cases” that the government naturally cites.

The proposed limitation of the new Rule to two particular sorts of cases affords little protection against the dangers of searches *for* (and then *of*) computers in unknown locations.

The first of the two alternative prerequisites for a warrant to remotely search a targeted computer is met when “the district where the media or information is located has been concealed through technological means.” Rule 41(b)(6)(A). Much of the Committee’s concern is focused upon the technology of rendering “anonymous” the identifying information that would reveal the Internet

³ Tor, TOR Metrics: Users, Top-10 countries by directly connecting users,” <https://metrics.torproject.org> (83.76% overseas in 2015).

⁴ *See* Center for Democracy & Technology, *supra* note 2, at 3.

Protocol address of the targeted digital device. Law enforcement must have device-specific IP address information to determine the physical location, and thus, the jurisdiction where the computer and its contents are located. If the goal of this warrant were only to hack through whatever means of technological concealment deprived investigating agents of the location data needed to find the device agents wished to search, the language of the proposed rule would be simpler: the search would be specific to location information only, and *not* authorize accessing the information *after* the location information establishing jurisdiction was obtained. The location of the targeted computer is not obtained solely for the purpose of identifying jurisdiction. Location information is an intermediate objective to the search and seizure of the contents of a computer or storage media that has been concealed by its owner-administrator. The extraordinary search authorized by the proposed Rule thus far exceeds in scope the special justification that is proffered for allowing it.

A target computer's anonymity may invoke a (b)(6)(A) warrant issued from any district where "activity related to a crime may have occurred," but it is ordinary probable cause to believe that a crime "may have occurred" that allows the warrant. Anonymity alone does not in any way add to the probable cause for a Fourth Amendment-qualified search and seizure. At most, it justifies going to a Magistrate Judge who might otherwise not have jurisdiction. The global framework of governments, industries, scientists, political activists, health care and legal professionals all conceal digital identity for lawful, justifiable reasons. Comparatively few hidden secrets are actually secret crimes.

One conundrum presented by the proposed amendment to Rule 41 is what scope of search and seizure is actually granted once the location of the target computer and its contents has been identified. As proposed to be amended, nothing in the Rule would clearly require that the highly intrusive search be limited to ascertaining the concealed location, or even to searching the particular media discovered at that location. A statute could provide that sort of restriction. Instead, a warrant issued under the amended Rule could seemingly grant a free pass to whatever resources are accessible from the targeted device, on the theory that access privileges are a sort of "information" in a stored media.

Anonymizing methods prevent identification of source. The language of the proposed Rule, tied to the precise problem at hand (identifying the appropriate Magistrate Judge), states that the remote access technique may be employed only if the *location* of the "the media" or "information" was concealed. The qualifying predicate for (b)(6)(A) warrants excludes all circumstances in which only the *content* in a storage media has been

concealed (for example, encrypted), since that form of concealment does not prevent ascertaining the IP address and thus the location. Although this plain language interpretation is unlikely to be the farthest reach attempted under the proposed amendment, if this change to Rule 41 is adopted the language should be revised to clearly restrict the scope of the warrant-authorized search to that media and content whose location was concealed, and only for the purpose of ascertaining their location. The warrant should not permit the agent using remote access techniques to reach into others systems, drives, computers and the like, nor to search or seize contents of computers that may have been concealed, other than location information for the device. (Similarly, information on a storage media that only cloaks the location of file content storage on the device media, such as steganographic measures,⁵ should not trigger Rule 41(b)(6)(A) – or be the object of such a search – because such measures do not conceal the federal district in which the information is located.) Even on an anonymous server, any mode of concealment of media or information not disguising “the district where the media or information has been concealed” should not be subject to the remote access techniques of law enforcement under this proposed rule change.

The amendment should not be adopted unless 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). Accessibility from an anonymous device does not bestow anonymity upon all devices that it accesses. The proposed Advisory Committee Note likewise does not elaborate on the scope of its allowable or intended use. Again, we suggest that such limitations, while necessary, are more appropriately provided in a statute, which would not be restricted to provisions that can be called merely procedural.

The second proposed limiting class of cases, under Rule 41(b)(6)(B), raises equally problematic issues. The condition specified – that computers located in five or more different districts have been “damaged” – logically would seem to justify the proposed remedy – that is, allowing issuance of the warrant by a Magistrate Judge in any affected district – only if the investigative technique to be authorized is anticipated to involve a search of those numerous victim computers. Otherwise, why would the thing to be searched be considered to be outside the District? In other words, the persons whose privacy is to be invaded with tools of unknown (but predictably harmful) effect are putative victims, not even suspects much less probable perpetrators.

⁵ Steganography is technique of concealment in which one type of message or file is hidden within another of a different type, such as concealing a text message, image, or video inside a computer file of a different type or format.

There are many discrete attacks in which the use of network investigative technology can identify and countermand the illicit requisitioning of computing resources and their use in criminal enterprises within the scope of 18 U.S.C. § 1030(a)(5) investigations. Beyond the “Botnet” example offered to the committee is any number of far more subtle and nuanced scenarios that will be tempting to solve with “network investigations” rather than more common police work where the boundaries of appropriate methods are well established. The limitation suggested at proposed (b)(6)(B) is therefore not a meaningful or effective restraint on the power that would be affirmed by this amendment.

The government’s original proposal for a change to Rule 41 came in response to Magistrate Judge Stephen Wm. Smith’s ruling in *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753 (S.D.Tex. 2013), where an FBI application for a warrant was denied. In references to this ruling before the Committee, the shorthand version of the holding focused on Rule 41 and the question of jurisdiction to issue a warrant to locate and then to search (and otherwise intrude) within an anonymized computer. That was one point that Judge Smith made, *id.* 756-58, but the opinion is more concerned with the FBI application’s not satisfying the requirements of the Fourth Amendment, including the enabling of video surveillance through the target computer’s built-in camera feature. *Id.* 758-61. Judge Smith’s opinion reflects the problem that the Internet is not an amorphous area to be searched at large, but rather a vast community of persons utilizing technology to support an exchange of ideas, of commerce, and of invention, as well as sometimes being a repository of evidence of crime. The many particular uses to which each individual’s own computer may be put require a careful measure of Fourth Amendment scrutiny.

It is surely possible to craft a constitutionally compliant procedure for searches in the virtual domain, but probably not within the confines of rulemaking. NACDL suspects that this *modus operandi* may require a series of graduated steps of iterative warrant applications as an investigation reveals the specific articles that are within reach of probable cause. This is analogous to the process under Title III, where 30-day reports are provided to justify renewals of a wiretap or extension of the tap to another phone number. Applying the guidance of the Supreme Court found in the *Berger* opinion, a legislative approach would be more apt. If, in the application of a procedural rule, a magistrate cannot know *a priori* the geographical reach, the ultimate scale, or the number of searches she is authorizing, a finding that Fourth Amendment requirements have been met is improbable. The proposed Rule 41 changes would inevitably send the opposite message, with the imprimatur of the federal judiciary. Because the very circumstances that

make problematic ascertaining the proper District within which a Magistrate Judge has jurisdiction are those which cause any digital search that could be authorized by an ordinary warrant to be open-ended and thus constitutionally unmanageable, the amendment should be rejected as currently drafted.

We thank the Committee for its efforts to improve our justice system and for this opportunity to contribute our thoughts.

Respectfully submitted,
THE NATIONAL ASSOCIATION
OF CRIMINAL DEFENSE LAWYERS

By: Samuel A. Guiberson
New York City, NY

*For the NACDL Committee
on the Fourth Amendment*

Peter Goldberger
Ardmore, PA

William J. Genego
Santa Monica, CA

Co-Chairs, Committee on Rules of Procedure

Please respond to:
Peter Goldberger, Esq.
50 Rittenhouse Place
Ardmore, PA 19003
E: peter.goldberger@verizon.net

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h99-ay4q
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0039](#)

Comment from Tadeas Liska, NA

Submitter Information

Name: Tadeas Liska

Organization: NA

General Comment

As an employee of a somewhat virtual company this amendment is concerning due to its broad scope. We routinely use and access VPN's for data transfer and meeting sessions. Confidentiality and privacy of our business is a key component in our intellectual property landscape. While accessing these services from both home and workplace I do not wish to be identified as conducting "suspicious activity".

I understand that these networks are used for malicious intents as well, but please do not take the general stance that they are in and of themselves tools of malice.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9a-4gxu
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0040](#)

Comment from the U.S. Department of Justice

Submitter Information

Name: David Bitkower

Organization: N/A

General Comment

See Attached

Attachments

Rule 41 DOJ Memo 12 22 2014



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

December 22, 2014

MEMORANDUM

TO: The Honorable Reena Raggi
Chair, Advisory Committee on Criminal Rules

FROM: David Bitkower *DB*
Deputy Assistant Attorney General

SUBJECT: Response to Comments Concerning Proposed Amendment to Rule 41

The Committee has asked the Department to address certain issues raised by commenters who presented testimony at a public hearing on November 5, 2014, regarding the Department's proposed amendment to Rule 41. We thank the Committee for the opportunity to address these issues.

As we have stated previously, the proposed amendment would ensure that a court has jurisdiction to issue a search warrant in two categories of investigations involving modern Internet crime: cases involving botnets and cases involving Internet anonymizing techniques. The proposal would do so by clarifying Rule 41's current venue provisions in these two circumstances. The proposal would not authorize the government to undertake any search or seizure or use any remote search technique not already permitted under current law. Certain of the comments received by the Committee have contested this assertion, but as discussed below, many of those comments appear to be misreading the text of the proposal or misunderstanding current law. We welcome the opportunity to clarify how the proposal would operate as a matter of law and practice.

First, we address concerns that warrants authorizing remote searches would violate the Fourth Amendment's particularity requirement. As with all search warrant applications, such concerns must ultimately be resolved through judicial determination on a case-by-case basis. We nevertheless explain here why we believe that remote search warrants can satisfy the Particularity Clause. To illustrate, we describe three investigative scenarios in which warrants for remote searches might be used, and we provide specific language that might be used for the "place to be searched" and "things to be seized" components of remote search warrants in these scenarios.

Second, we address concerns about the notice requirement of the proposed rule. Like the Rule 41 requirement for physical searches, the proposed amendment 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.

Third, we explain that the proposed amendment has no effect on the requirements of Title III. 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.

Fourth, we discuss the “concealed through technological means” requirement for obtaining a warrant pursuant to the proposed venue provision for remote searches. This requirement provides an appropriate and workable standard for obtaining a warrant for a remote search in cases involving Internet anonymizing technology. The 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.

Fifth, we note that the 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, just as it is careful to avoid injury to persons or damage to property in the far more common scenario of executing physical warrants. Although there is currently no Department regulation that specifically applies to the remote searches that would be conducted under the proposed amendment, such searches are scrutinized carefully, and they may be subject to other internal Department regulations depending on the circumstances.¹

Before addressing the substance of the comments in detail, we note that the commenters’ objections regarding issues such as particularity and notice do not relate to venue. Rather, they are general objections to obtaining and executing search warrants using certain remote search techniques. These objections are misplaced here because the proposed amendment is solely about the appropriate venue for applying for such warrants. The existing rules already allow the government to obtain and execute such warrants when the district of the targeted computer is known. Thus, the issue before the Committee is not whether to allow warrants to be executed by remote search; it is whether such warrants should as a practical matter be precluded in cases involving anonymizing technology due to lack of a clearly authorized venue to consider warrant applications. Finally, we note that none of the commenters who expressed opposition to the proposal offered any substantive alternative solution to provide venue for a search warrant application when the district in which the targeted computer is located is unknown.

Particularity requirement for remote search warrants

We believe that search warrants authorizing remote searches can satisfy the Fourth Amendment’s particularity requirement. A number of magistrate judges have issued warrants for remote searches, and those judges have been satisfied that the warrants fulfilled the

¹ This letter does not address potential international issues associated with the proposed amendment, as those concerns were previously addressed by the Department in a letter dated October 20, 2014.

requirements of the Fourth Amendment.² As an initial matter, however, we note that the law regarding the particularity requirement for remote searches cannot be resolved by the Rules Committee; it must develop, as it does for all search warrants, through judicial resolution of specific, concrete cases. As the Committee Note to the proposed amendment states, “[t]he 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.”

Nevertheless, because several commenters raised concerns about the particularity of remote search warrants, we discuss how remote search warrants can satisfy the Fourth Amendment’s particularity requirement.³ In addition to discussing relevant doctrine regarding the Fourth Amendment’s particularity requirement, we will describe three investigative scenarios and explain how warrants can be drafted in those scenarios to satisfy the Fourth Amendment.

The particularity requirement of the Fourth Amendment demands that “warrants must particularly describe the things to be seized, as well as the place to be searched.” *Dalia v. United States*, 441 U.S. 238, 255 (1979) (internal quotation marks omitted); *see also United States v. Grubbs*, 547 U.S. 90, 97 (2006).⁴ The particularity requirement “makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another.” *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (quoting *Stanford v. Texas*, 379 U.S. 476 (1965)). “As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927).

Describing the information to be seized pursuant to a remote search warrant need not be complicated. The warrant specifies evidence of crime that can be obtained through access to the targeted computer. For warrants in investigations of crime involving use of Internet anonymizing technology, this evidence will usually be information that helps to identify the suspect. For example, the MAC address and IP address of a computer help identify the computer and its owner.

² For example, in one recent investigation, the government sought a search warrant to help identify computers used to access a child pornography hidden service on Tor. The magistrate judge issued a warrant for the search; in the subsequent criminal prosecution, the district court denied a motion to suppress challenging the warrant. *See United States v. Cottom*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #155) (denying suppression motion), (Doc #122, Attachment 1) (search warrant).

³ Commenters including the Center for Democracy and Technology (“CDT”) and the ACLU recommend that Congress address whether to authorize warrants for remote searches. *See* CDT Memorandum at 11; ACLU Memorandum at 28. This recommendation suggests that these commenters agree that such searches can, in principle, comply with the Fourth Amendment; otherwise any Congressional action would be futile.

⁴ The scope of the particularity requirement does not extend to describing how a warrant will be executed. The Supreme Court has explained that “[n]othing in the language of the Constitution or in this Court’s decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed.” *Grubbs*, 547 U.S. at 98 (quoting *Dalia*, 441 U.S. at 255).

Because the physical location of the place to be searched by remote access is typically unknown, remote search warrants usually describe the place to be searched through some other means designed to specify the particular account or computer that officers have probable cause to search. For example, when investigators have the ability to send an email to the suspect, the place to be searched could be described as the computer used to access and open the email sent to the suspect.

Some commenters argue that a search warrant can satisfy the Fourth Amendment's particularity requirement only if it specifies the physical location of the computer to be searched. This argument is mistaken: the Supreme Court has made clear that the particularity requirement does not preclude use of warrants where the purpose of the search is to discover the location of the place to be searched. In *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court held that a warrant for a tracking device could satisfy the Fourth Amendment despite the fact that the purpose of the warrant was to determine the place to be searched:

The Government contends that it would be impossible to describe the "place" to be searched, because the location of the place is precisely what is sought to be discovered through the search. . . . However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance.

Id. at 718. These same principles apply to warrants for remote searches. The government may satisfy the Fourth Amendment with respect to a remote search warrant by describing the computer or web server to be searched (for example, the computer that is used to access and open a particular email message, or the web server hosting a particular hidden web site), the circumstances that justify the search, the information that will be obtained through the search, and the time period during which the search may be conducted. None of these things require knowledge of the physical location of the object of the search.

The ACLU also objects that the "proposed amendment would allow police to remotely search many people's computers using a single warrant," *see* ACLU Memorandum at 21, but the law it cites regarding multi-location search warrants makes clear that such warrants may in fact comply with the Fourth Amendment. "A search warrant designating more than one person or place to be searched must contain sufficient probable cause to justify its issuance as to each person or place named therein." *Greenstreet v. County of San Bernardino*, 41 F.3d 1306, 1309 (9th Cir. 1994) (quoting *People v. Easley*, 671 P.2d 813, 820 (Cal. 1983)). Courts can address the extent to which this rule applies to remote search warrants in the usual manner, just as they would in the case of warrants for physical searches: through judicial resolution when the issue arises in specific cases. In any event, even if there were a rule requiring the use of a separate warrant for every location to be searched, the proposed amendment would not modify that rule. Rather, it merely provides a venue for a court to decide whether a warrant application satisfies the Fourth Amendment.

Particularity requirement: sample warrant language

To illustrate how remote search warrants can satisfy the Fourth Amendment, it is helpful to describe their use in several investigative scenarios. Here, we will discuss three scenarios: a drug trafficker using an email account offered through a Tor hidden service, a fraud scheme facilitated by email, and a child pornography group. For each, we will explain how two key elements of the warrant – the place to be searched and the items to be seized – can be drafted in compliance with the Fourth Amendment.

Warrant scenario 1: obtaining stored email content from a hidden email provider by using a username and password

It is worth noting at the outset that the proposal does not relate only to remote searches conducted through the use of special software or computer exploits. A warrant for a remote search under the proposed amendment could closely resemble a search warrant of the sort that is routinely issued by magistrate judges across the country. Suppose that in executing a Rule 41 warrant on the home of a drug trafficker, agents discover the user name and password for an email account hosted on a Tor hidden service that the target uses to advertise and sell drugs. Investigators would like to search the account for evidence, but they likely will not know the location of the server hosting the account, and they cannot serve the email provider with a standard email search warrant under 18 U.S.C. § 2703 as they would with a commercial service provider. Instead, investigators would like to access the email account themselves using the user name and password that they have discovered. Doing so will not require use of any special or otherwise sensitive software.

A warrant authorizing a search of the drug trafficker's email account will comply with the Fourth Amendment. First, the affidavit in support of the warrant can present facts sufficient to establish probable cause that the target has used the account in connection with his crimes and that there is reason to believe that the account will contain information related to that activity. Second, the search warrant will specify the place to be searched. For example, the warrant can state that the place to be searched is the "target account on the target computer," defined as "the account associated with [username] that is stored on the server hosting [the specified Tor email service]." The affidavit can also explain that investigators intend to log on to the account directly in order to execute the warrant. Third, the warrant will specify the information to be obtained from the account, such as particularly-described information that constitutes evidence of drug trafficking within a specified date range. Such a warrant will comply with the Fourth Amendment and would not present any novel particularity issues.

Warrant scenario 2: identifying a criminal using a web-based email account

Criminals frequently use web-based email accounts, such as Gmail, Yahoo, or Hotmail accounts, to send and receive communications related to their criminal activity. For example, a fraudster will want to use a seemingly "normal" email address to communicate with a potential victim. Investigators can typically determine the IP address that was used to access a web-based email account at a particular time by serving a subpoena on the email provider. But criminals can hide their true IP address from their service providers and the government through

anonymizing techniques such as use of a proxy server.⁵ In such circumstances, investigators may be able to use a Network Investigative Technique (“NIT”) to identify the criminal’s true IP address.

Suppose, for example, that investigators become aware that a fraudster is communicating with a victim through a web-based email account, and that the fraudster is trying to persuade the victim to wire him a large sum of money. In addition, investigators determine that the fraudster accesses his email account only using proxy servers. With the assistance of the victim, investigators can send an email containing a NIT from the victim’s email account to the fraudster’s email account. If the fraudster accesses the email, the NIT will cause the fraudster’s computer to send identifying information, such as the computer’s true IP address, to investigators.⁶

A warrant authorizing use of a NIT in such a manner can satisfy the Fourth Amendment. First, the affidavit in support of the warrant can present facts sufficient to establish probable cause that the fraudster is committing a crime, that he is using a computer to do so, and that the identity and location of the fraudster and the computer will constitute evidence. Second, the search warrant will specify what computer will be searched. For example, the warrant can state that the place to be searched is the “target computer,” defined as “the computer that accesses [the fraudster’s email account] and retrieves an email that will be sent to that account from [the victim’s email account] in furtherance of this warrant.” Third, the warrant will specify the information to be obtained from the computer. For example, the warrant could state that the information to be obtained is: “the target computer’s actual IP address, and the date and time that the NIT determines that IP address; and the target computer’s MAC address and host name.” This information would assist investigators in identifying the physical location and owner of the computer. Such a warrant will comply with the Fourth Amendment.

Warrant scenario 3: investigating members of a child pornography group

Many producers and traffickers of child pornography rely on Internet anonymizing techniques, in particular the Tor network, to hide from law enforcement. As an example, suppose that law enforcement becomes aware of a password-protected Tor website dedicated to the production, receipt, and distribution of child pornography. As explained on the publically-accessible part of the website and corroborated by an undercover agent’s attempt to access the site, an individual can only obtain a user account and password necessary to access the website by providing the site administrator with samples of newly created images of child pornography. Because of the strict rules governing access to the website, there is probable cause to believe that anyone who uses a password to access the site is engaged in the ongoing abuse of children and the production, distribution, and possession of child pornography. Investigators thus seek to

⁵ Frequently, criminals route their communications through proxy servers that openly advertise the fact that they do not maintain records.

⁶ This type of warrant is analogous to an anticipatory warrant to search the residence of a person who accepts a package containing contraband, even if the precise residence is not known at the time the warrant is obtained. *See, e.g., United States v. Dennis*, 115 F.3d 524, 528 (7th Cir. 1997) (anticipatory warrant to search whichever of two apartments belongs to the individual who accepts delivery or opens a particular package containing drugs).

identify the location of the individuals accessing the site. They intend to do so by sending a NIT to each computer used to log on to the website using a password during a specified time period. Each NIT will then send identifying information from each computer back to the investigators.

A warrant authorizing such searches can be written to comply with the Fourth Amendment. First, the affidavit in support of the warrant would set forth the facts described above, establishing probable cause that each computer used to access the website (or portion of the website) in question will contain evidence of a crime. Second, the search warrant authorizing the use of the NIT will specify the places to be searched. The warrant can state that the places to be searched are the “target computers,” which are “the computers used to log on to [the child pornography website] with a valid password during [specified time period] and to which a NIT will be sent pursuant to this warrant.” Third, the warrant will specify the information to be obtained. For example, the warrant can state that the information to be obtained is: “for each target computer, the actual IP address, and the date and time that the NIT determines that IP address; and the target computer’s MAC address and host name.”

The ACLU calls this technique a “watering hole attack” and suggests that it may violate the Fourth Amendment. *See* ACLU Memorandum at 22. The Department disagrees both with that label and with the legal conclusion.⁷ As discussed above, when investigators can establish probable cause to search multiple locations, the Fourth Amendment allows investigators to obtain a warrant to search them. *See, e.g., United States v. Johnson*, 26 F.3d 669, 692 (7th Cir. 1994); *Greenstreet*, 41 F.3d at 1309. And by the same token, if investigators cannot establish probable cause to search a particular location, then they will not be able to obtain a warrant to authorize the search of that location. Nothing in the proposed amendment would hold otherwise.

As these three hypothetical scenarios demonstrate, warrants executed by remote search can satisfy the Fourth Amendment. We do not doubt that one could also conjure up hypothetical instances in which a remote warrant would *not* satisfy the Fourth Amendment. But that is beside the point because the proposed amendment would not authorize such searches. What the proposed amendment would do is ensure that a court is available to determine whether a specific warrant application satisfies the Fourth Amendment or not.

Notice requirement for remote search warrants

The proposed amendment’s notice requirement mandates that when executing a warrant for a remote search, “the officer must make reasonable efforts to serve a copy of the warrant on the person whose property was searched or whose information was seized or copied,” and that

⁷ The term “watering hole” attack is generally used to describe a technique whereby criminal hackers implant a virus on a widely-used website and cause it to infect large numbers of users who may not be of interest to the hackers, in hopes that the virus will also infect a smaller number of users who are of specific interest to the hackers. *See, e.g.,* <http://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-hole-sites>. By contrast, the search described in this scenario is – and by definition must be – targeted based on probable cause. The ACLU also asserts in its comment that the FBI performed such a “watering hole attack” on a particular Tor-based server known as Freedom Hosting that “forc[ed] all of the Freedom Hosting sites to deliver malware to visitors, not just those sites that were engaged in the distribution of illegal content.” ACLU Memorandum at 15. This assertion appears to be based on Internet rumor.

“[s]ervice may be accomplished by any means, including electronic means, reasonably calculated to reach that person.” Commenter EPIC asserts that this amendment authorizes surreptitious searches without a showing of need for the delay, *see* EPIC Memorandum at 7, but EPIC is misreading the proposed rule. The proposed amendment, as a default matter, requires officers to make reasonable efforts to give notice of the warrant at the time the warrant is executed.

The proposed amendment does not modify the delayed-notice statute. If investigators seek to delay notice of a warrant executed by remote search, they will be required to follow the existing delayed-notice procedures and meet the existing delayed-notice standard of 18 U.S.C. § 3103a. Under that statute, in order to authorize delayed notice, the issuing court must find “reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial).” 18 U.S.C. § 3103a(b)(1). This standard will be the same for remote searches as it is for physical searches. In addition, a court cannot authorize the seizure of either physical evidence or electronic information pursuant to a delayed-notice warrant without a judicial finding of reasonable necessity. *See* 18 U.S.C. § 3103a(b)(2) (requiring that a delayed-notice warrant must prohibit “the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure”). Again, this provision treats “stored wire or electronic information” that will be obtained by a remote search in precisely the same manner as “any tangible property.” The Department has interpreted “seizure . . . of any stored wire or electronic information” in Section 3103a(b)(2) broadly to include the copying of information stored on a computer. Finally, unless a longer period of delay is justified by the facts of the case, Section 3103a will allow for an initial 30-day period of delayed notice for a remote search warrant, with possible extensions of up to 90 days each. *See* 18 U.S.C. § 3103a(b), (c).⁸

The Department anticipates that it will seek judicial approval to delay notice in many of the cases in which it seeks a warrant for a remote search. This is so because, as described above, such warrants will often be sought when investigators are trying to identify or locate an online criminal who is taking steps to avoid identification. Such circumstances will typically provide reasonable cause for delaying notice of the search, but notice will be delayed only where appropriate under existing rules. For example, in *United States v. Cottom*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #155) (denying motion to suppress), investigators invoked Section 3103a to delay notice of a remote search warrant through which they identified users of a Tor-based hidden service child pornography website. The court held that “the 30-day delayed notice, under the facts of this case, did not create any violation of Rule 41.” *Id.* at 8.

⁸ Under the proposed amendment, the rules for delaying notice for warrants for remote searches will be more demanding than the existing rules for delaying notice for tracking device warrants. For a tracking warrant, the government need not provide notice of the warrant for up to ten days after the tracking has ended, and no showing of need is required for that initial period of delay. *See* Fed. R. Crim. P. 41(f)(2)(C). Because tracking warrants can last for 45 days, *see* Fed. R. Crim. P. 41(e)(2)(C), notice of a tracking warrant can therefore be given 55 days after the initial search without any showing of need for the delay.

The proposed amendment requires officers to make “reasonable efforts” to provide notice of a warrant. This standard recognizes that in some cases – particularly cases in which the location of the computer has been concealed – the officer may be unable to provide notice of the warrant. For example, even after officers conduct a remote search, they may still lack sufficient information to identify or contact the owner of the searched computer. The “reasonable efforts” language recognizes that there may be unusual difficulty in providing appropriate notice in cases where the district in which the computer is located is unknown; by contrast, if the government can provide notice using reasonable efforts, the rule will require it to do so. As the Supreme Court stated in *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995), “[t]he Fourth Amendment’s flexible requirement of reasonableness should not be read to mandate a rigid rule of announcement that ignores countervailing law enforcement interests.” As with other notice issues under the Fourth Amendment, the reasonableness of the government’s efforts to provide notice must be evaluated on a case-by-case basis.

Finally, the proposed amendment requires that a copy of the warrant be served on “the person whose property was searched or whose information was seized or copied” (emphasis added). This approach is consistent with Rule 41’s existing requirements for both standard search warrants and for tracking device warrants. See Fed. R. Crim. P. 41(f)(1)(C), (f)(2)(C); *United States v. Zacher*, 465 F.3d 336, 339 (8th Cir. 2006) (warrant for FedEx package). When the government executes a Rule 41 warrant in the physical world, it is not obliged to provide notice to everyone with a potential privacy interest in the place searched. For example, if the search of a house includes the search of a locked trunk stored at the house by a friend of the house’s owner, law enforcement has never been required to seek out and give notice of the warrant to the owner of the trunk. Similarly, if investigators execute a remote search warrant on a computer used to access a specified email account, and the computer turns out to belong to the suspect’s friend, the government should be able to satisfy its notice obligation – as it would in the physical world – by providing notice to the friend.

Interaction between the proposed amendment and Title III

The proposed amendment to Rule 41 would not affect law enforcement’s obligations to comply with the Wiretap Act, 18 U.S.C. §§ 2510-2522 (“Title III”). Title III generally requires a wiretap order to intercept⁹ wire, oral, or electronic communications, unless one of several statutory exceptions apply. See 18 U.S.C. § 2511. A Rule 41 search warrant does not permit law enforcement to intercept such communications, and nothing in the proposed amendment suggests otherwise. Thus, the ACLU is mistaken to assert that the proposed amendment “authorizes searches that can only be carried out pursuant to a Title III wiretap order.” ACLU Memorandum at 18. For example, if investigators sought an order to intercept wire, oral or electronic communications, they would have to proceed by Title III rather than Rule 41 (or in addition to Rule 41, if stored information was sought as well).

⁹ The Wiretap Act defines “intercept” to mean the “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). Communications are intercepted within the meaning of Title III when they are acquired contemporaneously with transmission. See, e.g., *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 460-63 (5th Cir. 1994).

Concealed through technological means

Under the proposed amendment, a magistrate judge in a district where activities related to a crime may have occurred will have authority to issue a warrant for a remote search if the location of the computer to be searched “has been concealed through technological means.” This “concealed through technological means” requirement provides an appropriate standard for obtaining warrants for remote searches. An officer seeking a warrant for a remote search can satisfy this component of the court’s jurisdiction to issue the warrant through an affirmative factual showing regarding the criminal’s conduct – for example, the criminal’s use of Tor to distribute child pornography. Alternative formulations of the proposed amendment, such as a requirement that the location of the computer to be searched be unknown, would likely lead to excessive *Franks* hearings on whether agents had disclosed every fact that might have suggested a possible location of the criminal’s computer; such formulations could also draw courts into determinations of whether investigators had taken appropriate steps to determine the location of the computer to be searched. In its current form, the proposed amendment provides a workable and reasonable standard for obtaining warrants for remote searches that is less likely to result in excessive litigation.

Commenter Center for Democracy and Technology (“CDT”) argues that the “concealed through technological means” standard is overly broad, *see* CDT Memorandum at 6, but its argument is based on a misunderstanding of the requirements for obtaining a criminal search warrant. CDT states that “[I]legitimate uses of technology that have the effect of ‘concealing through technological means’ a user’s location . . . should not trigger the ability for a judge to issue a Rule 41 warrant.” *Id.* at 7. Under the proposed amendment, however, investigators could not obtain a search warrant merely because a user’s location is concealed through technological means. Rather, the warrant application must also demonstrate probable cause that the search will uncover evidence, fruits, or instrumentalities of crime. *See* Fed. R. Crim. P. 41(c). The proposed amendment does not alter that rule, but instead provides an alternative means of satisfying Rule 41’s venue provisions. Standing alone, the use of Internet anonymizing techniques to conceal location does not provide a basis for obtaining a search warrant.¹⁰

Avoiding collateral damage and internal Department of Justice policies

Some commenters raised concerns about the possibility that the Department’s use of remote searches could damage a targeted computer or other computer systems. The Department is mindful of the impact that remote search software has on computers, and we are careful in our use of remote searches, just as we are careful to avoid injury to persons or damage to property in the far more common scenario of executing physical search warrants. In our efforts to date, we have balanced risks involved in technical measures against the importance of the objectives of an investigation in stopping crime and protecting public safety, and we have considered the

¹⁰ CDT is also concerned that a warrant could be issued when a user conceals location through a means that is “not technically technical,” such as misreporting of the city of residence in a Facebook profile. CDT Memorandum at 7. The language of the proposed amendment, however, requires that the location of the relevant “media or information” be concealed through “technological means.” It is unclear to us how misrepresenting one’s city of residence on Facebook would conceal the location of media or information subject to search in the first place, much less through technological means.

availability and risks of potential alternative investigative avenues. As a result of this caution, although remote searches are relatively uncommon, the searches we have undertaken have not resulted in the types of collateral damage that the commenters hypothesize. Such careful consideration of any future technical measures will continue.

Similarly, the successes of the Department's anti-botnet initiatives demonstrate that our efforts in the cyber realm can bring substantial benefits while avoiding collateral damage to victims. The Department, often in collaboration with public and private sector partners, has conducted technical operations pursuant to court authorization to disrupt and dismantle several botnets infecting computers of innocent users, including the Coreflood¹¹ and Gameover Zeus¹² botnets. The results of these operations demonstrate that our technical efforts have resulted in substantial benefits for computer users victimized by online crime, rather than any undue collateral damage.

Currently, the remote searches that would be applied for under the amended rule are not subject to mandatory internal regulation at the Department. However, remote searches may implicate other existing Departmental guidelines and regulations depending on the circumstances. Additionally, the FBI is required to adhere to the Attorney General's Guidelines for Domestic FBI Operations ("AGG-DOM") and the FBI's Domestic Investigations and Operations Guide ("DIOG") in conducting remote searches, and those guidelines require that the FBI use the least intrusive method available in conducting a search.¹³ Section I(C)(2)(a) of the AGG-DOM provides:

The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of different investigative methods that are each operationally sound and effective, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and potential damage to reputation. The least intrusive method feasible is to be used in such situations. It is recognized,

¹¹ In Operation Coreflood, the FBI worked with private sector and law enforcement partners to disable a botnet that had infected an estimated two million computers with malicious software. The malware on the Coreflood botnet allowed infected computers to be controlled remotely by criminals to steal private personal and financial information from unsuspecting users. The FBI obtained a court order to seize domain names, re-route the botnet to FBI-controlled servers, and stop the Coreflood software from running.

¹² Gameover Zeus, believed to have infected approximately 500,000 to one million computers worldwide and to have caused losses of over \$100 million, is an extremely sophisticated type of malware designed to steal banking and other credentials from the computers it infects. Those credentials are then used to initiate or redirect wire transfers to accounts overseas. The government obtained civil and criminal court orders in federal court in Pittsburgh authorizing measures to sever communications between the infected computers and criminal servers, and redirect them from the criminal servers to substitute servers under the government's control.

¹³ Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM), Sec. I(C)(2)(a); Domestic Investigations and Operations Guide (DIOG), Sec. 18.2.

however, that the choice of methods is a matter of judgment. The FBI shall not hesitate to use any lawful method consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of foreign intelligence sought to the United States' interests. This point is to be particularly observed in investigations relating to terrorism.

Likewise, Section 18.2 of the DIOG provides, "The AGG-DOM requires that the 'least intrusive' means or method be considered and—if reasonable based upon the circumstances of the investigation—used to obtain intelligence or evidence in lieu of more intrusive methods." The DIOG also contains a section providing extensive and detailed guidance on making least intrusive method determinations.¹⁴ Although the least intrusive methods requirement is primarily designed to address privacy and civil liberties concerns, its principles apply to avoiding collateral damage in remote searches as well and inform, among other things, the way in which a NIT is designed (so as to minimize the likelihood of damage), its capabilities, and the manner in which it is used.

Most remote searches are unlikely to have any significant lasting effect on the integrity of a targeted computer. In any case, as the Supreme Court has recognized, "the details of how best to proceed with the performance of a search authorized by warrant" are "generally left to the discretion of the executing officers." *Dalia*, 441 U.S. at 257. Subsequently, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Id.* at 258. This same standard would apply to any damage caused by officers executing a warrant by remote search. In addition, as with all investigative techniques, the Department will scrutinize the use of NITs, and the Department may in the future choose to impose additional regulations on their use.

- - -

We appreciate the opportunity to respond to issues raised by commenters on the proposed amendment to Rule 41. We look forward to further discussions with the Committee. Please let us know if there are other issues or concerns which you would like the Department to address.

¹⁴ DIOG § 4.4. The section includes subsections entitled, "General Approach to Least Intrusive Method Concept," Section 4.4.2; "Determining Intrusiveness," Section 4.4.3; and "Standard for Balancing Intrusion and Investigative Requirements," Section 4.4.4.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9a-84to
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0041](#)

Comment from Martin MacKerel, NA

Submitter Information

Name: Martin MacKerel

Organization: NA

General Comment

I concur with the point of view in the following article:

<https://cdt.org/blog/us-doj-seeks-to-search-and-seize-data-on-computers-worldwide/>

These changes are a dramatic extension of existing law enforcement powers and should be subject to robust public debate in the appropriate legislative forum.

They should **not** be the subject of an administrative rule change, and therefore I ask that these proposed amendments be rejected.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9c-vf7b
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0042](#)

Comment from Timothy Doughty, NA

Submitter Information

Name: Timothy Doughty

Organization: NA

General Comment

This is the digital equivalent of "your front door is locked, therefore, you're under suspicion of being a criminal!". VPNs are used the world over for various purposes. Last time I checked, we have a decently sized tech sector. You do realize that many of those employees who work from home do so while using a VPN? Please think before creating idiotic laws that will drive the tech companies out of this country and cost people who are unable to commute or move their jobs.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9c-q14j
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0043](#)

Comment from Stephen Argent, NA

Submitter Information

Name: Stephen Argent

Organization: NA

General Comment

Absolutely ludicrous changes are being proposed here. The fact that so many businesses rely on VPN's for encrypted communication to protect trade secrets, or journalists using Tor to protect their identities whilst abroad. This change is an unconstitutional overreaching that far exceeds any reasonable approach to this issue.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9d-8c1e
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0044](#)

Comment from Weymar Osborne, NA

Submitter Information

Name: Weymar Osborne

Organization: NA

General Comment

Using a VPN or some other way is not a sufficient reason to authorize the warrant. This is the Federal Government trying to allow itself to hack into any computer of a person who are simply trying to prevent others from accessing information that gets sent over their own network. A person having their curtains pulled in their house to give themselves some privacy is not enough to justify a search. Doing the same on a computer should not be either.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9d-4gra
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0045](#)

Comment from Anonymous Anonymous, NA

Submitter Information

Name: Anonymous Anonymous

Organization: NA

General Comment

I am writing to firmly oppose this proposed amendment. The 4th amendment is very clear in protecting against unreasonable searches and outlawing general warrants. This proposed amendment violates both of those clauses. This is the digital version of allowing warrants to be issued based upon the fact somebody has a dead bolt on the front door. Just because a lock, or encryption, is in use does not justify probable cause under the 4th amendment.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9d-tuhe
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0046](#)

Comment from Ryan Hodin, NA

Submitter Information

Name: Ryan Hodin

Organization: NA

General Comment

I respectfully, but firmly, oppose this alteration. The United States government has funded research into, and supported the use of, TOR and VPNs. Both have many legitimate and wholly legal uses: Their use does not constitute an illegal act, and nor should it, and their presence does not in any way constitute "probable cause" as required by US law. This is similar to owning a bicycle: There are many legitimate uses of a bicycle, and many illegal uses of a bicycle, but the latter does not justify their being used to justify search warrants. Thus, it is my firm position that this section of the proposal should be removed.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9e-qhvx
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0047](#)

Comment from Hannah Bloch-Wehba, Reporters Committee for Freedom of the Press

Submitter Information

Name: Hannah Bloch-Wehba

Organization: Reporters Committee for Freedom of the Press

General Comment

See attached.

Attachments

RCFP Comment on Rule 41

February 17, 2015

1156 15th St. NW, Suite 1250
Washington, D.C. 20005
(202) 795-9300
www.rcfp.org

Bruce D. Brown
Executive Director
bbrown@rcfp.org (202) 795-9301

STEERING COMMITTEE

STEPHEN J. ADLER
Reuters

SCOTT APPLEWHITE
The Associated Press

WOLF BLITZER
CNN

DAVID BOARDMAN
Temple University

CHIP BOK
Creators Syndicate

JAN CRAWFORD
CBS News

MICHAEL DUFFY
Time

RICHARD S. DUNHAM
Tsinghua University, Beijing

ASHLEA EBELING
Forbes Magazine

SUSAN GOLDBERG
National Geographic

FRED GRAHAM
Founding Member

JOHN C. HENRY
Freelance

NAT HENTOFF
United Media Newspaper Syndicate

JEFF LEEN
The Washington Post

DAHLIA LITHWICK
Slate

TONY MAURO
National Law Journal

JANE MAYER
The New Yorker

DAVID McCUMBER
Hearst Newspapers

JOHN McKINNON
The Wall Street Journal

DOYLE MCMANUS
Los Angeles Times

ANDREA MITCHELL
NBC News

MAGGIE MULVIHILL
Boston University

SCOTT MONTGOMERY
NPR

BILL NICHOLS
Politico

JEFFREY ROSEN
The National Constitution Center

CAROL ROSENBERG
The Miami Herald

THOMAS C. RUBIN
Seattle, Wash.

ERIC SCHMITT
The New York Times

ALICIA SHEPARD
Freelance

MARGARET LOW SMITH
The Atlantic

JENNIFER SONDAG
Bloomberg News

PAUL STEIGER
Pro Publica

PIERRE THOMAS
ABC News

SAUNDRA TORRY
USA Today

JUDY WOODRUFF
PBS/The NewsHour

Members of the Advisory Committee on Criminal Rules

Re: Comment of the Reporters Committee for Freedom of the Press on the Proposed Amendment to Federal Rule of Criminal Procedure 41 Concerning “Remote Access” Searches of Electronic Storage Media and Electronic Information

The Reporters Committee for Freedom of the Press (“Reporters Committee”) appreciates this opportunity to comment on the proposed amendment to Rule 41 of the Federal Rules of Criminal Procedure concerning “remote access” searches of computers and other electronic devices. The amendment was proposed by the Department of Justice and modified by the Committee in April 2014.¹

The Reporters Committee is a voluntary, unincorporated association of reporters and editors dedicated to safeguarding the First Amendment rights and freedom of information interests of the news media and the public. The Reporters Committee has provided assistance, guidance, and research in First Amendment and freedom of information litigation since 1970. The Reporters Committee frequently represents the interests of the press and the public before Article III courts. The Reporters Committee is concerned that the proposed amendment to Rule 41 would intrude on vital constitutional and statutory rights protecting the news media and the free press.

If amended as proposed, Rule 41 would permit a court in a district where activities related to a crime have occurred to issue a warrant authorizing remote access searches of electronic storage media and electronic information located within or outside that district.² Under the proposed amended Rule 41, magistrates would be able to exercise this power:

- i. When the physical location of the media or information is “concealed through technological means,” or
- ii. In an investigation of 18 U.S.C. 1030(a)(5), when the damaged protected computers are located in five or more districts.³

The proposed amendment presents significant legal and policy issues for journalists and their sources. In particular, the Reporters Committee is

¹ See generally Advisory Comm. on Criminal Rules, Materials for April 7–8, 2014 Meeting 155–266 (“Advisory Comm. Materials”) (April 7-8, 2014), available at <http://1.usa.gov/1o8ocLf>.

² See, e.g., *Memo to Members*, Advisory Comm. Materials at 155.

³ Under 18 U.S.C. § 1030(e), the term “damage” means “any impairment to the integrity or availability of data, a program, a system, or information,” and the term “protected computer” means any computer “which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States.”

concerned about the vague definition of remote access, which could reveal sensitive journalist-source communications; language such as “concealed through technological means,” which may lead to the potential targeting of journalists who use anonymization tools in connection with newsgathering, including to protect their communications with sources; and the absence of language that would prevent law enforcement from impersonating the news media when it seeks to carry out remote access searches.

Of particular concern is the inability of law enforcement officials to know, before applying for a warrant under the proposed amendment to Rule 41, whether the computer or electronic storage medium that is the target of a search belongs to a journalist using an anonymization tool in connection with newsgathering. Computers and electronic storage devices such as hard drives, cell phones, and cloud storage are integral to the modern journalistic profession. As the Supreme Court has recognized, digital devices such as cell phones “are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form.”⁴ Searching electronic storage devices for evidence of a crime is akin to simultaneously rifling through a journalist’s “cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.”⁵

Indeed, any search of a journalist’s computer or other electronic devices implicates the Privacy Protection Act of 1980 (“PPA”), which prohibits searches and seizures of work product and documentary materials held by a person with “a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication,” with a few expressly enumerated, and very narrow, exceptions.⁶ Searches of reporters’ electronic devices also implicate the First Amendment rights of the press.

Rule 41 may “not modify any statute regulating search or seizure.”⁷ As a practical matter, however, the proposed amendment to the Rule places journalists’ statutory and constitutional rights at risk by sanctioning the remote access of electronic devices to search for evidence of a crime without requiring that any determination be made prior to such a search as to whether the targeted devices are being used for newsgathering. To be in accord with the PPA and the First Amendment, any amendment to Rule 41 that is intended to allow for remote access searches by law enforcement must ensure that such searches will not compromise the work product and communications of journalists who may use anonymization tools in connection with newsgathering, including to protect the identities of and their communications with confidential sources.

As the Committee considers this amendment, it must take into account that the language and vagueness of the proposed Rule creates serious, far-reaching threats to the constitutional, common law, and statutory rights that protect journalists and media in the

⁴ *Riley v. California*, 134 S. Ct. 2473, 2490.

⁵ *Id.* at 2496–97 (Alito, J., concurring).

⁶ 42 U.S.C. § 2000aa.

⁷ Fed. R. Crim. P. 41(a).

United States. Indeed, because the proposed amendment to Rule 41 would substantially abridge and modify essential rights under the PPA and the First Amendment, these issues are beyond the scope of the Federal Rules of Procedure, and any potential changes should be addressed by Congress.⁸ We urge the Committee to reject the proposed amendment to Rule 41 in full.

I. The proposed amendment to Rule 41 offers insufficient safeguards for newsgathering and other First Amendment-protected activity.

Remote-access searches of journalists' computers can reveal a variety of confidential information, including lists of contacts, work product, and reporter-source communications. While the Constitution, common law, and statute protect against needless searches targeting the news media, the proposed amendment to Rule 41 would allow the government to circumvent those restrictions when it comes to journalists employing anonymization tools to protect their own privacy and that of their sources.

A. The First and Fourth Amendments and the PPA protect journalists against searches of their communications and work product.

The Fourth Amendment prohibition on unreasonable searches of “persons, houses, papers, and effects” arose from a long list of abusive practices in the colonial era, many of which targeted printers and publishers of dissenting publications.⁹ As a result, the Fourth Amendment’s roots are intertwined with the First Amendment’s guarantees of free speech and a free press. Indeed, the history of the Fourth Amendment is “largely a history of conflict between the Crown and the press.”¹⁰

Because of the historic link between the First and Fourth Amendments, the Supreme Court found in *Zurcher v. Stanford Daily* that where materials to be searched or seized “*may be protected by the First Amendment*, the requirements of the Fourth Amendment must be applied with ‘scrupulous exactitude.’”¹¹ The Fourth Amendment case law relied upon in *Stanford Daily* also calls for “consideration of First Amendment values in issuing search warrants.”¹² The Government has proposed that the amended Rule “does not address any constitutional questions” regarding whether a given search is constitutional under the Fourth Amendment.¹³ However, neither the Government nor the Committee have addressed the difficulty of considering First Amendment values in the context of a remote access search, as *Stanford Daily* makes clear is mandated by the Constitution.

⁸ See *Sibbach v. Wilson & Co.*, 312 U.S. 1, 10 (1941).

⁹ U.S. Const. amend. IV; see also, e.g., *Entick v. Carrington*, 19 How. St. Tr. 1029 (1765) (dismissing a general warrant against a dissenting printer); *Wilkes v. Wood*, 19 How. St. Tr. 1153 (1763) (same).

¹⁰ *Stanford v. Texas*, 379 U.S. 476, 482 (1965).

¹¹ *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1979) (emphasis added).

¹² *Id.* at 565.

¹³ Advisory Comm. Materials at 158.

Remote access searches of journalists' computers and electronic storage media raise statutory questions as well. The proposed amendment to Rule 41 would permit law enforcement to obtain a remote access warrant to search for evidence of crime. With quite limited exceptions, the PPA bars such searches when the documents to be searched for or seized are related to newsgathering.¹⁴ The PPA was enacted in response to *Stanford Daily*, in which the Supreme Court ruled that the Fourth Amendment's requirements of probable cause, particularity, and reasonableness "should afford sufficient protection against the harms that are assertedly threatened by warrants for searching newspaper offices."¹⁵ Congress disagreed that Fourth Amendment safeguards were sufficient to protect First Amendment activity. Recognizing the "threat that *Stanford Daily* poses to the vigorous exercise of First Amendment rights," Congress prohibited searches for "work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication."¹⁶ Congress also barred searches for "documentary materials" possessed for the same purpose.¹⁷

The PPA "affords the press and certain other persons not suspected of committing a crime with protections not provided currently by the Fourth Amendment."¹⁸ Thus, it protects journalists who may possess evidence of a crime, but who are not themselves suspected of criminal activity. The proposed amendment to Rule 41 contravenes these protections insofar as it would permit "remote access searches" for work product or documentary materials without any investigation into or determination as to whether those materials are possessed in connection with a purpose to publish or communicate.¹⁹ Those searches could reveal the identities of journalists' confidential sources and the contents of sensitive reporter-source communications, among other newsgathering material, and thus interfere with the flow of information to the public.

B. Remote access searches can unmask reporters' confidential sources and communications.

Many significant pieces of American journalism have relied heavily on confidential sources. The *New York Times* used such contacts to break the story that the NSA had an illegal wiretapping program that monitored phone calls and email messages

¹⁴ 42 U.S.C. § 2000aa; see also *Guest v. Leis*, 255 F.3d 325, 340 (6th Cir. 2001). The statutory definition of "documentary materials" is "materials upon which information is recorded," and "includes, but is not limited to, written or printed materials, photographs, motion picture films, negatives, video tapes, audio tapes, and other mechanically, magnetically, or electronically recorded cards, tapes, or discs."

¹⁵ *Stanford Daily*, 436 U.S. at 565.

¹⁶ 42 U.S.C. § 2000aa(a).

¹⁷ 42 U.S.C. § 2000aa(b).

¹⁸ S. Rep. No. 96-874, at 4 (1980).

¹⁹ The PPA requires a "reasonable investigation" of an entity before a search in order to ensure that the entity does not possess the sought-after materials in connection with a purpose to distribute a communication to the public. See, e.g., *Steve Jackson Games, Inc. v. Secret Service*, 816 F. Supp. 432, 440-41 (W.D. Tex. 1993) (finding the Secret Service liable for PPA violations in part because it failed to "make a reasonable investigation" of a publisher before it seized the publisher's work product).

involving suspected terrorist operatives without the approval of federal courts.²⁰ The *Times* also used confidential sources to report on the waterboarding and other so-called “enhanced interrogation techniques” that terrorism suspects in U.S. custody have faced.²¹ The *Washington Post* relied on confidential government sources, among others, to break the story of the Central Intelligence Agency’s use of “black sites,” a network of secret prisons for terrorism suspects.²² The identities of confidential sources like these could be easily obtained and revealed if law enforcement uses remote access to search a journalist’s device.

The proposed amendment to Rule 41 offers no protections for these confidential documents and communications. By broadening federal law enforcement’s ability to search journalists’ work product, communications, and contacts remotely, without probable cause to suspect them of a crime, the proposed amendment to Rule 41 would significantly chill reporter-source communications, contrary to the public interest in government accountability. As the Supreme Court has recognized, “Awareness that the Government may be watching chills associational and expressive freedoms.”²³ In other contexts, journalists have reported that the knowledge of call metadata monitoring has made sources unwilling to speak to them, even on unclassified matters.²⁴ And elsewhere, the use of remote monitoring of reporters’ satellite phones may have put those reporters’ lives at risk.²⁵ If anonymization tools placed reporters at greater risk of being targeted by law enforcement, reporter-source communications would suffer, impeding newsgathering as a result.

Under the proposed amendment to Rule 41, those journalists who are adopting new encryption and anonymization technologies in order to safeguard their sources and materials are at particular risk. Journalists routinely use anonymization tools to safeguard their sources and communications. Encryption helps journalists protect the content of their communications by scrambling the information in a way that only allows intended recipients to read it. Journalists can use encryption to prevent outside parties from reading or listening to a variety of digital communications by encrypting Internet traffic

²⁰ See, e.g., James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005), available at <http://nyti.ms/neIMIB>.

²¹ See, e.g., Scott Shane, David Johnston, James Risen, *Secret U.S. Endorsement of Severe Interrogations*, N.Y. Times (Oct. 4, 2007), available at <http://nyti.ms/1dkyMgF>.

²² See, e.g., Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, Wash. Post (Nov. 2, 2005), available at <http://wapo.st/Ud8UD>.

²³ *United States v. Jones*, 132 S.Ct. 945, 956, 565 U.S. ___, __ (2012) (slip op., at 3) (Sotomayor, J., concurring).

²⁴ In a report that former *Washington Post* executive editor Leonard Downie Jr. wrote for the Committee to Protect Journalists, numerous journalists said surveillance programs and leak prosecutions deter sources from speaking to them. Comm. To Protect Journalists, *The Obama Administration and the Press: Leak investigations and surveillance in post-9/11 America* 3, Oct. 10, 2013, <http://bit.ly/1c3Cnfg>; see also *With Liberty to Monitor All: How Large-Scale Surveillance is Harming Journalism, Law and American Democracy* 25, Human Rights Watch (July 2014), <http://bit.ly/1uz3CL1>.

²⁵ See, e.g., Rod Nordland and Alan Cowell, *Two Western Journalists Killed in Syria Shelling*, N.Y. Times (Feb. 22, 2012), available at <http://nyti.ms/19leEe6> (reporting that journalists killed in Syria may have been targeted by government forces who traced their satellite phones).

and stored data. Sophisticated systems can even mask who is communicating with whom, or that any communication took place at all. Reporters use encryption to protect themselves, their sources, and the newsgathering process. These practices are likely to become increasingly prevalent as journalists become more aware of the threats insecure communications pose to their sources, communications, and work product.

To protect metadata—the data about data, including when and with whom a person is communicating—journalists need to use anonymity tools that hide the location and identity of the sender of a communication. One such tool, Tor, also protects communications and sources from passive Internet surveillance known as “traffic analysis” which can allow an outsider to ascertain who is talking to whom and thereby track interests and behavior.²⁶ Tor protects journalists from this surveillance by distributing journalists’ transactions over several places on the Internet, so no single point can link the journalist to his or her destination.

Indeed, while remote access searches pose serious dangers to the confidentiality of reporter-source communications and to journalists’ security, the proposed amendment to Rule 41 includes no protections whatsoever for journalists, reporters, or other non-suspects who are engaged in First Amendment activity. The Reporters Committee urges the Committee to consider these important First Amendment values and reject the proposed amendment to the Rule.

The proposed amendment to Rule 41 would allow a judge to issue a warrant authorizing law enforcement “to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district.”²⁷ The proposed amendment and the proposed committee note do not define “remote access,” although Department of Justice submissions to the Subcommittee on Rule 41 provide some explanation.²⁸

Remote access searches could reveal the identities of sources and the contents of reporter-source communications in myriad ways. First, remote access searches can reveal a substantial amount of sensitive information on a person’s electronic device, including contacts and geo-location information, a computer’s MAC address, operating system, registered user of the operating system, and the address of the last website visited in the user’s web browser, among other information.²⁹ This technology can also be used to remotely control communication devices such as webcams and microphones.³⁰

The scope or extent of any remote access search involving the installation of malware could also make reporters’ communications, contacts, and work product

²⁶ See, e.g., Tor: Overview, <https://www.torproject.org/about/overview.html.en>.

²⁷ See, e.g., Proposed Amendments Materials at 338.

²⁸ See generally Advisory Comm. Materials at 179–235.

²⁹ See, e.g., Kevin Poulson, *FBI’s Secret Spyware Tracks Down Teen Who Made Bomb Threats*, *Wired* (July 18, 2007), available at <http://wrd.cm/1v12K2D>

³⁰ See e.g., Craig Timberg and Ellen Nakashima, *FBI’s search for ‘Mo,’ suspect in bomb threats, highlights use of malware for surveillance*, *Wash. Post* (Dec 6, 2013), available at <http://wapo.st/1gdutVf>.

susceptible to ongoing vulnerabilities. Since at least the early 2000s, federal law enforcement agencies have used sophisticated surveillance software in national security and criminal investigations to remotely access targeted computers.³¹ Yet security flaws have been repeatedly discovered in popular interception and surveillance tools, leading to vulnerabilities that can be exploited by other adversaries.³² In addition, once malware is released into the “wild” (i.e. where it is able to infect computers) it can be difficult to contain. It can collect information in an ongoing manner and outside the scope of the original purpose.³³ Security flaws such as these can put reporters and their sources at risk.³⁴

C. The proposed amendment offers no protection to journalists who use anonymization tools to protect communications with and identities of sources

If the proposed amendment is adopted, a warrant could be issued to remotely search and seize or copy electronic media outside the district when the physical location of the media or information is “concealed through technological means.” The Reporters Committee is concerned that this language, if adopted, will affect journalists who use encryption³⁵ and anonymity tools³⁶ to improve their own security and privacy and that of their sources.

The use of anonymization tools such as Tor has become a best practice for reporters to safeguard the confidentiality of their work product, communications, and sources. Prestigious journalism schools like Columbia University’s Graduate School of Journalism and its Tow Center for Digital Journalism have conducted research into digital security practices for journalists, including how best to systematically integrate

³¹ See e.g., Reuters, *FBI Sheds Light on 'Magic Lantern' PC Virus*, Reuters, (Dec. 13, 2001) available at <http://usat.ly/1DCnsYg>.

³² See, e.g., Craig Timberg, *German researchers discover a flaw that could let anyone listen to your cell calls*, Wash. Post (Dec. 18, 2014), available at <http://wapo.st/1AkQ7zt>; see also National Security Agency, DOCID No. 352694, *Phone Freaks Can Invade Your Privacy* (1976), available at <http://explodingthephone.com/docs/db904> (declassified NSA memo describing how interfaces used by phone company employees to determine if a line was busy were subverted by outsiders to listen to phone conversations).

³³ See, e.g., Rachel King, *Stuxnet Infected Chevron's IT Network*, Wall St. J. (Nov. 8, 2012), <http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/>

³⁴ See, e.g., Matthieu Aikins, *The spy who came in from the code*, Columbia J. Rev. (May 3, 2012), available at <http://bit.ly/1L1BK7j> (detailing how lack of digital security protections exposed journalists’ Syrian sources to retaliation by intelligence services).

³⁵ Encryption is a process that involves making a message unreadable except to the person who knows how to decrypt it back into readable form. Encryption can be used across a variety of platforms, including phone, Voice over Internet Protocol (VoIP), email, online chat and file-sharing.

³⁶ Tools that can help provide anonymity include proxies, which channel communications through an intermediary device. Not all proxies provide anonymity, even if they can help journalists access information online that was previously censored. In addition, not all proxies utilize encryption and those that do, do not necessarily provide anonymity.

digital security trainings in newsrooms and journalism school curricula.³⁷ The proposed amendment would undermine these best practices because a journalist using anonymization tools could be the target of a remote access warrant to obtain evidence, even if that person is not suspected of criminal activity.

Tor and other anonymizing proxies are widely used by journalists seeking to protect their communications and their sources. These tools are critical for journalists to protect their communications with sources and to carry out their constitutionally recognized role. As currently written, the proposed amendment to Rule 41 could detrimentally impact journalists and erode the confidentiality of their relationships with sources, even when using Tor or other anonymizing tools to obscure identifying information.

II. **Methods for infecting computers with malware can compromise the credibility of news media.**

The proposed amendment to Rule 41 also fails to appropriately address the manner in which law enforcement can perform remote access searches. News organizations have been used as “covers” for the installation of malware. The impersonation of the news media in order to execute a remote access search contemplated by the proposed amendment to Rule 41 is unacceptable.

Law enforcement can deliver malicious software to their targets in numerous ways. One way is through a watering hole attack, which occurs when custom malicious code is installed on a website that is popular with the target group and which infects the computers of everyone who visits the site.³⁸ The FBI, non-state actors, and foreign governments have used this method to surveil sources.³⁹ A few years ago, the website for the Council on Foreign Relations was the victim of a watering-hole attack.⁴⁰ More recently, advertising on the website for Forbes magazine was compromised, resulting in the installation of malware on readers’ computers.⁴¹

Another delivery method for malware is through social engineering, or the practice of obtaining confidential information by the manipulation of legitimate users. In

³⁷ See, e.g., Frank Smyth, *Digital Security Basics for Journalists*, Medill National Security Zone, <http://bit.ly/LeuRpv>; Susan E. McGregor, *Digital Security and Source Protection for Journalists*, Columbia Journalism School (2014), <http://bit.ly/1Abz0PT>; Chris Walker and Carol Waters, *Learning Security: Information Security Education for Journalists*, Tow Center for Digital Journalism at Columbia Journalism School (Feb. 5, 2015), <http://bit.ly/1BXZqCR>; Pew Research Center, *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior* (Feb. 5, 2015), <http://pewrsr.ch/1DPwQ9b>.

³⁸ See, e.g., Threat Encyclopedia, TrendMicro, <http://bit.ly/1zX6Klf>.

³⁹ See, e.g., Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired (Aug. 5, 2014), available at <http://wrd.cm/1As2qfV>; see also Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired (Sept. 13, 2013), available at <http://wrd.cm/1v11NYi>.

⁴⁰ Michael Mimoso, *Council on Foreign Relations Website Hit by Watering Hole Attack, IE Zero-Day Exploit*, Threatpost (Dec. 29, 2012), available at <http://bit.ly/1zgXAfE>.

⁴¹ Thomas Fox-Brewster, *Forbes.com Hacked In November, Possibly By Chinese Cyber Spies*, Forbes.com (Feb. 10, 2015, 6:44 P.M.), <http://onforb.es/1CgbMZw>.

2007, the Federal Bureau of Investigation impersonated the Associated Press (the “AP”) in order to deliver malware surreptitiously to a criminal suspect in the course of an investigation and thereby trace his location.⁴² The FBI sought review from the Office of General Counsel (“OGC”) and obtained a Title III warrant from a magistrate judge.

In that case, FBI agents sent a fake AP article to a target suspected of making bomb threats to his school. Once the target clicked on the link, he unknowingly downloaded sophisticated malware, which revealed his computer location and Internet Protocol address, and which helped agents confirm his identity.⁴³ While the FBI did seek the appropriate warrants it appears that the FBI failed to notify the OGC and the judge that the malware was delivered in the guise of an AP article, with an AP byline, and therefore impersonated a news media organization.

In response, the AP demanded that the FBI cease its impersonation of the news media. AP President and CEO Gary Pruitt said, “In stealing our identity, the FBI tarnishes that reputation, belittles the value of free press rights enshrined in our Constitution and endangers AP journalists and other newsgatherers around the world...[t]his deception corrodes the most fundamental tenet of a free press—our independence from government control and corollary responsibility to hold government accountable.”⁴⁴ Ultimately, this type of action “erodes our ability to gather news by intimidating sources who might otherwise speak freely with our journalists.”⁴⁵

In addition to lacking any safeguards for First Amendment activity, and undermining existing statutory and constitutional protections, the proposed amendment to Rule 41 turns a blind eye to the threat of law enforcement impersonation of the news media in an effort to execute a remote access search. The interests protected by the First Amendment demand that law enforcement not impersonate the news media to facilitate remote access searches. However, under the proposed amendment to Rule 41, law enforcement is not required to disclose how it plans to execute a search when it applies for a remote access warrant. It would be impossible for a judge presented with a request to issue a warrant for a remote access search to understand that First Amendment rights may be implicated, thereby triggering the “scrupulous exactitude” requirement of

⁴² Mike Carter, *FBI confirms it used fake story, denies bogus Times Web link*, Seattle Times (Oct. 28, 2014), available at <http://bit.ly/1DZSbNR>.

⁴³ See e.g., Ellen Nakashima and Paul Farhi, *FBI Lured Suspect with Fake Web Page, but May Have Leveraged Media Credibility*, Wash. Post (Oct. 28, 2014), available at <http://wapo.st/1xCpHpk>; see also Eric Tucker, *Associated Press Demands FBI Never Again Impersonate Media*, Huffington Post, (Nov. 10, 2014), available at <http://huff.to/1MovNmw>.

⁴⁴ Tucker, *supra* n.42.

⁴⁵ *Id.* As the Reporters Committee stated in a letter to the Attorney General and FBI Director, sent on behalf of 26 media organizations concerning the FBI’s impersonation of the AP, using the news media as a cover for remote access searches “endangers the media’s credibility and creates the appearance that the media is not independent of the government. It undermines media organizations’ ability to independently report on law enforcement. It lends itself to the appearance that media organizations are compelled to speak on behalf of the government.” Reporters Comm. for Freedom of the Press, Ltr. to Attorney General Holder and FBI Director Comey (Nov. 6, 2014), available at <http://www.rcfp.org/sites/default/files/2014-11-06-letter-to-doj-fbi-regarding-se.pdf>.

Stanford Daily. The omission of these safeguards risks treading on vital First Amendment rights.

The proposed amendment to Rule 41 implicates constitutional and statutory rights of journalists and news media organizations in myriad ways that must be addressed by Congress if they are to be altered. Given the host of legal and policy considerations raised by the proposed amendment to Rule 41, the Reporters Committee urges the Committee to reject the proposed language in full.

Sincerely,

Bruce D. Brown, Esq.
Katie Townsend, Esq.
Hannah Bloch-Wehba, Esq.
Jennifer Henrichsen
Reporters Committee for Freedom of
the Press

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9f-97dd
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0048](#)

Comment from Cormac Mannion, NA

Submitter Information

Name: Cormac Mannion

Organization: NA

General Comment

This proposed change to Rule 41 is abhorrent in its method and supposition of wrongdoing for the "accused." The use of technical means a la Tor or VPN encryption to engage in private communications does not constitute any malfeasance on the part of the "accused." The commonality between Tor/VPN users and the intended target of this amendment, is a technical inclination and motivation to keep their communications private from the bulk collection methods that we know to be used by sophisticated governments like our own, as well as by criminal networks of sophisticated hackers, throughout the world. The common factor in the correlation between Tor/VPN use and online crime is that aforementioned understanding of the government and hackers' capacity to break common encryption standards and protocols to maintain ostensibly private communications, and the technical capacity and willingness to download readily available software like Tor or OpenVPN for everyday use. Many innocent people use this software, thus the net is being cast far too wide in practical terms.

Please do not subvert the will of the People to be safe in our personal effects using this sort of legal wrangling. The chilling effect that this has on free speech is just not worth it.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9g-iwqk
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0049](#)

Comment from Raul Duke, NA

Submitter Information

Name: Raul Duke

Organization: NA

General Comment

This is an infringement on first, fourth, and fifth amendment grounds, if not illegal in other ways. I suggest that DOJ saves the years of attorney fees and wasted taxpayer money defending what is possibly an unwise and illegal policy.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9g-8n88
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0050](#)

Comment from Michael Boucher, NA

Submitter Information

Name: Michael Boucher

Organization: NA

General Comment

My full comments are in the attached document. This is taken from the introduction:

Others have already commented on the problems with the fact that the warrants can be issued nationwide. As an entrepreneur who has started and operated several successful technology companies, I have considerable worries about the way that three other elements of the proposed amendment combine:

the lax standard required to establish probable cause that a computer contains evidence of a crime; the irrational focus on whether a target computer conceals its media or information; and the absence of any credible procedures and safeguards governing how the hacker warrants are executed

Although it would be possible to correct some of the problems, it is more likely that adequately addressing some of the substantive issues goes outside of the scope of this procedural body and requires a legislative approach. Therefore, I urge the Committee to reject the proposal in full.

Attachments

Comment to Rule 41, February 17, 2015

To: Members of the Advisory Committee on Criminal Rules
From: Michael Boucher
Date: February 17, 2015
Re: Comment on the Proposed Amendment to Rule 41 Concerning “Remote Access” Searches of Electronic Storage Media

Dear Members of the Committee,

I submit these comments to aid the Committee’s consideration of the proposed amendment to Rule 41 concerning remote access searches or “hacking warrants” for computers and other electronic devices.

Others have already commented on the problems with the fact that the warrants can be issued nationwide. As an entrepreneur who has started and operated several successful technology companies, I have considerable worries about the way that three other elements of the proposed amendment combine:

- the lax standard required to establish probable cause that a computer contains evidence of a crime;
- the irrational focus on whether a target computer conceals its media or information; and
- the absence of any credible procedures and safeguards governing how the hacker warrants are executed

Although it would be possible to correct some of the problems, it is more likely that adequately addressing some of the substantive issues goes outside of the scope of this procedural body and requires a legislative approach. Therefore, I urge the Committee to reject the proposal in full.

This comment begins by describing why the standard for establishing probable cause that a computer contains evidence of a crime is too low. I do not object to the current showing of probable cause required to support a Rule 41(e)(2)(B) warrant against a computer. However, the showing required to support a hacking warrant is too low. The next section discusses why considering whether a target computer conceals the location of its media or information is a poor idea. The next section summarizes why credible procedures and safeguards governing how hacker warrants are executed must be added. The final section is a summary.

I appreciate the Committee’s consideration of this comment.

I. The nature of computer crimes and the evidence of computer crimes is such that we must exercise special care when issuing warrants to access information on personal computers and other electronic devices to protect the right to privacy when the target has a reasonable expectation of privacy.

The nature of computer crimes and the associated evidence is such that we must think differently about the probable cause required to support Rule 41 warrants against computers and computer information, and we must be especially carefully about what should be required to support something as intrusive as the proposed hacking warrant.

Where a criminal intends to use a computer to commit an act that he knows is a crime, it is the job and proper role of law enforcement and the courts to cooperate to the extent possible and permitted to bring the criminal to justice. However, the unique characteristics of computers, computer crime, and evidence of computer crime are such that it is necessary to consider very carefully whether and how to take tools intended for use against dangerous criminals and deploy them against ordinary and innocent citizens. Exceptionally powerful weapons such as the proposed hacking warrant pose an especially grave danger to areas of citizens' lives in which the citizens have a reasonable expectation of privacy.

Consider the Department of Justice's concern about viruses and botnets. Assume that law enforcement knows that a particular botnet is involved in crime and has probable cause to believe that a particular computer is infected by the botnet, meaning that software owned by the botnet has infiltrated the computer in question. In that case, the botnet program that is secretly running on that computer is evidence of a crime and 41(c)(1) allows a warrant to issue to seize evidence of a crime. That allows search and seizure of the computer and its data related to the bot. In this situation, it seems that the only thing that the proposed amendment adds to the existing Rule 41 is the ability to seize the evidence with "remote access" or hacking.

However, that situation is unlike other situations in which a warrant is against a facility or container that contains evidence of a crime. For example, if law enforcement officers have probable cause to believe that my house contains evidence of a meth lab or marked money from a bank robbery or a murder weapon and those officers are correct then I'm probably cooking meth, robbing banks, or murdering people. Get a warrant, seize the evidence, and call the prosecutor.

By contrast, in the hypothetical case above of the computer with a bot, the owner is totally uninvolved in any crime. The Government is able to convince a judge in an *ex parte* hearing that it has probable cause that his computer does or did contain a bot, that is technically evidence of a crime, and so it is technically a legitimate target for an existing Rule 41 search warrant. However, unlike in the hypothetical, the owner has no specific intent to commit a crime, did not commit a crime, did not abet a crime, did not profit from a crime, and does not know anything about any crime. Too bad for his team. The actions of a criminal with whom the owner has no contact results in a warrant that enables extremely intrusive hacking of the target computer, search of a computer that may contain intimate details of the owners life, and seizure of that and other information.

The new hacking warrant in the proposed amendment just makes things worse for this innocent target. He has done nothing to deserve having his most private and intimate information rummaged and tossed by some hacker regardless of whether the hacker is a criminal or is an agent of the Government with one of the new hacking warrants. Having the hacker be employed by his own government and violating areas of his life in which he maintains a reasonable expectation of privacy adds insult to injury.

Anyone's computer can fall victim to a computer virus that installs a bot that is part of a criminal enterprise, and many millions of innocent citizens have. A bot that is part of a criminal enterprise is evidence of that criminal enterprise. Therefore, anyone's computer can be subject to the sweeping new surveillance, search, and seizure authority that the proposed amendment grants the Government. Bots are becoming more capable and outrunning security measures by ever-greater margins, so the number of computers that will at some point host a bot will only increase. Therefore, the number of computers and the number of citizens whose privacy will be subject to invasion by the Government will only increase. It is critical that additional safeguards be added to the hacking warrant. A hacking warrant should not issue against a target where there is no showing of criminal intent, knowledge, or *mens rea*.

II. The proposed amendment is grossly overbroad because it targets computers that conceal the location of their data by technological means, and virtually all modern computers conceal the location of their data by technological means almost all of the time because that is how modern computers work.

The proposed amendment to allow a national hacking warrant to issue because the location of a computer or its data are concealed is overbroad and ignores the way that modern computers work. All modern computers conceal their locations and the location of their information as part of the way that they must work. The relevant consideration is whether the concealment prevents law enforcement from getting access to data for which it has a legitimate need supported by a warrant. If it does not, the hacker warrant should not issue. Because it is so intrusive, a hacker warrant should issue only when law enforcement cannot get access to data in any other way.

A good analogy to the way modern computers work is the way that libraries work. If you ask a librarian the location of a specific book, the librarian may well answer, "I don't know, the intern has concealed its location from me by taking it off of my desk and putting it back on the shelves where it belongs." In a library, the concealed book problem is not solved by amending Rule 41 of Library Procedure to authorize the waterboarding of the intern. Instead, the librarian will simply consult a catalog or index and then tell you how and where to find the book. Concealed information is not always information that is kept from you, or even information that is hard to retrieve. It's just concealed. Remain calm. Ask the librarian for help. You'll get your information. It's no big deal.

This is how libraries work, and in the subsections that follow on cloud computing, virtual private networks, and dial-up internet connections, you will see that this is also how virtually all modern computers work, why it is necessary that they work that way, and why there is no need to panic and waterboard the intern or panic and create new invasive national hacking warrants with inadequate safeguards. If reading about details of technology isn't your thing, there's a summary at the end that wraps it all up and puts a bow on it for you.

A. Virtually everyone uses multiple cloud computing services, and cloud computing services necessarily conceal the location of media or information through technological means, so simply using one of myriad computing services that is necessary for daily life exposes almost everyone to the threat of intrusive surveillance, search, and seizure.

Almost everyone uses cloud services every day. Cloud services are services in which processing is done or data is hosted by a collection of remote computer and data storage resources that are said to be “in the cloud.” These remote computers are spread around the world to satisfy requirements including, but not limited to, surviving disaster, sharing a workload among distributed computer centers, proximity to customers, access to cheap electricity, and many others.¹

Files containing media and information automatically move freely and frequently within the cloud to achieve the goals of the cloud operator at the direction of proprietary algorithms and without the knowledge or direction of the user who owns the data. The fact that data automatically migrate among servers whose locations are unknown means that anyone who uses almost any cloud service satisfies the requirement that “the district where the media or information is located has been concealed through technological means.”

The picture that follows depicts a map of the locations of the data centers that house the data in the Google cloud.² It is representative of comparable clouds operated by Amazon, Microsoft, news and media companies, and countless others. A particular datum such a specific email message or notes maintained by a reporter in electronic form may be located in any of these servers and the user does not know or care which. Copies of the same data may or may not be present on more than one server simultaneously so that losing access to one data center need not impair access to specific data because that data will be mirrored in other data centers.

¹ As Google explains at <https://support.google.com/googleforwork/answer/6056694?hl=en>, “Your data will be stored in Google's network of data centers. Google maintains a number of geographically distributed data centers.” Navigate to the web page above, then click the plus sign (“+”) next to the question, “Where does Google store my data?” It will expand to show the text above.

² The original version of this map, along with additional supporting data, is available at <https://www.google.com/about/datacenters/inside/locations/index.html>. The U.S. data centers are located in Georgia, Iowa, North Carolina, Oklahoma, Oregon, and South Carolina, and the international data centers are located in Belgium, Chile, Finland, Ireland, Netherlands, Singapore, and Taiwan.

However, it is not necessary that copies of all data are present on all servers, so nobody really ever knows whether a particular server contains some specific data.



One can readily see that the constant movement, copying, and transformation of data in this cloud of servers may move media or information across the boundaries of judicial districts or even of nations. Because almost no one knows where a particular datum is at any given time, it is obviously true that the location of all information in the cloud has been concealed through technological means.

One can also readily see that this concealment is not part of any nefarious scheme to do... well, anything. It's not nefarious. It's not a scheme. It's a computer doing what we need a computer to do. Unless we want to lose all of our emails every time a server crashes, the data has to be replicated in multiple locations. Unless we want our email to be slow every time a server gets busy, the data needs to be moved in response to system load. Unless we want to manually manage how and where our email is stored and duplicated and migrated within the Google cloud, it has to all happen with technology, which means that the only way that anything works is that the location of most of our information has to be concealed through technological means.

It is also obvious that the overly broad surveillance, search, and seizure powers granted to the Government by the proposed amendment are completely unnecessary for cloud services. Even though the location of a specific email, document, or other cloud-resident datum is concealed via technological means, the Government can readily get access to the data from Google, Amazon, or whoever the cloud operator is. Getting access from the cloud provider is easier than hacking (i.e., getting "remote access" to) a target computer and it can provide more complete data. For example, while the target computer may be able to provide data, the cloud provider may also be able to provide related deleted data and metadata.

In addition to it being easier for the Government to work directly with the cloud providers, such a system is better for the data owner. Allowing the hacking warrant as described in the proposed amendment would allow the Government to get access to this information by directly hacking a target computer, which allows no effective representation of the interests of the data owner. Requiring the Government to work with a cloud provider allows for the possibility that the cloud provider would act to protect the interests of the data owner in various ways. For example, the provider may test an overly broad or invalid warrant in court. The provider may also perform some minimization on the data before surrendering it to the Government. Both of these are useful safeguards, but neither of these occur if the Government is allowed to hack the remote computer and take the data directly. Thus, requiring the Government to get the data from the cloud provider introduces some small measure of fairness and balance into the *ex parte* warrant process that would otherwise have no representation for the interests of the data owner.

The files and data in these services contain our core political speech, medical information, religious affiliation and other constitutionally protected associations, and many other private details of our lives about which we have a reasonable expectation of privacy. When the Government gets access to these files and data by hacking rather than by working with the cloud provider, it subjects our protected speech and other rights to extra scrutiny by the Government at the cost of higher inconvenience, less complete access, greater expense, and more delay, yet without a corresponding advance in a significant and legitimate Government interest. These problems are mitigated by a rule that a hacking warrant will not issue unless there is no other way to get the data.

The sections below describe some of the cloud services in routine use by almost everyone all of the time. The reader is reminded that because each of these is a cloud service, all of the data in each will be subjected to the intrusive search and seizure procedures specified in the proposed amendment because the location of the data is concealed by technological means. The reader is also reminded that because each of these is a cloud service, legitimate search and seizure is in no way affected by the adoption or rejection of the proposed amendment. Legitimate searches and seizures against these sources will continue to be done in the fastest, easiest, cheapest, most efficient, and most complete way possible, which is to issue a subpoena to the cloud provider, just as they are today.

a. Email

Widely used email services that are hosted in various clouds include Google's Gmail, Microsoft's Hotmail, Yahoo!'s Yahoo Mail, and many others. Email contains a broad variety of our speech on many topics including core political speech, a list of our associations with whom we have communicated, and many other topics in which we have a reasonable expectation of privacy.

b. Data Storage

There are many services that store data in the cloud that would have once been stored on a user's computer. These include simple data storage systems, integration of cloud storage into applications that previously used desktop storage, and applications that operate on data that is intrinsically stored in the cloud. Hybrids of these are also common.

An example of a simple data storage system based in the cloud is Dropbox.³ Dropbox mirrors a computer directory into the cloud. As files in the mirrored directories are added, deleted, or updated, Dropbox updates their cloud versions to add, delete, or update in an identical way. In its simplest form with only one computer, this basically acts as a real-time backup system for the mirrored directories. When multiple computers mirror the same directory, Dropbox acts as an easy file sharing mechanism. When a file in a directory on one computer is created or updated, it is created or updated in the same way on all computers that mirror the same directory.

One can readily see that it can be difficult to keep track of the location of data and one could even argue that the location information had been concealed by technical means, especially in configurations with multiple computers. However, one can just as readily see that it does not make any difference to law enforcement because they will readily get any data to which they are legitimately entitled with no more difficulty than serving a subpoena on Dropbox, Inc.

Another form of cloud-based data storage is embodied in data backup services such as Carbonite.⁴ As with Dropbox, Carbonite automatically copies data from a computer to cloud-based storage whose location has been concealed by technological means. Although the location of the data is kept constantly concealed, the data may

³ <https://www.dropbox.com/business> contains more information about this commercial service.

⁴ <https://www.carbonite.com> contains more information about this commercial service.

be trivially retrieved. Users retrieve data to which they are legitimately entitled with the easy-to-use Carbonite control panel. Law enforcement retrieves data to which they are legitimately entitled by serving a subpoena on Carbonite, Inc.

Unlike the single file image that they would get by hacking, competent law enforcement officers who use the more efficient subpoena on Dropbox or Carbonite can get many previous versions of the files to which they are entitled in addition to the single version of the file that they would get from a hack. This ability to see the history of a file develop, together with a timeline showing when each modification was made, is exactly the sort of detailed information that any law enforcement officer wanting the data for a legitimate reason would find very useful. By contrast, a law enforcement officer using a hacking warrant to retrieve previous versions of a file directly from a target computer would likely destroy current versions of the file in the process. It would not take exceptional clumsiness for the hacker officer to compound that error by making his efforts prematurely visible to the target, a risk that the officer using a subpoena would not face.

Another class of cloud services in addition to simple data storage and recovery involves integrating cloud storage into existing applications. For example, Microsoft is integrating its SkyDrive storage technology into its Office productivity suite. One example of this new capability in Office allows a user to create a Word document on her desktop at work, store it in SkyDrive, and then have it available to work on with her SkyDrive-enabled version of Office at home. She no longer has to copy the file to a disk or USB drive. Anywhere she can access the internet, she can access all of her Office documents, spreadsheets, schedules, drawings, and other files.

c. Cloud-based Applications

Another class of cloud services comprises applications that work natively in the cloud. Google Docs is an example of this type of service. Google Docs is an office productivity suite that includes a word processor, spreadsheet, and so forth just like Microsoft Office. However, rather than using a technology like SkyDrive to copy data into the cloud, the data are in the cloud all the time. This enables various collaboration features that are not available or not yet as well-developed on systems that are based on a user's computer.

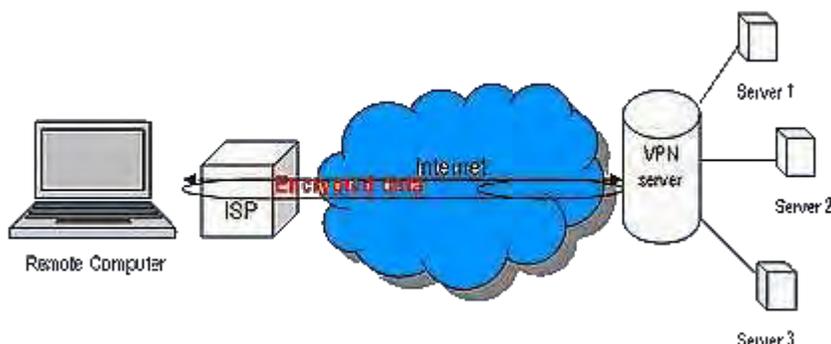
The reader will anticipate that the SkyDrive and Google Docs files containing data that may be of interest to law enforcement are in the cloud and therefore their locations are concealed by technological means. As expected, it is true that their locations are concealed but that has no relevance to the question of whether law

enforcement will find it all difficult to access them with existing probable cause warrants. No new hacking warrant is required.

B. Virtual Private Network (VPN)

Virtual Private Network (VPN) software uses encryption and other techniques to maintain a virtual computer network that can run on top of one or more physical networks, including the public internet, but behaves in most respects like a private network. Almost all computers have some type of VPN-like technology built in.⁵ Many or all of the computers on a VPN will have their locations or the locations of their media or information concealed through technological means. In general, users do not want or need such concealment, often are not even aware that it is happening, have no specific intent for it to happen, and cannot enable, disable, or change it.

In one VPN configuration of interest to this discussion, a corporation has a secure private network consisting of many computers collocated at some physical facility such as an office building. An employee may also have a machine at home with a connection from home to the public internet. The employee uses that connection to reach the corporate network. The point of connection into the corporate network is equipment called a VPN server. This setup is depicted below.



Ordinarily, when the employee's computer wants to interact with other computers on the internet, it will send requests of various sorts through its own

⁵ <http://windows.microsoft.com/en-us/windows/connect-using-remote-desktop-connection#connect-using-remote-desktop-connection=windows-7> describes a VPN named RDP that has been installed by default on every copy of Windows for years. <http://www.hotspotshield.com/vpn-for-mac> describes a VPN for Mac. There are at least dozens of others available for Linux, UNIX, Android phones and tablets, iPhone, iPad, at least one for a smart watch, and almost any other platform you can think of.

internet connection and ask that results be returned to its location in the employee's home. When the employee's computer is being used as a VPN, it does not interact directly with the public internet in that way. Special software running on the employee's computer instead redirects all of those requests to the corporate VPN server, which then executes them as if they had come from a computer located in the employer's building.

This arrangement allows the employee working from home to get all of the benefits of working from the employer's building. All of the resources on the private network including files, printers, and other computers are available just as if the employee's computer were in the employer's building.

Of course, this means that someone looking at traffic originating from the employee's computer would also believe that the employee's computer was located in the employer's building. The location of the employee's computer and all of its data is concealed by technological means, specifically the combination of VPN hardware and software. The employee may have no specific intent to conceal her location, is not participating in any nefarious scheme or untoward activity, and generally has done nothing that should subject her home computer to the heightened surveillance, search, and seizure from a hacking warrant. However, as similarly to other situations described elsewhere in this comment, her simple act of holding a certain type of job in the 21st century causes her to satisfy the very low threshold that the Government proposes to set for its extraordinarily harsh hacking invasion of areas of her life in which she has as reasonable expectation of privacy.

Fortunately, as with virtually every other situation in which a computer does such concealment, law enforcement with a valid probable cause warrant of a type already authorized by Rule 41 will have no difficulty getting access to concealed information on a VPN. Given that most employers would not care to have their employees using company computer resources to hold down a second job as a computer criminal, most employers would probably grant law enforcement officers their desired access even without a warrant. Regardless, the point remains that here, as with virtually all instances of computers concealing their locations through technological means, legitimate law enforcement objectives can be met with existing mechanisms.

Perhaps something much narrower and more constrained than a national hacking warrant may still be needed for some instances. However, this example demonstrates yet again that simply noticing that a computer conceals its location

through technological means should not be enough to trigger such an intrusion into our personal computers and private lives.

C. Connecting to the internet via dial-up connections necessarily conceals the location of the connecting computer through technological means.

Although most Americans access the internet through broadband provided in their homes by an Internet Service Provider (ISP), around 10 million Americans access the internet by calling an ISP on their telephones.⁶ This is referred to as dial-up access. The technical characteristics of a dial-up connection necessarily uses technical means to conceal the location of the user's computer, and therefore the media or information that it contains.

It is necessary to understand the configuration of a dial-up connection to the internet to see why dial-up connections inherently and unavoidably conceal the location of the connecting computer, along with its media and information, through technological means. To use dial-up internet access, a user attaches a computer to a telephone with a device called a modem. When the user calls a telephone number supplied by an ISP, a modem on the ISP side connects to the user's modem.⁷ The ISP then connects to the internet and passes packets of information back and forth between the user's computer and the internet.

Because the telephone system that the user is using to call the ISP is not part of the internet, there is no way to tell the other computers on the internet that the user's connection enters the ISP's building and then continues through the phone line to the user's house. The internet connection itself goes to the ISP's building, so it appears to the computers on the internet that the user is connecting from the ISP's building. In other words, the user has used technological means to conceal the location of the computer and the media and information that it contains.

⁶ Home Broadband 2013 by the Pew Research Center's Internet and American Life Project, available at <http://pewinternet.org/Reports/2013/Broadband.aspx> on page 2 states that 3% of adults over 18 use dial-up internet access. It does not give data on children, so this assumes that 3% of the total population uses dial-up internet access. The State & County QuickFacts publication from the United States Census, available at <http://quickfacts.census.gov/qfd/states/00000.html>, estimates the 2014 population at 318,857,056. 3% of 318,857,056 people is 9,565,712.

⁷ As an example, <http://access.web.aol.com/accessnum/?ac=571> shows the list of telephone numbers that an AOL dial-up subscriber near Arlington, Virginia might use. The modems at each number may have different properties and so a user may not dial the number of the closest facility. For example, a user in Manassas with a high-performance modem might call the Arlington or Leesburg modem bank to get access to a better connection. Also, one might call a more distant facility if all of the modems at the closest facility are in use.

However, as with virtually all instances in which a computer's location is concealed by technological means, the user has no intent or desire to enable or disable the concealment, likely has no idea that the concealment is occurring, and is not intentionally or otherwise using the concealment to advance a nefarious purpose. In fact, the user probably does not even want the true location concealed because the concealment breaks software on the internet that relies on being able to determine a computer's true location. A user in Leesburg who dials in to a modem bank in Arlington appears to computers on the internet to be located in Arlington so the Best Buy Store Locator will refer the user to far away stores, the Domino's Pizza Finder will connect to stores in Arlington that do not deliver to Leesburg, and so forth.

As one would expect, dial-up users tend to be nonwhite, have less education, less household income, and are more likely to be elderly than broadband users.⁸ These users are among the most vulnerable users on the internet and do not deserve to have their own government treat them with a presumption of ill intent just because the only internet connection they can afford makes their lives harder by telling everyone that their computer is some place that it is not.

Although exact numbers vary by situation, dial-up internet access can be around 100x slower than broadband. Because their connections are so slow, the bandwidth consumed even by surveillance and search will be a significant percentage of the total available. Bandwidth consumed by surreptitious seizure of any substantial amount of data will render their connections useless during the period in which the seizure is taking place. Although broadband is always on, the nature of dial-up access is such that it is only on when users are actually using it. As a result, any seizure activity undertaken by law enforcement will occur at exactly the same time as users are trying to use the connection for their own use and will therefore substantially harm or even make impossible common internet tasks such as paying bills in a timely manner, using the internet to work from home, and so forth.

However, this is a group of almost 10 million people and so some of them are going to be bad actors. Should law enforcement be denied an opportunity to surreptitiously hack into the computers of a few bad actors just because of some crazy desire to preserve the rights and dignity of all of the vast majority? Well, yes.

⁸ Home Broadband 2013 by the Pew Research Center's Internet and American Life Project, available at <http://pewinternet.org/Reports/2013/Broadband.aspx> on page 3.

As with almost every instance of computers whose locations are masked by technological means, the problem of bad actors on the other end of a dial-up connection can be readily solved with a subpoena, this time to the ISP. ISPs maintain logs for billing and other purposes and will have little difficulty in locating subscribers who are of interest to law enforcement. Law enforcement officers with the ordinary probable cause warrants authorized today by Rule 41 will have no trouble getting the information even without a new national hacking warrant.

D. Using common and even legally required operations on cell phones and portable electronic devices conceal the location of media or information through technological means.

As anyone who has flown can attest, your seat trays must be in the upright and locked position and all electronic devices must be turned off or put into “airplane mode” before takeoff. Although the tray thing does not have to be a big deal, the same cannot be said for airplane mode. Airplane mode disconnects your device and all of its data from the internet, thereby concealing its location through technical means. Turning off WiFi on an Android degrades its ability to determine its location, thereby partially concealing its location even from itself.

One might imagine that I threw this one in just for fun, but one would be wrong. Fun is what the library intern waterboarding suggestion was for. This one is serious. Some prosecutors have argued that defendants have acted suspiciously in turning off their cell phones to avoid advertising their locations to cell phone towers that might later relay the data to law enforcement. It is no stretch at all to imagine that investigators attempting to use cell phone tower data to track a suspect would treat airplane mode, turning off WiFi, or other steps a suspect might take as an attempt to conceal location by technological means and seek a hacking warrant on the phone.

However, we have a right to keep things private, even if that introduces inconvenience for law enforcement. If I want to turn off my cell phone, I should be able to do that without exposing myself to the argument that I’m trying to have some privacy and that desire for privacy gives the Government authority to hack my phone with measures that are even more intrusive than they would have used if I had not sought privacy. Recalling from the beginning of this comment the ease with which “evidence of a crime” can appear on the computer or electronic device of wholly innocent people, this Committee needs to show some real care and

consideration before authorizing something as powerful as national hacking warrants.

E. Summary

The tiny set of examples given above taken from a very small set of tasks on which modern computers operate does not even approach a comprehensive list of the ways in which any modern computer will conceal its location and the location of the media and information it contains. However, one can readily see that the location-masking is not done for nefarious purposes and that it is often unavoidable for doing even mundane tasks such as reading email. Because almost all computers will use one or more of the location-masking technologies described above and because there are so many ways for a file that may contain “evidence of a crime” to appear on a computer, the supposedly narrow expansion of Rule 41 that the Government proposes actually makes a huge number of computers owned by innocent computer owners subject to hacking warrants.

These examples also make clear the need for some meaningful attempt to limit this huge expansion of the Government’s power so that it does not needlessly expose innocent citizens to invasive searches and seizures. Simply allowing concealment to stand alone as a justification for special treatment is senseless and unnecessary.

III. The requirements specified in the proposed amendment for issuing a hacking warrant are ludicrously loose, especially when compared with the requirements for issuing a less-potent wiretap order.

The conditions under which the proposed amendment allows a powerful remote hacking warrant to issue are extremely loose. The conditions under which a hacking warrant may issue must be made considerably tighter to accord with statutory requirements on warrants or orders of comparable power and to respect the rights of those against whom the hacking warrants will be deployed.

It is useful to compare the very loose conditions for a hacking warrant with the more protective conditions under which a wiretap is authorized because both are powerful search and seizure mechanisms, although a wiretap is in many ways less intrusive than a hacking warrant. Unlike with hacking warrants, wiretaps can reveal only what is said at a particular time on a particular device. The more powerful hacking warrants enabled by the proposed amendment can authorize

trolling through a large body of stored data to reveal a lifetime of intimate detail about one's core political speech, religious beliefs and practices, associations, and much more. Any damage not done by the authorized trolling can be enabled by the plain view doctrine to allow the searcher to surveil, search, and seize even further.

It is therefore extremely important that the processes and procedures controlling the issuance and execution of the hacking warrants be thoughtfully designed and thorough. Tossing a couple of vaguely-worded subsections into the middle of Rule 41 and hoping that subsequent case law sorts it all out simply will not do. Comparing the proposed amendment with similar parts of the wiretap process will illustrate the difference in approach between the Government's proposed amendment enabling hacking warrants and what has been proven over time to work well for law enforcement and protecting the substantive rights of citizens with wiretap.

This section starts with a short summary of what the proposed amendment allows a hacking warrant to do and why the warrant created by the proposed amendment is so powerful. It then contrasts the procedures for requesting the two types of searches and seizures, the processes by which the two types are accomplished, and the protections awarded to citizens under each search/seizure regime.

The hacking warrant enabled by the proposed amendment allows the Government to:

- remotely hack into a target computer without the authorization, knowledge, or consent of the owner, and with no meaningful opportunity for the owner to contest that intrusion;
- access a storage device on the target computer capable of holding an amount of intimate personal information equal in size to the contents of an academic research library and close to the size of the Library of Congress⁹;
- seize the information on the target computer, including some of the most intimate details of the owners life, and hold it indefinitely or forever; and

⁹ <http://apps.americanbar.org/lpm/lpt/articles/fwr01041.html> estimates that 2 terabytes, which is well within the capacity of an ordinary personal computer, could hold the entire contents of an academic research library and 10 terabytes could hold the contents of the Library of Congress.

- often enable a camera or other recording capability on the computer to allow ongoing surveillance of the owner, owner’s family, and visitors as they are in various states of vulnerability, intimacy, undress, and other states that are within the reasonable expectation of privacy of the subjects.

First and foremost, such a gross intrusion into the right to privacy as a wiretap is not permitted at all without a showing that the individual targeted “is committing, has committed, or is about to commit a particular [serious federal] offense...”.¹⁰ In sharp contrast, the proposed amendment merely requires a showing that “activities related to a crime may have occurred”¹¹ and that the target computer may have “evidence of a crime.”¹² Although it may never be used for this purpose, it is nevertheless true that the proposed amendment’s requirements are so feeble that it would allow remote hacking of a cell phone and search and seizure its data if its GPS data would probably show that the owner may have performed “activities related to [the] crime” of exceeding the speed limit in a residential street. Even if such a permissive standard were not an open invitation for pretext searches and seizures, it would still be far too permissive for an intrusion on the scale of the hacking warrant.

A violation of the reasonable expectation of privacy on the scale of a wiretap is also not permitted unless the offense is a serious offense.¹³ A serious offense for which a wiretap may be appropriate includes “sabotage of nuclear facilities,” “weapons of mass destruction threats,” “sex trafficking of children,” and offenses “relating to biological weapons,”¹⁴ among many others of comparable gravity. By contrast, the proposed amendment is limited only by the requirement that “activities related to a crime may have occurred.” Is the power of the hacking warrant limited only to serious federal crime? No. Any federal crime? No. A crime with a lot of victims? No. A crime with any victim, any at all, even one, and even if it was just a hamster? No. A crime that someone might prosecute? No. What about a crime that is just used as a pretext to perform a hack, search, and seizure that would otherwise be illegal? No, even that is not restricted in the proposed amendment.

¹⁰ 18 USC § 2518(3)(a).

¹¹ Proposed rule 41(b)(6).

¹² FRCrP R. 41(c)(1).

¹³ 18 USC § 2518(3)(a) (“there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516”) and 18 USC § 2516 (listing the particular offenses).

¹⁴ 18 USC § 2516(1)(a) and (b).

An investigative technique that touches on and perhaps even extinguishes as many fundamental substantive rights as a wiretap can only be authorized by a small set of high-level people who have the experience, training, and judgment to evaluate and balance competing concerns of law and policy.¹⁵ By contrast, the proposed amendment allows a hacking warrant to be demanded by any federal law enforcement officer authorized to seek a warrant or any attorney for the government, with no restriction that the officer or attorney must even be an employee of the Government or have any particular authority, skills, training, or special competence. According to 28 CFR part 60, this includes officers with the Bureau of Sport Fisheries and Wildlife and the DC Metropolitan Police Department, among many others.¹⁶

This is especially worrisome in light of the imperative rather than permissive language of Rule 41(d)(1), which requires that “[a]fter receiving an affidavit or other information, a magistrate judge... *must* issue the warrant...”.¹⁷ This Committee should not authorize the hacking warrant in its present form in the first place. However, even if the proposed amendment is adopted in some form, it simply beggars belief that this Committee will allow a hacking warrant to be demanded in an *ex parte* process by such a broad range of potential applicants having no required competence in the myriad legal, technical, and policy issues that such a warrant raises.

If the conditions that ensure an appropriate balance between the desires of the Government and the needs and rights of the citizens are met, a wiretap order may be requested and issued. At that point, rules that ensure that a duly authorized wiretap is used correctly become operative. Wiretap processes include provisions that the Government “accomplish the interception unobtrusively and with a minimum of interference”¹⁸ and that procedures be established so that the seizure is done in a way that will “minimize the interception of [information] not

¹⁵ In Title III of the Omnibus Crime Control and Safe Streets Act (18 USC § 2516(1)), Congress required that requests for wiretaps be approved by a very small set of high-level people limited to the Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General.

¹⁶ Although it is generally clear who is or is not allowed to seek warrants under Rule 41, there is an ambiguity that makes it difficult to determine whether the proposed amendment would allow the National Zoological Park Police to demand a nationwide hacking warrant. They definitely do not get to request wiretaps.

¹⁷ Rule 41(d)(1), emphasis added.

¹⁸ 18 USC § 2518(4).

otherwise subject to interception...”¹⁹. Where there is substantial cost to the owners of the facilities used in wiretapping, the applicable rules provide that the owners “shall be compensated therefor by the applicant for reasonable expenses incurred.”²⁰ By contrast, the proposed amendment simply authorizes “remote access to search... and to seize” information, and then walks away with not so much as a thought given to necessary safeguards on the means of the access, search, or seizure. This whatever-happens-dude! approach of the proposed amendment compares extremely unfavorably, even unprofessionally, with the thoughtfully crafted procedures around a wiretap.

We citizens rely on our computers to do our jobs, pay bills, store irreplaceable information, and otherwise perform tasks indispensable to our everyday lives. Even transient loss of access to a computer or loss or corruption of data due to hacking by the Government can lead to job loss, the consequences of unpaid bills, and the loss of irreplaceable information. It is simply unacceptable that the Government would be allowed to not only hack access to the most private and intimate areas of our lives, but to do it with neither thought nor care for the interference, damage, and costs inflicted in the process.²¹ The proposed amendment cannot be approved without adding the proven existing procedures and safeguards that now guide wiretapping. This includes requirements for non-interference or minimum interference with target computers, data, networks, and other facilities; minimization of seized data to include no more than what is legitimately necessary for a specific investigation; and compensation for monetary and non-monetary costs imposed by the Government on others.

¹⁹ 18 USC § 2518(5)

²⁰ 18 USC § 2518(4).

²¹ The risks to data accessed, read, and stored by the Government are not merely speculative. The Government has repeatedly demonstrated that it cannot even protect its own data (<http://www.washingtonpost.com/news/morning-mix/wp/2014/07/09/report-chinese-hacked-into-the-federal-governments-personnel-office/>) even when the data in question is as important as nuclear secrets (<http://www.nytimes.com/2000/06/13/us/nuclear-secrets-reported-missing-from-los-alamos.html>). Once the Government gets data, it cannot seem to figure out how to access it reliably (<http://www.nbcnews.com/news/us-news/irs-says-it-lost-lois-lerner-emails-tea-party-probe-n131101> and <http://www.nbcnews.com/news/us-news/irs-says-it-lost-lois-lerner-emails-tea-party-probe-n131101>). In other words, even if the Government did treat the hacked computers and data of its citizens as carefully as it treats its own computers and data, including its most highly prized and protected computers such as those related to nuclear weapons, there is still an unacceptable likelihood that citizen computers and data will be compromised in myriad ways.

A consistent set of processes and procedures designed by professionals is required before nationwide hacking warrants can be authorized to permit the Government hackers to take our data.

IV. Summary

The universal hacking warrant that the proposed amendment would create is extremely powerful and has obvious potential hazards to the civil liberties of the citizens against whom it will be deployed. Therefore, it is necessary to make sure that systems and procedures are set up so that collateral damage to innocents is limited.

First, the proposed amendment must do more to safeguard the rights of those who have no involvement in a crime other than being unfortunate enough to host a virus on their machines. There needs to be a recognition that a criminal who breaks into someone's computer does not thereby waive the computer owner's reasonable expectation of privacy in the contents of the computer. Before a hacking warrant can issue, there should be a showing that the owner of the computer has some knowledge or involvement in the crime being investigated. If not, the extent to which any information seized from the computer should be sharply limited, preferably to zero.

Second, the bare fact that a computer conceals its location or the location of its media or information should not be enough to enable a hacking warrant. If the rights of the innocent computer owner were better protected as summarized above then it might be a different story, but the combination of a trivially-met standard to show probable cause about the contents of a computer together with a concealment condition that is met by almost every computer in the United States makes it far too easy to get such a powerful warrant.

Finally, the hacking warrant is very powerful, at least as powerful as a wiretap in many circumstances, and so the procedures and safeguards that accompany it must be as protective as those associated with wiretap.

I thank the Committee for considering this comment.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9g-w7jf
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0051](#)

Comment from CRWG Staff, Clandestine Reporters Working Group, LLC

Submitter Information

Name: CRWG Staff

Organization: Clandestine Reporters Working Group, LLC

General Comment

We are afraid the proposed amendment to Rule 41(b) (authority to issue a warrant) would revert our tradition of probable cause for search and seizures back to the distorted theme that any "secret" or "hidden" activity is ipso facto "illicit" activity. A secret meeting becomes cause for suspicion because it is secret, which is a stretch of the State's arm into citizens' lives based on their decisions to use certain privacy methods.

Attachments

crwg-lg-COLOR-WEB-LLC-medium



CLANDESTINE REPORTERS

March 16-17, 2015

WORKING GROUP LLC

Page 464 of 596

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9g-dout
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0052](#)

Comment from Andrew Gordon, NA

Submitter Information

Name: Andrew Gordon

Organization: NA

General Comment

The 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. With the vast resources available to many, including our own government, in order pry into the lives of anyone at a whim had ushered in a state in which many feel it necessary to protect what they do and say online. Taking precautions in order to protect oneself online should never be assumed that one is conducting in illegal activity in which law enforcement is granted a warrant.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9u-rgjd
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0053](#)

Comment from Ahmed Ghappour

Submitter Information

Name: Ahmed Ghappour

Organization: N/A

General Comment

See Attached

Attachments

Ghappour.Rule41.Comment

MEMORANDUM

TO: Members of the Advisory Committee on Criminal Rules
FROM: Ahmed Ghappour, UC Hastings College of the Law¹
DATE: February 17, 2014
RE: **Comment on the Proposed Amendment to Rule 41**

Dear Members of the Committee,

Thank you for the opportunity to submit comments on the proposed amendments to the Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure.

This comment focuses on the first prong of the proposed amendment to Rule 41, which would permit domestic law enforcement agencies to hack into computers of people attempting to protect their anonymity on the Internet. While the Department of Justice has explicitly stated that the amendment is not meant to give courts the power to issue warrants that authorize searches in foreign countries, the practical reality of the underlying technology means doing so is almost unavoidable.² As such, the proposed amendment results in an enlargement of the substantive right of law enforcement to conduct extraterritorial investigative activities without the consent of the encroached-upon foreign country. Because the Federal Rules of Criminal Procedure are limited to regulating procedure (and *not* expanding substantive powers), the proposed amendment exceeds judicial rulemaking authority and should not be adopted.

The comment proceeds in five parts. Part I provides a brief overview of the hacking techniques that would be permitted under the proposed amendment. Part II argues that these techniques will necessarily result extraterritorial cyber operations. Part III contends that extraterritorial law enforcement hacking without foreign country consent comprises a radical shift in how domestic law enforcement operates abroad. Part IV argues that this constitutes an enlargement of law enforcement's substantive authority to conduct investigative activities overseas. Part V recommends against adoption of the amendment, and proposes a number measures to minimize the encroachment on other states' sovereignty, leaving open the possibility for diplomatic overtures.

¹ Affiliation listed for identification purposes only. This Comment is based on a prior publication by the same author. See Ahmed Ghappour, Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance, JustSecurity (Sept 16, 2014), <http://justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/>

² See Letter from Mythili Raman, Acting Assistant Att'y Gen. of DOJ's Crim. Div., to Hon. Reena Raggi, Advisory Committee on Crim. Rules Chair (Sept. 18, 2013) (Raman Letter).

I. Network Investigative Techniques

Broadly, the term “Network Investigative Techniques” (“NITs”) describes a method of surveillance that entails “hacking,” or the remote access of a computer to install malicious software (“malware”) without the knowledge or permission of the owner. Once installed, malware remotely controls the target computer.

Malware can cause a computer to perform any variety of tasks. For example, some techniques can cause the computer to covertly upload files, photographs and stored e-mails to an FBI controlled server,³ and other techniques may use a computer’s camera and microphone to gather images and sound at any time the FBI chooses. Other NITs can even take over⁴ computers that associate with the target, for instance, by causing malicious code to be deployed onto any computer that visits a particular webpage hosted by the target.⁵

Network Investigative Techniques are especially handy in the pursuit of targets on the anonymous Internet—defined for the purposes of this Comment as those using Tor, a popular and robust privacy software, in order to obscure their location (and other identifying information),⁶ and to utilize so-called “hidden” websites on servers whose physical locations are theoretically untraceable.⁷ Knowledge of a target’s location is operationally paramount to the execution of existing search and seizure techniques, particularly where third party assistance is not available.

Since Network Investigative Techniques work by sending surveillance software over the Internet, the physical location of the target computer is not essential to the execution of the search.⁸ Indeed, the DOJ proposal is justified as the only reasonable

³ See Craig Timberg & Ellen Nakashima, *FBI’s Search for ‘Mo,’ Suspect In Bomb Threats, Highlights Use of Malware for Surveillance*, WASHINGTON POST (Dec. 6, 2013), http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html.

⁴ See Exhibit 4: Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, WIRED (Aug. 8, 2014) http://www.wired.com/2014/08/operation_torpedo/.

⁵ *Id.*

⁶ See e.g., TOR, www.torproject.org (last visited Oct. 28, 2014).

⁷ See TOR: HIDDEN SERVICE PROTOCOL, www.torproject.org/docs/hidden-services.html.en (last visited Oct. 28, 2014).

⁸ See Report of Advisory Comm. on Crim. Rules from Hon. Reena Raggi, to Hon. Jeffrey S. Sutton Comm. on Rules of Practice and Procedure Chair (May 5, 2014).

way to confront the use of anonymizing software, “because the target of the search has deliberately disguised the location of the media or information to be searched.”⁹

II. As Proposed, Rule 41(b)(3) Would Permit Extraterritorial Searches.

The proposed amendment alters a jurisdictional limitation in the current version of Rule 41(b)(1) that prevents a judge from issuing a warrant unless the target is known to be located within her district.¹⁰

(6) a magistrate judge with authority in any district where activities related to 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 of that district* if (A) the district where the media or information is located has been concealed through technological means¹¹

The amendment mirrors language setting out the jurisdictional scope of terrorism investigations under Rule 41(b)(3) (emphasized above), but applies to investigations for *general crimes*.¹² As for extraterritorial hacking, the DOJ commentary explicitly states that the proposal does not seek power to extend search authority beyond the United States:

In light of the presumption against international extraterritorial application, and consistent with the existing language of Rule 41(b)(3), this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries.¹³

Yet the commentary also articulates a standard of searches that “are within the United States or where the location of the electronic media is unknown.”

⁹ *Id.*

¹⁰ See Fed. R. Crim. P. 41(b).

¹¹ F.R.Cr.P. Rule 41(b)(6)(A) (proposed) (emphasis added).

¹² See Memorandum from Jonathan J. Wroblewski, Dir. Office of Pol’y & Legis. To Judge John F. Keenan, Subcomm. On Rule 41 Chair (Jan. 17, 2014) (“The Department’s proposal is intended to clarify that the issuance of such a warrant is proper in other criminal investigations as well.”)

¹³ See Raman Letter.

Under this proposed amendment, law enforcement could seek a warrant either where the electronic media to be searched are within the United States or where the location of the electronic media is unknown. In the latter case, should the media searched prove to be outside the United States, the warrant would have no extraterritorial effect, but the existence of the warrant would support the reasonableness of the search.¹⁴

The latter standard is a significant loophole in the DOJ's own formulation of the approach, particularly given the global nature of the Internet. For instance, over 85% of computers¹⁵ directly connecting to the Tor network are located *outside* the United States. And since (according to the DOJ) each computer's "unknown location" is virtually indistinguishable from the next, *any* law enforcement target pursued under this provision of the amendment may be located overseas.

III. Radical Departure From Current Exercise of Law Enforcement Functions Overseas

The FBI's extraterritorial activities have generally fallen in line with international law, where it is considered an invasion of sovereignty for one country to carry out law enforcement activities within another country without that country's consent.¹⁶ To that end, the FBI avoids acting unilaterally—relying instead on the United States' diplomatic relations with other countries and the applicability of any treaties, seeking permission from the host country before deploying personnel, and requesting assistance from local authorities when possible.

The DOJ proposed amendment will result in significant departures from the FBI's customary practice abroad: overseas cyber-operations will be unilateral and invasive; they will not be limited to matters of national security, nor will they be executed with the consent of the host country or with meaningful coordination with internal agencies. Instead, under the DOJ's proposal, unilateral state action will be the rule, not the exception whenever an anonymous target "prove[s] to be outside the United States." The reason is simple: without knowing the target's location *before* the fact, there is no way to provide notice or obtain consent from a host country until *after* a DOJ interference.

Without advanced knowledge of the host country, law enforcement will not be able to adequately avail itself to protocols currently in place to facilitate foreign

¹⁴ *Id.*

¹⁵ See Tor Metrics: Direct Users by Country, <https://metrics.torproject.org/users.html> (last visited Oct. 28, 2014).

¹⁶ See *infra* Part IV.

relations. For example, the FBI will not be able to coordinate with the Department of State before launching a Network Investigative Technique. This puts the US in a position where its law enforcement entity may encroach on the territorial sovereignty of foreign states without coordination with the agency in charge of its foreign relations.

The encroachments that result will be public—bound to arise in the event of a criminal trial. In 2002, for example, Russia’s Federal Security Service (FSB) filed criminal charges against an FBI agent for “illegally accessing” servers in Chelyabinsk, Russia in order to seize evidence against Russian hackers later used in their criminal trial.¹⁷ Evidently, the FSB was tipped off to the fact when the defendants were indicted in Seattle, Washington. Reportedly, an FBI press release stated that this was “the first FBI case to ever utilize the technique of extraterritorial seizure of digital evidence.” The FBI accessed the overseas server through the web, using login information it obtained from a suspect in custody.¹⁸

IV. The Proposal Results in an Enlargement of the Substantive Right of Law Enforcement to Conduct Extraterritorial Investigative Activities

Although the proposed Committee Note purports to leave “constitutional questions” to be addressed in future case law, in practice the amendment will enlarge the government’s substantive power to conduct searches. The Restatement (Third) of Foreign Relations Law notes that although a state is generally free to enforce its criminal law within its own territory,¹⁹ “a state’s law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given

¹⁷ See Mike Bruner, *FBI Agent Charged With Hacking*, NBC NEWS (Aug. 15, 2014).

¹⁸ See Press Release, U.S. Dep’t of Justice, *Russian Computer Hacker Convicted by Jury* (Oct. 10, 2011), available at: <http://www.justice.gov/criminal/cybercrime/press-releases/2001/gorshkovconvict.htm>.

¹⁹ RESTATEMENT (Third) of Foreign Relations Law § 432(1). The Restatement notes some limitations on the ability of a state to enforce laws even within *its own* territory, which may further complicate matters. It states:

A state may enforce its criminal law within its own territory through the use of police, investigative agencies, public prosecutors, courts, and custodial facilities, provided (a) the law being enforced is within the state’s jurisdiction to prescribe; (b) when enforcement is through the courts, the state has jurisdiction to adjudicate with respect to the person who is the target of enforcement; and (c) the procedures of investigation, arrest, adjudication, and punishment are consistent with the state’s obligations under the law of international human rights.

Id.

by duly authorized officials of that state.”²⁰ The comments to the Restatement make the requirement of host nation consent clear:

It is universally recognized, as a corollary of state sovereignty, that officials of one state may not exercise their functions in the territory of another state without the latter’s consent. Thus, while a state may take certain measures of non-judicial enforcement against a person in another state, ...its law enforcement officers cannot arrest him in another state, and can engage in criminal investigation in that state only with that state’s consent. Within a state’s own territory, the rules governing arrest and other steps in criminal law enforcement generally apply regardless of the nationality, residence, or domicile of the person accused or investigated, subject only to defined exceptions for persons enjoying diplomatic or consular immunity . . . and to the obligation to observe basic human rights²¹

When a state’s sovereignty is encroached upon, its response depends on the nature and intensity of the encroachment. In the context of cyberspace, states (including the United States) have asserted sovereignty over their cyber infrastructure, despite the fact that cyberspace as a whole, much like the high seas or outer space, is considered a “global common” under international law.

To be sure, the FBI’s known arsenal of Network Investigative Techniques, if executed properly, do not rise to the level of a cyber “armed attack”—as defined in Article 51 of the UN Charter—for which a use of (cyber or kinetic) force in response would be permissible. Doing so would require the attack be reasonably expected to cause injury or death to persons or damage or destruction to objects of a significant scale. Forceful responses to cyber attacks below that threshold are only permissible with UN Security Council authorization. Moreover, and as a general matter, there are no explicit prohibitions on cyber espionage (clandestine information gathering by one state from the territory of another) in international law.

²⁰ *Id.* § 432(2).

²¹ *Id.* § cmt b. The comment also notes that if a state’s law enforcement officials exercise their functions in the territory of another state without host nation consent, the offended state is entitled to protest and, in certain cases, may even receive reparation from the offending state. *Id.* § cmt c. While states are afforded a certain degree of latitude in exercising prescriptive and adjudicative jurisdiction, restrictions on enforcement jurisdiction are markedly constrained and deemed to violate the principle of nonintervention.

As such, law enforcement hacking (as with other forms of espionage by organs of the State) will probably be regulated by the violated state's domestic criminal law, counterespionage, or countermeasures.²² Indeed, given the public nature of the U.S. criminal justice system, it is hard to see how the FBI will avoid risk of prosecution (similar to that in the Chelyabinsk incident) if the DOJ proposal is approved.

Still, the Federal Rules of Procedure are limited to regulating procedure,²³ and may not "abridge, enlarge or modify any substantive right."²⁴ Indeed, federal courts adopting rules are not free to extend or restrict jurisdiction conferred by statute.²⁵ Here, adoption of the proposed amendment to Rule 41 would exceed judicial rulemaking authority because it enlarges the substantive right of law enforcement to conduct extraterritorial investigative activity by authorizing the extraterritorial exercise of law enforcement functions without first obtaining consent of the foreign country.

V. Recommendations

In light of the above, I would be hesitant to amend Rule 41 at this time without first having a thorough discussion of the potentially far-reaching consequences of the change. The technologies involved are rapidly developing and poorly understood, as are the existing international legal norms that apply to them. It is critical that these issues be approached with comprehensive deliberation (between technologists, policy makers and lawyers) that looks beyond the operational frame.

Nonetheless, if we do amend the Rule, we should certainly take steps to minimize the encroachment on other states' sovereignty, leaving open the possibility for diplomatic overtures. To that end, the Rule should require Network Investigative Techniques to return only country information at first, prompting the executing FBI agent to utilize the appropriate protocols and institutional devices.

²² See *Draft Articles of State Responsibility*.

²³ *Sibbach v. Wilson & Co.*, 312 U.S. 1, 10 (1941).

²⁴ 28 U.S.C. § 2072(b).

²⁵ *Willy v. Coastal Corp.*, 503 U.S. 131, *rehearing denied* 504 U.S. 935; *Collins v. Bolton*, 287 F.Supp. 393 (N.D.Ill. 1968)(Delegation of rule-making power to Supreme Court under this section does not authorize expansion or contraction of jurisdiction conferred by statute); *Compare Hart v. Knox County, Tenn.*, 171 F.2d 45 (C.A.6 1948)(The Supreme Court had authority under former §§ 723b and 723c of this title to promulgate amended rule 73(a) which requires that in an action in which an agency of the United States is a party, the time permitted for appeal from a district court to court of appeals is 60 days from entry of judgment appealed, and rule does not affect substantive rights but relates to practice and procedure and the rule neither enlarges or abridges the jurisdiction of the court of appeals but merely implements its jurisdiction over the subject matter which Congress has conferred by providing the procedure for review.).

The Rule should also insure that Network Investigative Techniques are used sparingly and only when necessary by requiring a showing similar to that required by the Electronic Communications Privacy Act, namely, that less intrusive investigative methods have failed or are reasonably unlikely to succeed.²⁶ Another way to do this might be to narrow the class of potential targets, from targets whose location is “concealed through technological means” to those whose location is not “reasonably ascertainable” by less invasive means.

The Rule should also limit the range of hacking capabilities it authorizes. “Remote access” should be limited to the use of constitutionally permissible methods of law enforcement trickery and deception that result in target-initiated access (e.g., requiring the target to click a link contained within a deceptive email in order to initiate delivery and installation of malware). “Search” capabilities should be limited to monitoring and duplication of data on the target (e.g., copying a hard drive or monitoring keystrokes).

The Rule should not authorize drive-by-downloads that infect every computer that associates with a particular webpage, the use of weaponized software exploits in order to establish “remote access” of a target computer, or deployment methods that risk indiscriminately infecting computer systems along the way to the target. Nor should the Rule authorize a “search” method that requires taking control of peripheral devices (such as a camera or microphone).

There are other suggestions, of course. As it stands, the proposed amendment allows the FBI to use a wide array of invasive (and potentially destructive) hacking techniques where it may not be necessary to do so, against a broad pool of potential targets that could be located virtually anywhere.

Thank you got your consideration of these comments.

Respectfully,

Ahmed Ghappour
Visiting Assistant Professor
Director, Liberty, Security & Technology Clinic
UC Hastings, College of the Law
200 McAllister St.
San Francisco, CA 94102

²⁶ See e.g., 18 U.S.C. § 2518(1)(c).

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8h9b-j514
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0054](#)

Comment from Brett Remsen, NA

Submitter Information

Name: Brett Remsen

Organization: NA

General Comment

This idea is shit.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8hd3-uy2v
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0055](#)

Comment from David Bitkower, U. S. Department of Justice

Submitter Information

Name: David Bitkower

Organization: NA

General Comment

See Attached

Attachments

Memo FINAL to Judge Raggi 102014



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

October 20, 2014

MEMORANDUM

TO: The Honorable Reena Raggi
Chair, Advisory Committee on Criminal Rules

FROM: David Bitkower^{DB}
Deputy Assistant Attorney General

SUBJECT: Response to Post on Proposed Amendment to Rule 41

The Committee has asked the Department to respond to a September 16, 2014 post by Professor Ahmed Ghappour on the *Just Security* blog arguing that the Department's proposed amendment to Rule 41 would expand the extraterritorial surveillance authorities of the FBI.¹ We thank the Committee for this opportunity, and offer the following response.

The post's central premise is that the proposal expands the FBI's authority to access computers outside the United States. That premise is incorrect. The proposed amendment has no effect on the FBI's authorities outside the United States. As the Department explained in its September 18, 2013 letter to the Committee, the proposed amendment "does not purport to authorize courts to issue warrants that authorize the search of electronic storage media that is located in a foreign country or countries." Indeed, the amendment 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. Rather, with respect to anonymizing technology, it would only ensure that a judge is available to hear a search warrant application in a narrow category of cases where, under Rule 41's current venue provisions, that might not otherwise be the case because the nature of modern Internet crimes has frustrated the existing warrant process.

Overseas Authorities and Rule 41

In fact, with limited exceptions, the FBI's overseas authorities have nothing to do with Rule 41. In cases where the Fourth Amendment's warrant requirement applies, the procedures

¹ See <http://justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/>.

for obtaining a warrant in Rule 41 effectively limit the FBI's ability to conduct searches and seizures. But the Fourth Amendment's warrant requirement does not apply to searches outside of the United States, even searches of United States persons. Instead, such searches are evaluated under the Fourth Amendment's reasonableness requirement. *See United States v. Stokes*, 726 F.3d 880, 890-93 (7th Cir. 2013); *In re Terrorist Bombings*, 552 F.3d 157, 170-71 (2d Cir. 2008); *see also United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990) (describing a warrant issued by United States magistrate as "a dead letter outside the United States"). Because Rule 41 warrants are not required in the first place, the current venue limitations in Rule 41 do not limit the FBI's authority to conduct extraterritorial searches. A modification of those venue limitations, therefore, would not expand that authority.

As discussed in the Department's proposal, it is possible that a defendant may move to suppress evidence obtained from the search of computer media that proves to be outside the United States. In such a case, the government could point to the magistrate's determination of probable cause as part of its argument that the extraterritorial search was reasonable under the Fourth Amendment. But the issuance of the warrant in such a case would not have authorized any action the FBI was not already permitted to take under its current extraterritorial authorities.

Practical Considerations

Beyond its argument about expanded legal authorities, the post also makes the practical claim that the proposal will result in "overseas cyber operations [that are] unilateral and invasive." This argument is also incorrect. Nothing in the proposal changes the government's foreign policy considerations, which are also not governed by Rule 41, one way or the other. In fact, the Department of Justice (including the FBI) has long maintained internal protocols for handling investigations with potential overseas effects. But these practices are not mandated by Rule 41 – rather, the Department employs them because they are good policy. There is thus no basis to argue that the Department's practices in this regard would change if the proposed amendment to Rule 41 is adopted.

There may be cases in which it is impossible, without undertaking a remote search, to determine whether a computer that is involved in criminal conduct is located in the United States or abroad. This may be the case even though the conduct is in flagrant violation of American law. For example, pedophiles involved in the ongoing sexual exploitation of children, including American children, often use "hidden," or anonymized, websites to sell or exchange the child pornography that they have produced. In such cases, law enforcement authorities may be confronted with the choice of undertaking a remote search to locate the server that is hosting the website, potentially in another country – or permitting harmful criminal conduct to continue unabated. These are, unfortunately, precisely the cases in which international cooperation is least likely to be available, because there are no identifiable "local authorities" to ask for help. This problem predates our proposal and will continue to exist even if our proposal is adopted: as noted above, Rule 41 does not currently limit the FBI's authority to remotely access a computer outside the United States. What our proposal would accomplish is untying the hands of law enforcement when it is not yet known whether the Fourth Amendment requires a warrant because it is unknown whether the media is in the United States – and it accomplishes that by ensuring that a judge is available to hear the warrant application.

Additional Restrictions Are Unnecessary and Would Be Counterproductive

The Committee should reject the post's suggestions to impose unnecessary and unworkable restrictions on remote search authority in Rule 41, such as a requirement to search only for "country information." Restrictions on seizing evidence for which the government establishes probable cause are inconsistent with the role of a magistrate judge considering a warrant application. To the extent the computer media is in the United States, the scope of what can be seized should be governed by the same probable cause and particularity standards whether the data is taken from the computer by walking up to it or by connecting to it remotely. And to the extent there is a possibility that the computer media is not in the United States, and hence there is a theoretical foreign policy concern, the Federal Rules of Criminal Procedure are not the right mechanism to balance the foreign policy implications (if any) of proceeding with a search against the risk of conducting multiple searches of the same media, or of not searching at all. For example, in a given case it may be advisable to search only for location information; but in another case, there may be only one opportunity to employ a remote search, and a "location information-only" rule could thwart the investigation.

Second, the Committee should reject the recommendation that Rule 41 include a "necessity" requirement like that of the Wiretap Act for remote search warrants. Under this requirement, to obtain a warrant for a remote search, the government would first be required to demonstrate that other investigative methods have failed or are unlikely to succeed. But it would not be wise to use Rule 41 to enact a policy preference favoring, for example, physical intrusions into residences over remote searches of computers. Nor, as discussed above, do we think it would be consistent with the institutional advantages of the different branches of government to embed into the Federal Rules a foreign policy decision that requires magistrate judges to study and consider the international relations effects of various potential investigative steps – or investigative inaction, for that matter. *Cf. Zurcher v. Stanford Daily*, 436 U.S. 547, 552, 559 (1978) (reversing a district court ruling that had essentially adopted a necessity requirement for warrants, noting that "[t]he Fourth Amendment has itself struck the balance between privacy and public need" and rejecting the district court's attempt to "strike a new balance by denying the search warrant . . . on the theory that [a subpoena] is a less intrusive alternative"). Rather, courts should be authorized to issue warrants when the government satisfies the Fourth Amendment's probable cause and particularity requirements.

Finally, prohibiting the use of certain types of software to conduct remote searches would be out of place in a federal rule of procedure. As the Supreme Court has explained, "the details of how best to proceed with the performance of a search authorized by warrant" are "generally left to the discretion of the executing officers." *Dalia v. United States*, 441 U.S. 238, 257 (1979). There is no compelling reason for the Committee to limit such discretion, which must be employed on a case-by-case basis, and which of course remains subject to judicial review for reasonableness. *Id.* at 258; *see also United States v. Schesso*, 730 F.3d 1040, 1050 (9th Cir. 2013) (holding that magistrate judges may impose protocols on warrant execution and recognizing that the protocols "must be determined on a case-by-case basis").

Conclusion

The Department looks forward to further engagement on this issue during the public comment period. Please let us know if there is any further information we can provide to you.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8hd8-6big
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0056](#)

Comment from David Bitkower, U. S. Department of Justice

Submitter Information

Name: David Bitkower

Organization: NA

General Comment

See Attached

Attachments

December 2014 Rule 41 Memo 122214



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

December 22, 2014

MEMORANDUM

TO: The Honorable Reena Raggi
Chair, Advisory Committee on Criminal Rules

FROM: David Bitkower *DB*
Deputy Assistant Attorney General

SUBJECT: Response to Comments Concerning Proposed Amendment to Rule 41

The Committee has asked the Department to address certain issues raised by commenters who presented testimony at a public hearing on November 5, 2014, regarding the Department's proposed amendment to Rule 41. We thank the Committee for the opportunity to address these issues.

As we have stated previously, the proposed amendment would ensure that a court has jurisdiction to issue a search warrant in two categories of investigations involving modern Internet crime: cases involving botnets and cases involving Internet anonymizing techniques. The proposal would do so by clarifying Rule 41's current venue provisions in these two circumstances. The proposal would not authorize the government to undertake any search or seizure or use any remote search technique not already permitted under current law. Certain of the comments received by the Committee have contested this assertion, but as discussed below, many of those comments appear to be misreading the text of the proposal or misunderstanding current law. We welcome the opportunity to clarify how the proposal would operate as a matter of law and practice.

First, we address concerns that warrants authorizing remote searches would violate the Fourth Amendment's particularity requirement. As with all search warrant applications, such concerns must ultimately be resolved through judicial determination on a case-by-case basis. We nevertheless explain here why we believe that remote search warrants can satisfy the Particularity Clause. To illustrate, we describe three investigative scenarios in which warrants for remote searches might be used, and we provide specific language that might be used for the "place to be searched" and "things to be seized" components of remote search warrants in these scenarios.

Second, we address concerns about the notice requirement of the proposed rule. Like the Rule 41 requirement for physical searches, the proposed amendment 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.

Third, we explain that the proposed amendment has no effect on the requirements of Title III. 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.

Fourth, we discuss the “concealed through technological means” requirement for obtaining a warrant pursuant to the proposed venue provision for remote searches. This requirement provides an appropriate and workable standard for obtaining a warrant for a remote search in cases involving Internet anonymizing technology. The 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.

Fifth, we note that the 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, just as it is careful to avoid injury to persons or damage to property in the far more common scenario of executing physical warrants. Although there is currently no Department regulation that specifically applies to the remote searches that would be conducted under the proposed amendment, such searches are scrutinized carefully, and they may be subject to other internal Department regulations depending on the circumstances.¹

Before addressing the substance of the comments in detail, we note that the commenters’ objections regarding issues such as particularity and notice do not relate to venue. Rather, they are general objections to obtaining and executing search warrants using certain remote search techniques. These objections are misplaced here because the proposed amendment is solely about the appropriate venue for applying for such warrants. The existing rules already allow the government to obtain and execute such warrants when the district of the targeted computer is known. Thus, the issue before the Committee is not whether to allow warrants to be executed by remote search; it is whether such warrants should as a practical matter be precluded in cases involving anonymizing technology due to lack of a clearly authorized venue to consider warrant applications. Finally, we note that none of the commenters who expressed opposition to the proposal offered any substantive alternative solution to provide venue for a search warrant application when the district in which the targeted computer is located is unknown.

Particularity requirement for remote search warrants

We believe that search warrants authorizing remote searches can satisfy the Fourth Amendment’s particularity requirement. A number of magistrate judges have issued warrants for remote searches, and those judges have been satisfied that the warrants fulfilled the

¹ This letter does not address potential international issues associated with the proposed amendment, as those concerns were previously addressed by the Department in a letter dated October 20, 2014.

requirements of the Fourth Amendment.² As an initial matter, however, we note that the law regarding the particularity requirement for remote searches cannot be resolved by the Rules Committee; it must develop, as it does for all search warrants, through judicial resolution of specific, concrete cases. As the Committee Note to the proposed amendment states, “[t]he 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.”

Nevertheless, because several commenters raised concerns about the particularity of remote search warrants, we discuss how remote search warrants can satisfy the Fourth Amendment’s particularity requirement.³ In addition to discussing relevant doctrine regarding the Fourth Amendment’s particularity requirement, we will describe three investigative scenarios and explain how warrants can be drafted in those scenarios to satisfy the Fourth Amendment.

The particularity requirement of the Fourth Amendment demands that “warrants must particularly describe the things to be seized, as well as the place to be searched.” *Dalia v. United States*, 441 U.S. 238, 255 (1979) (internal quotation marks omitted); *see also United States v. Grubbs*, 547 U.S. 90, 97 (2006).⁴ The particularity requirement “makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another.” *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (quoting *Stanford v. Texas*, 379 U.S. 476 (1965)). “As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927).

Describing the information to be seized pursuant to a remote search warrant need not be complicated. The warrant specifies evidence of crime that can be obtained through access to the targeted computer. For warrants in investigations of crime involving use of Internet anonymizing technology, this evidence will usually be information that helps to identify the suspect. For example, the MAC address and IP address of a computer help identify the computer and its owner.

² For example, in one recent investigation, the government sought a search warrant to help identify computers used to access a child pornography hidden service on Tor. The magistrate judge issued a warrant for the search; in the subsequent criminal prosecution, the district court denied a motion to suppress challenging the warrant. *See United States v. Cottom*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #155) (denying suppression motion), (Doc #122, Attachment 1) (search warrant).

³ Commenters including the Center for Democracy and Technology (“CDT”) and the ACLU recommend that Congress address whether to authorize warrants for remote searches. *See* CDT Memorandum at 11; ACLU Memorandum at 28. This recommendation suggests that these commenters agree that such searches can, in principle, comply with the Fourth Amendment; otherwise any Congressional action would be futile.

⁴ The scope of the particularity requirement does not extend to describing how a warrant will be executed. The Supreme Court has explained that “[n]othing in the language of the Constitution or in this Court’s decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed.” *Grubbs*, 547 U.S. at 98 (quoting *Dalia*, 441 U.S. at 255).

Because the physical location of the place to be searched by remote access is typically unknown, remote search warrants usually describe the place to be searched through some other means designed to specify the particular account or computer that officers have probable cause to search. For example, when investigators have the ability to send an email to the suspect, the place to be searched could be described as the computer used to access and open the email sent to the suspect.

Some commenters argue that a search warrant can satisfy the Fourth Amendment's particularity requirement only if it specifies the physical location of the computer to be searched. This argument is mistaken: the Supreme Court has made clear that the particularity requirement does not preclude use of warrants where the purpose of the search is to discover the location of the place to be searched. In *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court held that a warrant for a tracking device could satisfy the Fourth Amendment despite the fact that the purpose of the warrant was to determine the place to be searched:

The Government contends that it would be impossible to describe the "place" to be searched, because the location of the place is precisely what is sought to be discovered through the search. . . . However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance.

Id. at 718. These same principles apply to warrants for remote searches. The government may satisfy the Fourth Amendment with respect to a remote search warrant by describing the computer or web server to be searched (for example, the computer that is used to access and open a particular email message, or the web server hosting a particular hidden web site), the circumstances that justify the search, the information that will be obtained through the search, and the time period during which the search may be conducted. None of these things require knowledge of the physical location of the object of the search.

The ACLU also objects that the "proposed amendment would allow police to remotely search many people's computers using a single warrant," *see* ACLU Memorandum at 21, but the law it cites regarding multi-location search warrants makes clear that such warrants may in fact comply with the Fourth Amendment. "A search warrant designating more than one person or place to be searched must contain sufficient probable cause to justify its issuance as to each person or place named therein." *Greenstreet v. County of San Bernardino*, 41 F.3d 1306, 1309 (9th Cir. 1994) (quoting *People v. Easley*, 671 P.2d 813, 820 (Cal. 1983)). Courts can address the extent to which this rule applies to remote search warrants in the usual manner, just as they would in the case of warrants for physical searches: through judicial resolution when the issue arises in specific cases. In any event, even if there were a rule requiring the use of a separate warrant for every location to be searched, the proposed amendment would not modify that rule. Rather, it merely provides a venue for a court to decide whether a warrant application satisfies the Fourth Amendment.

Particularity requirement: sample warrant language

To illustrate how remote search warrants can satisfy the Fourth Amendment, it is helpful to describe their use in several investigative scenarios. Here, we will discuss three scenarios: a drug trafficker using an email account offered through a Tor hidden service, a fraud scheme facilitated by email, and a child pornography group. For each, we will explain how two key elements of the warrant – the place to be searched and the items to be seized – can be drafted in compliance with the Fourth Amendment.

Warrant scenario 1: obtaining stored email content from a hidden email provider by using a username and password

It is worth noting at the outset that the proposal does not relate only to remote searches conducted through the use of special software or computer exploits. A warrant for a remote search under the proposed amendment could closely resemble a search warrant of the sort that is routinely issued by magistrate judges across the country. Suppose that in executing a Rule 41 warrant on the home of a drug trafficker, agents discover the user name and password for an email account hosted on a Tor hidden service that the target uses to advertise and sell drugs. Investigators would like to search the account for evidence, but they likely will not know the location of the server hosting the account, and they cannot serve the email provider with a standard email search warrant under 18 U.S.C. § 2703 as they would with a commercial service provider. Instead, investigators would like to access the email account themselves using the user name and password that they have discovered. Doing so will not require use of any special or otherwise sensitive software.

A warrant authorizing a search of the drug trafficker's email account will comply with the Fourth Amendment. First, the affidavit in support of the warrant can present facts sufficient to establish probable cause that the target has used the account in connection with his crimes and that there is reason to believe that the account will contain information related to that activity. Second, the search warrant will specify the place to be searched. For example, the warrant can state that the place to be searched is the "target account on the target computer," defined as "the account associated with [username] that is stored on the server hosting [the specified Tor email service]." The affidavit can also explain that investigators intend to log on to the account directly in order to execute the warrant. Third, the warrant will specify the information to be obtained from the account, such as particularly-described information that constitutes evidence of drug trafficking within a specified date range. Such a warrant will comply with the Fourth Amendment and would not present any novel particularity issues.

Warrant scenario 2: identifying a criminal using a web-based email account

Criminals frequently use web-based email accounts, such as Gmail, Yahoo, or Hotmail accounts, to send and receive communications related to their criminal activity. For example, a fraudster will want to use a seemingly "normal" email address to communicate with a potential victim. Investigators can typically determine the IP address that was used to access a web-based email account at a particular time by serving a subpoena on the email provider. But criminals can hide their true IP address from their service providers and the government through

anonymizing techniques such as use of a proxy server.⁵ In such circumstances, investigators may be able to use a Network Investigative Technique (“NIT”) to identify the criminal’s true IP address.

Suppose, for example, that investigators become aware that a fraudster is communicating with a victim through a web-based email account, and that the fraudster is trying to persuade the victim to wire him a large sum of money. In addition, investigators determine that the fraudster accesses his email account only using proxy servers. With the assistance of the victim, investigators can send an email containing a NIT from the victim’s email account to the fraudster’s email account. If the fraudster accesses the email, the NIT will cause the fraudster’s computer to send identifying information, such as the computer’s true IP address, to investigators.⁶

A warrant authorizing use of a NIT in such a manner can satisfy the Fourth Amendment. First, the affidavit in support of the warrant can present facts sufficient to establish probable cause that the fraudster is committing a crime, that he is using a computer to do so, and that the identity and location of the fraudster and the computer will constitute evidence. Second, the search warrant will specify what computer will be searched. For example, the warrant can state that the place to be searched is the “target computer,” defined as “the computer that accesses [the fraudster’s email account] and retrieves an email that will be sent to that account from [the victim’s email account] in furtherance of this warrant.” Third, the warrant will specify the information to be obtained from the computer. For example, the warrant could state that the information to be obtained is: “the target computer’s actual IP address, and the date and time that the NIT determines that IP address; and the target computer’s MAC address and host name.” This information would assist investigators in identifying the physical location and owner of the computer. Such a warrant will comply with the Fourth Amendment.

Warrant scenario 3: investigating members of a child pornography group

Many producers and traffickers of child pornography rely on Internet anonymizing techniques, in particular the Tor network, to hide from law enforcement. As an example, suppose that law enforcement becomes aware of a password-protected Tor website dedicated to the production, receipt, and distribution of child pornography. As explained on the publically-accessible part of the website and corroborated by an undercover agent’s attempt to access the site, an individual can only obtain a user account and password necessary to access the website by providing the site administrator with samples of newly created images of child pornography. Because of the strict rules governing access to the website, there is probable cause to believe that anyone who uses a password to access the site is engaged in the ongoing abuse of children and the production, distribution, and possession of child pornography. Investigators thus seek to

⁵ Frequently, criminals route their communications through proxy servers that openly advertise the fact that they do not maintain records.

⁶ This type of warrant is analogous to an anticipatory warrant to search the residence of a person who accepts a package containing contraband, even if the precise residence is not known at the time the warrant is obtained. *See, e.g., United States v. Dennis*, 115 F.3d 524, 528 (7th Cir. 1997) (anticipatory warrant to search whichever of two apartments belongs to the individual who accepts delivery or opens a particular package containing drugs).

identify the location of the individuals accessing the site. They intend to do so by sending a NIT to each computer used to log on to the website using a password during a specified time period. Each NIT will then send identifying information from each computer back to the investigators.

A warrant authorizing such searches can be written to comply with the Fourth Amendment. First, the affidavit in support of the warrant would set forth the facts described above, establishing probable cause that each computer used to access the website (or portion of the website) in question will contain evidence of a crime. Second, the search warrant authorizing the use of the NIT will specify the places to be searched. The warrant can state that the places to be searched are the “target computers,” which are “the computers used to log on to [the child pornography website] with a valid password during [specified time period] and to which a NIT will be sent pursuant to this warrant.” Third, the warrant will specify the information to be obtained. For example, the warrant can state that the information to be obtained is: “for each target computer, the actual IP address, and the date and time that the NIT determines that IP address; and the target computer’s MAC address and host name.”

The ACLU calls this technique a “watering hole attack” and suggests that it may violate the Fourth Amendment. *See* ACLU Memorandum at 22. The Department disagrees both with that label and with the legal conclusion.⁷ As discussed above, when investigators can establish probable cause to search multiple locations, the Fourth Amendment allows investigators to obtain a warrant to search them. *See, e.g., United States v. Johnson*, 26 F.3d 669, 692 (7th Cir. 1994); *Greenstreet*, 41 F.3d at 1309. And by the same token, if investigators cannot establish probable cause to search a particular location, then they will not be able to obtain a warrant to authorize the search of that location. Nothing in the proposed amendment would hold otherwise.

As these three hypothetical scenarios demonstrate, warrants executed by remote search can satisfy the Fourth Amendment. We do not doubt that one could also conjure up hypothetical instances in which a remote warrant would *not* satisfy the Fourth Amendment. But that is beside the point because the proposed amendment would not authorize such searches. What the proposed amendment would do is ensure that a court is available to determine whether a specific warrant application satisfies the Fourth Amendment or not.

Notice requirement for remote search warrants

The proposed amendment’s notice requirement mandates that when executing a warrant for a remote search, “the officer must make reasonable efforts to serve a copy of the warrant on the person whose property was searched or whose information was seized or copied,” and that

⁷ The term “watering hole” attack is generally used to describe a technique whereby criminal hackers implant a virus on a widely-used website and cause it to infect large numbers of users who may not be of interest to the hackers, in hopes that the virus will also infect a smaller number of users who are of specific interest to the hackers. *See, e.g.,* <http://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-hole-sites>. By contrast, the search described in this scenario is – and by definition must be – targeted based on probable cause. The ACLU also asserts in its comment that the FBI performed such a “watering hole attack” on a particular Tor-based server known as Freedom Hosting that “forc[ed] all of the Freedom Hosting sites to deliver malware to visitors, not just those sites that were engaged in the distribution of illegal content.” ACLU Memorandum at 15. This assertion appears to be based on Internet rumor.

“[s]ervice may be accomplished by any means, including electronic means, reasonably calculated to reach that person.” Commenter EPIC asserts that this amendment authorizes surreptitious searches without a showing of need for the delay, *see* EPIC Memorandum at 7, but EPIC is misreading the proposed rule. The proposed amendment, as a default matter, requires officers to make reasonable efforts to give notice of the warrant at the time the warrant is executed.

The proposed amendment does not modify the delayed-notice statute. If investigators seek to delay notice of a warrant executed by remote search, they will be required to follow the existing delayed-notice procedures and meet the existing delayed-notice standard of 18 U.S.C. § 3103a. Under that statute, in order to authorize delayed notice, the issuing court must find “reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial).” 18 U.S.C. § 3103a(b)(1). This standard will be the same for remote searches as it is for physical searches. In addition, a court cannot authorize the seizure of either physical evidence or electronic information pursuant to a delayed-notice warrant without a judicial finding of reasonable necessity. *See* 18 U.S.C. § 3103a(b)(2) (requiring that a delayed-notice warrant must prohibit “the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure”). Again, this provision treats “stored wire or electronic information” that will be obtained by a remote search in precisely the same manner as “any tangible property.” The Department has interpreted “seizure . . . of any stored wire or electronic information” in Section 3103a(b)(2) broadly to include the copying of information stored on a computer. Finally, unless a longer period of delay is justified by the facts of the case, Section 3103a will allow for an initial 30-day period of delayed notice for a remote search warrant, with possible extensions of up to 90 days each. *See* 18 U.S.C. § 3103a(b), (c).⁸

The Department anticipates that it will seek judicial approval to delay notice in many of the cases in which it seeks a warrant for a remote search. This is so because, as described above, such warrants will often be sought when investigators are trying to identify or locate an online criminal who is taking steps to avoid identification. Such circumstances will typically provide reasonable cause for delaying notice of the search, but notice will be delayed only where appropriate under existing rules. For example, in *United States v. Cottom*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #155) (denying motion to suppress), investigators invoked Section 3103a to delay notice of a remote search warrant through which they identified users of a Tor-based hidden service child pornography website. The court held that “the 30-day delayed notice, under the facts of this case, did not create any violation of Rule 41.” *Id.* at 8.

⁸ Under the proposed amendment, the rules for delaying notice for warrants for remote searches will be more demanding than the existing rules for delaying notice for tracking device warrants. For a tracking warrant, the government need not provide notice of the warrant for up to ten days after the tracking has ended, and no showing of need is required for that initial period of delay. *See* Fed. R. Crim. P. 41(f)(2)(C). Because tracking warrants can last for 45 days, *see* Fed. R. Crim. P. 41(e)(2)(C), notice of a tracking warrant can therefore be given 55 days after the initial search without any showing of need for the delay.

The proposed amendment requires officers to make “reasonable efforts” to provide notice of a warrant. This standard recognizes that in some cases – particularly cases in which the location of the computer has been concealed – the officer may be unable to provide notice of the warrant. For example, even after officers conduct a remote search, they may still lack sufficient information to identify or contact the owner of the searched computer. The “reasonable efforts” language recognizes that there may be unusual difficulty in providing appropriate notice in cases where the district in which the computer is located is unknown; by contrast, if the government can provide notice using reasonable efforts, the rule will require it to do so. As the Supreme Court stated in *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995), “[t]he Fourth Amendment’s flexible requirement of reasonableness should not be read to mandate a rigid rule of announcement that ignores countervailing law enforcement interests.” As with other notice issues under the Fourth Amendment, the reasonableness of the government’s efforts to provide notice must be evaluated on a case-by-case basis.

Finally, the proposed amendment requires that a copy of the warrant be served on “the person whose property was searched or whose information was seized or copied” (emphasis added). This approach is consistent with Rule 41’s existing requirements for both standard search warrants and for tracking device warrants. See Fed. R. Crim. P. 41(f)(1)(C), (f)(2)(C); *United States v. Zacher*, 465 F.3d 336, 339 (8th Cir. 2006) (warrant for FedEx package). When the government executes a Rule 41 warrant in the physical world, it is not obliged to provide notice to everyone with a potential privacy interest in the place searched. For example, if the search of a house includes the search of a locked trunk stored at the house by a friend of the house’s owner, law enforcement has never been required to seek out and give notice of the warrant to the owner of the trunk. Similarly, if investigators execute a remote search warrant on a computer used to access a specified email account, and the computer turns out to belong to the suspect’s friend, the government should be able to satisfy its notice obligation – as it would in the physical world – by providing notice to the friend.

Interaction between the proposed amendment and Title III

The proposed amendment to Rule 41 would not affect law enforcement’s obligations to comply with the Wiretap Act, 18 U.S.C. §§ 2510-2522 (“Title III”). Title III generally requires a wiretap order to intercept⁹ wire, oral, or electronic communications, unless one of several statutory exceptions apply. See 18 U.S.C. § 2511. A Rule 41 search warrant does not permit law enforcement to intercept such communications, and nothing in the proposed amendment suggests otherwise. Thus, the ACLU is mistaken to assert that the proposed amendment “authorizes searches that can only be carried out pursuant to a Title III wiretap order.” ACLU Memorandum at 18. For example, if investigators sought an order to intercept wire, oral or electronic communications, they would have to proceed by Title III rather than Rule 41 (or in addition to Rule 41, if stored information was sought as well).

⁹ The Wiretap Act defines “intercept” to mean the “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). Communications are intercepted within the meaning of Title III when they are acquired contemporaneously with transmission. See, e.g., *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 460-63 (5th Cir. 1994).

Concealed through technological means

Under the proposed amendment, a magistrate judge in a district where activities related to a crime may have occurred will have authority to issue a warrant for a remote search if the location of the computer to be searched “has been concealed through technological means.” This “concealed through technological means” requirement provides an appropriate standard for obtaining warrants for remote searches. An officer seeking a warrant for a remote search can satisfy this component of the court’s jurisdiction to issue the warrant through an affirmative factual showing regarding the criminal’s conduct – for example, the criminal’s use of Tor to distribute child pornography. Alternative formulations of the proposed amendment, such as a requirement that the location of the computer to be searched be unknown, would likely lead to excessive *Franks* hearings on whether agents had disclosed every fact that might have suggested a possible location of the criminal’s computer; such formulations could also draw courts into determinations of whether investigators had taken appropriate steps to determine the location of the computer to be searched. In its current form, the proposed amendment provides a workable and reasonable standard for obtaining warrants for remote searches that is less likely to result in excessive litigation.

Commenter Center for Democracy and Technology (“CDT”) argues that the “concealed through technological means” standard is overly broad, *see* CDT Memorandum at 6, but its argument is based on a misunderstanding of the requirements for obtaining a criminal search warrant. CDT states that “[I]legitimate uses of technology that have the effect of ‘concealing through technological means’ a user’s location . . . should not trigger the ability for a judge to issue a Rule 41 warrant.” *Id.* at 7. Under the proposed amendment, however, investigators could not obtain a search warrant merely because a user’s location is concealed through technological means. Rather, the warrant application must also demonstrate probable cause that the search will uncover evidence, fruits, or instrumentalities of crime. *See* Fed. R. Crim. P. 41(c). The proposed amendment does not alter that rule, but instead provides an alternative means of satisfying Rule 41’s venue provisions. Standing alone, the use of Internet anonymizing techniques to conceal location does not provide a basis for obtaining a search warrant.¹⁰

Avoiding collateral damage and internal Department of Justice policies

Some commenters raised concerns about the possibility that the Department’s use of remote searches could damage a targeted computer or other computer systems. The Department is mindful of the impact that remote search software has on computers, and we are careful in our use of remote searches, just as we are careful to avoid injury to persons or damage to property in the far more common scenario of executing physical search warrants. In our efforts to date, we have balanced risks involved in technical measures against the importance of the objectives of an investigation in stopping crime and protecting public safety, and we have considered the

¹⁰ CDT is also concerned that a warrant could be issued when a user conceals location through a means that is “not technically technical,” such as misreporting of the city of residence in a Facebook profile. CDT Memorandum at 7. The language of the proposed amendment, however, requires that the location of the relevant “media or information” be concealed through “technological means.” It is unclear to us how misrepresenting one’s city of residence on Facebook would conceal the location of media or information subject to search in the first place, much less through technological means.

availability and risks of potential alternative investigative avenues. As a result of this caution, although remote searches are relatively uncommon, the searches we have undertaken have not resulted in the types of collateral damage that the commenters hypothesize. Such careful consideration of any future technical measures will continue.

Similarly, the successes of the Department's anti-botnet initiatives demonstrate that our efforts in the cyber realm can bring substantial benefits while avoiding collateral damage to victims. The Department, often in collaboration with public and private sector partners, has conducted technical operations pursuant to court authorization to disrupt and dismantle several botnets infecting computers of innocent users, including the Coreflood¹¹ and Gameover Zeus¹² botnets. The results of these operations demonstrate that our technical efforts have resulted in substantial benefits for computer users victimized by online crime, rather than any undue collateral damage.

Currently, the remote searches that would be applied for under the amended rule are not subject to mandatory internal regulation at the Department. However, remote searches may implicate other existing Departmental guidelines and regulations depending on the circumstances. Additionally, the FBI is required to adhere to the Attorney General's Guidelines for Domestic FBI Operations ("AGG-DOM") and the FBI's Domestic Investigations and Operations Guide ("DIOG") in conducting remote searches, and those guidelines require that the FBI use the least intrusive method available in conducting a search.¹³ Section I(C)(2)(a) of the AGG-DOM provides:

The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of different investigative methods that are each operationally sound and effective, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and potential damage to reputation. The least intrusive method feasible is to be used in such situations. It is recognized,

¹¹ In Operation Coreflood, the FBI worked with private sector and law enforcement partners to disable a botnet that had infected an estimated two million computers with malicious software. The malware on the Coreflood botnet allowed infected computers to be controlled remotely by criminals to steal private personal and financial information from unsuspecting users. The FBI obtained a court order to seize domain names, re-route the botnet to FBI-controlled servers, and stop the Coreflood software from running.

¹² Gameover Zeus, believed to have infected approximately 500,000 to one million computers worldwide and to have caused losses of over \$100 million, is an extremely sophisticated type of malware designed to steal banking and other credentials from the computers it infects. Those credentials are then used to initiate or redirect wire transfers to accounts overseas. The government obtained civil and criminal court orders in federal court in Pittsburgh authorizing measures to sever communications between the infected computers and criminal servers, and redirect them from the criminal servers to substitute servers under the government's control.

¹³ Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM), Sec. I(C)(2)(a); Domestic Investigations and Operations Guide (DIOG), Sec. 18.2.

however, that the choice of methods is a matter of judgment. The FBI shall not hesitate to use any lawful method consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of foreign intelligence sought to the United States' interests. This point is to be particularly observed in investigations relating to terrorism.

Likewise, Section 18.2 of the DIOG provides, "The AGG-DOM requires that the 'least intrusive' means or method be considered and—if reasonable based upon the circumstances of the investigation—used to obtain intelligence or evidence in lieu of more intrusive methods." The DIOG also contains a section providing extensive and detailed guidance on making least intrusive method determinations.¹⁴ Although the least intrusive methods requirement is primarily designed to address privacy and civil liberties concerns, its principles apply to avoiding collateral damage in remote searches as well and inform, among other things, the way in which a NIT is designed (so as to minimize the likelihood of damage), its capabilities, and the manner in which it is used.

Most remote searches are unlikely to have any significant lasting effect on the integrity of a targeted computer. In any case, as the Supreme Court has recognized, "the details of how best to proceed with the performance of a search authorized by warrant" are "generally left to the discretion of the executing officers." *Dalia*, 441 U.S. at 257. Subsequently, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Id.* at 258. This same standard would apply to any damage caused by officers executing a warrant by remote search. In addition, as with all investigative techniques, the Department will scrutinize the use of NITs, and the Department may in the future choose to impose additional regulations on their use.

- - -

We appreciate the opportunity to respond to issues raised by commenters on the proposed amendment to Rule 41. We look forward to further discussions with the Committee. Please let us know if there are other issues or concerns which you would like the Department to address.

¹⁴ DIOG § 4.4. The section includes subsections entitled, "General Approach to Least Intrusive Method Concept," Section 4.4.2; "Determining Intrusiveness," Section 4.4.3; and "Standard for Balancing Intrusion and Investigative Requirements," Section 4.4.4.

PUBLIC SUBMISSION

As of: February 23, 2015
Tracking No. 1jz-8hd8-kr4w
Comments Due: February 17, 2015

Docket: [USC-RULES-CR-2014-0004](#)

Proposed Amendments to the Federal Rules of Criminal Procedure

Comment On: [USC-RULES-CR-2014-0004-0001](#)

Preliminary Draft of Proposed Amendments to the Federal Rules of Criminal Procedure

Document: [USC-RULES-CR-2014-0004-0057](#)

Comment from David Bitkower, U. S. Department of Justice

Submitter Information

Name: David Bitkower

Organization: NA

General Comment

See Attached

Attachments

Hearing Response Final 2-20-15



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

February 20, 2015

MEMORANDUM

TO: The Honorable Reena Raggi
Chair, Advisory Committee on Criminal Rules

FROM: David Bitkower *DB*
Deputy Assistant Attorney General

SUBJECT: Additional Response to Comments Concerning Proposed Amendment to Rule 41

The Committee has asked the Department to address recent comments received in opposition to the Department's proposed amendment to Rule 41. We thank the Committee for the opportunity to address these comments. Because many of the comments reiterate concerns raised by other commenters and previously addressed by the Department, we will not fully repeat our discussion of those issues here.¹

The Rules Committee is an appropriate forum to address venue for warrant applications.

Several comments, including comments from Google and the Pennsylvania Bar Association ("PBA"), argue that the proposal expands the government's investigative authority and therefore should only be addressed by Congress. The Department believes that these arguments are mistaken for multiple reasons.

First, the criticisms appear to misunderstand what is at stake in the proposal. As the Department has repeatedly emphasized, the proposal would not authorize the government to undertake any search or seizure or use any remote search technique not already permitted under current law. Rather, the proposed amendment would merely ensure that some court is available to *consider* whether a particular warrant application comports with the Fourth Amendment. Google characterizes the proposal as impacting substantial rights, Google Memo at 4, but

¹ For example, Google's memo at pages 1-4 addresses international issues. The Department addressed these issues in its letter to the Committee dated October 20, 2014, which explained that a warrant is not required to conduct searches outside the United States. Google's memo at pages 8-10 addresses particularity, collateral damage, Title III, and notice; the Department addressed each of these issues in its letter to the Committee dated December 22, 2014.

provides no support for this claim; there is no substantive right to be free from a search warrant that complies with the Fourth Amendment. Because only warrants that meet the relevant substantive legal requirements can be lawfully issued by a court, a rule concerning which court can consider applications cannot accurately be said to be substantive.²

Second, it is entirely proper for the Rules Committee to address the appropriate venue for issuing a search warrant. Indeed, the Committee did so in 1990 (creating what is now Rule 41(b)(2) governing property that may move out of the issuing district after the warrant is issued), and it did so more recently in 2006 (creating Rule 41(b)(4) to provide venue to issue tracking warrants) and 2008 (creating Rule 41(b)(5) to provide venue to issue warrants for, among other places, diplomatic and consular missions). Accordingly, Google's assertion that the proposed amendment would violate the Rules Enabling Act is also incorrect.³

Third, certain commenters suggest that law enforcement generally should not be permitted to use new investigative techniques absent congressional approval. This suggestion is incorrect on two counts. Initially, the premise underlying the suggestion is incorrect because the use of remote searches is not new (as other commenters have pointed out), and warrants for remote searches are currently issued under the Federal Rules. Moreover, there is not and has never been a practice of forswearing the use of "new" techniques absent congressional approval. As one example, Congress has never specifically authorized video surveillance warrants, but courts have appropriately approved such warrants under Rule 41. *See, e.g., United States v. Falls*, 34 F.3d 674, 678-83 (8th Cir. 1994); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987). The Supreme Court also approved warrants to collect dialing information from telephones long before Congress enacted the Pen Register and Trap and Trace statute. *See United States v. New York Tel. Co.*, 434 U.S. 159 (1977). Nor has Congress passed statutes governing other investigative techniques that may be judicially authorized via search warrant, ranging from thermal imaging to the compulsory taking of a DNA sample. A rule that law enforcement cannot use a new investigative technique absent specific congressional authorization would thus be both inconsistent with historical practice and unwise.

Finally, the Rules Committees and the Judicial Conference, which exercise authority delegated by Congress over federal court procedures, have repeatedly counseled the Department to raise procedural issues with the appropriate Rules Committee first, rather than directly with Congress. Congress delegated to the courts "the power to prescribe general rules of practice and

² Google also argues that that Rule would impact substantial rights because it would weaken Fourth Amendment protections. Google Memo at 4-5. But an amendment to the rules cannot limit the application of the Fourth Amendment, and courts will address constitutional issues associated with remote search warrants on a case-by-case basis, just as they do with physical warrants.

³ Google appears to argue that the 2008 amendment was attributable to Congress and not the Committee because seven years prior to that amendment Congress authorized the prosecution of certain criminal offenses taking place in a subset of the locations in which the amendment later authorized searches. This logic does not follow. In any event, the 2008 amendment clarified venue to issue warrants in investigations of crimes defined by Congress, which is exactly what the proposed amendment would do here.

procedure.” 28 U.S.C. § 2072. Of course, Congress continues to exercise oversight over the rules, and no new rule goes into effect until Congress is given the opportunity to review it. And should Congress determine that additional regulation of remote searches is desirable, it can enact legislation to provide such regulation. But the Department shares the Judiciary’s view that congressional consideration of this important issue, which will follow passage of any amendment, will benefit greatly from this Committee’s work. We therefore believe that following this standard practice to amend the Federal Rules of Criminal Procedure with respect to venue for search warrant applications is entirely appropriate in this circumstance.

The language of the proposed rule is not vague.

The National Association of Criminal Defense Lawyers (“NACDL”), Google, and commenter Michael Boucher argue that certain language in the proposed amendment is either vague or too broad, including the phrases “in any district where activities related to a crime may have occurred,” “remote access,” and “concealed through technological means.” The Department believes that each of these phrases is appropriately clear and limited.

The Department addressed the scope of the phrase “concealed through technological means” in its December 22, 2014 memorandum, and we will not fully repeat that discussion here. However, because many commenters appear to have misunderstood this point, we again take the opportunity to note that under the proposed amendment, investigators could not obtain a search warrant merely because a user’s location is concealed through technological means. Rather, the warrant application must also demonstrate probable cause that the search will uncover evidence, fruits, or instrumentalities of crime. *See Fed. R. Crim. P. 41(c)*. Nothing in the proposed amendment would affect the existing probable cause requirement or any other substantive requirement to issue a warrant. By the same token, satisfaction of the “concealed through technological means” requirement would not by itself result in issuance of a warrant, but rather merely identify which subpart of the rule would govern which court was empowered to consider the warrant application in the first instance.

The NACDL objects that the phrase “in any district where activities related to a crime may have occurred” is vague. This language, however, was copied verbatim from the existing Rule 41(b)(3) and (b)(5). The Department believes that using existing language where possible minimizes confusion and uncertainty in the interpretation of the Rules. To the extent that there is any ambiguity in this phrase – and we doubt there is much – courts can give appropriate meaning to this language in the context of specific facts.⁴

Google asserts that the proposed amendment is vague because it does not limit or specify how “remote access” searches are conducted. But the Supreme Court has repeatedly specified that “[n]othing in the language of the Constitution or in this Court’s decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed.” *United States v. Grubbs*, 547 U.S. 90, 98 (2006) (quoting *Dalia v. United States*, 441 U.S. 238, 255 (1979)). The Department believes that the meaning of “remote access” is clear. The dictionary defines “remote” as “far away; distant.”

⁴ Google similarly objects to use of the word “media,” but that word is also adopted from the language of the current rule.

New Oxford American English Dictionary 1433 (2nd ed. 2005). The term “remote access” means that the search will not be conducted by agents physically accessing the media, but rather by agents connecting to the computer remotely – from far away – such as through a network.

The botnet amendment is appropriate.

We continue to believe that the portion of the proposal addressing botnets is important and appropriate despite objections raised by Google, NACDL, and Michael Boucher. Again, the botnet proposal does not authorize any searches that cannot already be conducted under current law; it merely concerns venue, specifying which judge (or how many judges) may consider an application for a warrant in investigations of violations of 18 U.S.C. § 1030(a)(5) affecting five or more districts.

Google objects to the scope of botnet warrants, noting that they could authorize remote searches of millions of computers. But the large scope of botnet warrants is not a function of Rule 41, it is a function of the scope of botnet crime. Botnets may affect millions of people. And importantly, Google offers no solution for obtaining a warrant in such cases. It would be odd to adopt a “too big to investigate” rule in response to vast criminal activity.

NACDL and Michael Boucher correctly note that the computers searched pursuant to a botnet warrant may belong to innocent victims. Again, this fact is not unique to the botnet context, or even the digital evidence context. In *Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978), the Supreme Court held that search warrants may be directed to evidence in the possession of innocent parties, and investigations involving crimes ranging from burglary to murder frequently involve searches of a victim’s premises or property for evidence left behind by the perpetrator. We anticipate that the items to be searched or seized from victim computers pursuant to a botnet warrant will typically be quite limited in order to remain within the scope of current law concerning reasonableness. However, we believe that it may be reasonable in a given botnet investigation to obtain information from a large number of victim computers – for example, to measure the scope of the botnet. The purpose of our proposed rule is not to mandate such searches in every case or to alter any of the substantive rules governing when such searches are reasonable under the law, but to ensure that if such searches are appropriate they are not effectively precluded because of the practical difficulty of obtaining simultaneous judicial authorization from 94 different magistrate judges.

The proposed amendment does not conflict with the Privacy Protection Act.

Finally, the Reporters Committee for Freedom of the Press (“RCFP”) is concerned that the proposed amendment contravenes the protections of the Privacy Protection Act, 42 U.S.C. § 2000aa (“PPA”). These concerns are misplaced, as the PPA would apply to warrants issued under the proposed amendment in the same manner as it currently applies to other search warrants. The RCFP also objects that the proposed amendment does not substantively preclude “law enforcement impersonation of the news media in an effort to execute a remote access search.” But again, the proposal neither authorizes nor precludes the use of any particular undercover activities with respect to remote search, just as the current Rule 41 does not authorize or preclude the impersonation of journalists (or anyone else) when executing physical search

warrants. Those matters are appropriately addressed, if at all, through substantive law rather than venue provisions.

- - -

Few of the recently received comments raise any issue not already addressed by the Department and the Committee. Several of the arguments are premised on incorrect understandings of what the proposal would actually authorize or of current law. We continue to believe that the proposed amendment would provide needed clarity concerning venue and thus ensure the availability of prior judicial consideration of these important investigative techniques. Of course, Congress will have the final say on the proposal, but Congress's review only benefits from the Judicial Conference's thorough consideration. We appreciate the opportunity to respond to issues raised by commenters and look forward to further discussions with the Committee.

TAB 6A

MEMO TO: Members, Criminal Rules Advisory Committee

FROM: Professors Sara Sun Beale and Nancy King, Reporters

RE: Rule 35 Proposal (14-CR-E)

DATE: February 15, 2015

Prior to its November 2014 meeting the Committee received a proposal from the New York Council of Defense Lawyers to amend Rule 35 to permit a judge to reduce the sentence of a defendant who has served two thirds of his incarceration term and establishes one of the following circumstances by clear and convincing evidence: (1) newly discovered scientific evidence that raises a substantial question about the validity of his conviction; (2) substantial rehabilitation during confinement; or (3) deterioration of medical condition (providing an alternative compassionate release).

After a brief discussion of the proposal at the November meeting, Judge Raggi appointed a Subcommittee to consider the proposal (Ms. Brook, Judges Feinerman and Lawson, Mr. Siffert, Mr. Wroblewski for the Department of Justice, and Judge James Dever, Chair).

The Subcommittee met by telephone conference to discuss the proposal (Tab C), as well as a detailed memorandum prepared by the Reporters (Tab B), and a letter from the NYCDL (Tab D) withdrawing one aspect of the proposal, namely the provision that would have authorized a judge to impose a sentence lower than the otherwise applicable statutory minimum sentence. The Reporters' memo discussed:

- the history of Rule 35 and the elimination of the discretionary authority to reduce a sentence by the Sentencing Reform Act of 1984,
- a previous proposal to restore that authority which was rejected by the Criminal Rules Committee in 2003,
- the concern that the proposal might exceed the Committee's rulemaking authority, and
- the opposition by the Judicial Conference's Criminal Law Committee to a somewhat similar legislative amendment.

After discussion, the Subcommittee unanimously agreed that the proposed amendment to Rule 35 involves changes beyond the Committee's purview. Accordingly, it recommends that the Committee take no further action on the proposed amendment.

TAB 6B

MEMO TO: Rule 35 Subcommittee

FROM: Sara Sun Beale and Nancy King, Reporters

RE: Background for December 17 conference call

DATE: December 5, 2014

We are providing this memorandum to assist the Subcommittee with its consideration of the proposal to amend Rule 35 submitted by the New York Council of Defense Lawyers (NYCDL). The proposed amendment would authorize a federal judge to reduce the sentence of a defendant who has served two thirds of his incarceration term and establishes one of the following circumstances by clear and convincing evidence: (1) newly discovered scientific evidence that raises a substantial question about the validity of his conviction; (2) substantial rehabilitation during confinement; or (3) deterioration of medical condition (providing an alternative compassionate release). A letter from the NYCDL supporting the proposal states that the proposal is advanced to “help to ease the problems of lengthy and unnecessary incarceration in some cases, by permitting defendants to obtain release from prison somewhat earlier than they can under the current sentencing regime.”¹

At the Committee’s November meeting, the proposal was discussed briefly before being referred to Subcommittee. Comments in favor included approval of the proposal as a means for reducing the prison population, and the observation that judges found it helpful under former Rule 35 to grant motions to reduce sentences on grounds beyond those available under the current version of the rule. Concerns about the proposal included observations that it overlapped with pending legislation and conflicted with existing statutes governing sentencing and collateral review.

Part I of this memorandum provides a history of Rule 35, including the use of motions to reduce sentences under the Rule in effect prior to 1987, the elimination of the discretionary authority to reduce a sentence by the Sentencing Reform Act of 1984 (SRA), and a previous proposal to restore that authority, considered and rejected by the Committee in 2003. Part II reviews the current proposal and its rationale. Part III examines several issues raised by the proposal, including the concern that the proposal may exceed the rulemaking authority conferred by the Rules Enabling Act. We also note that the Judicial Conference’s Criminal Law Committee has opposed legislation that is similar in some respects to the current proposal.

¹ Letter from Alexandra Shapiro, President, NYCDL, to the Hon. Reena Raggi, Circuit Judge, U.S. Court of Appeals for the Second Circuit 3 (Oct. 17, 2014) [hereinafter NYCDL Letter], *available at* <http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/cr-suggestions-2014/14-CR-E-Suggestion.pdf>.

I. Rule 35 History and Overview

A. Rule 35 before the Sentencing Reform Act of 1987

The original 1944 version of Rule 35 authorized (1) the correction of an illegal sentence at any time and (2) the reduction of a sentence within 60 days after imposition or after receipt of an order following review by a higher court.²

1. Correction of Illegal Sentences

In 1948, two years after Rule 35 went into effect, 28 U.S.C. § 2255³ was enacted, creating some uncertainty about which claims could be raised under the new statutory remedy and which could be raised under Rule 35. In 1962, the Court held in *Hill v. United States*⁴ that unlike Section 2255, Rule 35 reached only claims that the sentence itself was illegal (*e.g.*, exceeded the statutory maximum), and did not extend to errors in trial, sentencing, or other proceedings leading to the conviction or sentence.⁵ In 1966, the Committee specifically rejected the Court's interpretation of the Rule in *Hill* and amended Rule 35 to expressly authorize courts to correct sentences imposed in an illegal manner.⁶ Thereafter, it was not uncommon for a prisoner to seek relief under both remedies, moving in the district court for relief under Rule 35 and Section 2255.⁷

2. Judicial Sentence Reduction

In addition to authorizing procedural attacks on a sentence, the 1966 amendment also extended the time for seeking *reduction* of sentence, from 60 days to 120 days.⁸ As one court

² At the time the Rule was adopted, a court could modify a valid sentence only during the term at which it was entered. The Rule substituted a time limitation that would be the same in every case.

³ Section 2255 was designed to mirror the remedy of habeas corpus, and authorized a judge to vacate or correct a federal sentence “upon the ground that the sentence was imposed in violation of the Constitution or laws of the United States, or that the court was without jurisdiction to impose such sentence, or that the sentence was in excess of the maximum authorized by law, or is otherwise subject to collateral attack.” 28 U.S.C. § 2255(a) (2014).

⁴ 368 U.S. 424, 430 (1962).

⁵ *See id.* at 428–30 (holding failure to provide allocution opportunity was not cognizable under Section 2255 as it was “neither jurisdictional nor constitutional,” nor was it the proper subject of a motion under Rule 35).

⁶ The amendment limited the time for correction of legal sentences imposed in an illegal manner to 120 days after imposition of sentence. Because correction of an illegal sentence had no time limitation, courts between 1966 and 1987 struggled to classify various claims as illegal manner claims or illegal sentence claims, with mixed success. *See* 3 FED. PRAC. & PROC. CRIM. § 617, nn.20–23 (4th ed.); *see, e.g.*, *United States v. Cevallos*, 538 F.2d 1122, 1127–28 (5th Cir. 1976) (“[T]o be properly within the scope of a Rule 35 motion to correct sentence, brought after the 120-day limitation on challenges to sentences imposed in an illegal manner, the error in sentencing need not be so great as to be jurisdictional or constitutional, but the error must render the sentence imposed illegal.”). Moreover, a movant had to pick between the two sections of the Rule because reduction of sentence was not available if the defendant challenged his sentence as illegal. *See, e.g.*, *United States v. Dean*, 752 F.2d 535, 545 (11th Cir. 1985) (“[T]he district court lacked the authority to reduce Dean's sentence under Rule 35(a).”).

⁷ *See, e.g.*, *United States v. Malcolm*, 432 F.2d 809, 811 (2d Cir. 1970). A prisoner could seek Section 2255 relief without first filing a Rule 35 motion, *see, e.g.*, *United States v. Corsentino*, 685 F.2d 48, 50 (2d Cir. 1982), and could file multiple Rule 35 motions. *See, e.g.*, *United States v. Kimberlin*, 781 F.2d 1247, 1249 (7th Cir. 1985).

⁸ The 120-day time limit marked the end of the opportunity for a reduced sentence. Discretionary reduction was not available under Section 2255. *See United States v. Patterson*, 739 F.2d 191, 196 (5th Cir. 1984) (citing *United States*

explained: “The time limitation appears to have as its dual purpose the protection of the district court from continuing and successive importunities and to assure that the district court's power to reduce a sentence will not be misused as a substitute for the consideration of parole by the Parole Board.”⁹

Courts treated a motion for reduction of sentence under Rule 35 as “essentially a plea for leniency . . . addressed to the sound discretion of the district court.”¹⁰ A Second Circuit case explained:

Rule 35 is intended to give every convicted defendant a second round before the sentencing judge, and at the same time, it affords the judge an opportunity to reconsider the sentence in the light of any further information about the defendant or the case which may have been presented to him in the interim.¹¹

For example, a court might reduce a sentence if it realized after sentencing “that the [parole] guidelines would cause [the defendant] to be imprisoned substantially longer than . . . intended,”¹² or that the sentence exceeded the expectations of the parties in the plea agreement.¹³

Some regarded the possibility of reduction as somewhat of a safety valve for correcting injustice, like clemency.¹⁴ Motions for reduction of sentence in some courts were routinely filed,

v. Addonizio, 442 U.S. 178, 179 (1979)). In 1985, the Rule was amended to clarify that the motion need only be *made* within 120 days, and that a court “shall determine the motion within a reasonable time.”

⁹ United States v. Taylor, 768 F.2d 114, 118 (6th Cir. 1985) (quoting United States v. Stollings, 516 F.2d 1287, 1289 (4th Cir. 1975)); *see also* Gaertner v. United States, 763 F.2d 787, 794 n.7 (7th Cir. 1985) (noting that “many cases confronting such a usurpation of Parole Board authority have held that the sentencing judge involved delayed his consideration of a timely-filed Rule 35 motion for an unreasonable time”).

¹⁰ United States v. Hooton, 693 F.2d 857, 859 (9th Cir. 1982); *see also* Poole v. United States, 250 F.2d 396, 401 (D.C. Cir. 1957).

¹¹ United States v. Ellenbogen, 390 F.2d 537, 543 (2d Cir. 1968); *see also* United States v. Colvin, 644 F.2d 703, 705 (8th Cir. 1981) (reduction available whenever judge decided “that the sentence originally imposed was, for any reason, unduly severe”).

¹² Geraghty v. U.S. Parole Comm'n, 579 F.2d 238, 242 n.7 (3d Cir. 1978) (judge reduced sentence “from 4 years to 30 months”), *vacated on other grounds*, 445 U.S. 388 (1980); *see also* United States v. Kabat, 797 F.2d 580, 583 n.3 (8th Cir. 1986) (“The court based its action on a Parole Commission ruling as to the severity of the offenses that would have resulted in Woodson being incarcerated longer than the district court had anticipated.”); United States v. DeMier, 671 F.2d 1200, 1203 (8th Cir. 1982) (court did not receive the applicable parole guidelines until after sentencing the defendant); United States v. Slutsky, 514 F.2d 1222, 1229 (2d Cir. 1975) (reviewing an appeal of a motion to reduce, and remanding for resentencing after concluding that given developments subsequent to the district court’s denial of the motion, “in all probability the appellants will not receive the parole treatment envisioned by the sentencing judge,” so “there should be an opportunity for reconsideration in light of all recent developments in the area”).

¹³ For example, in one case Judge Weinstein reduced a five-year probation term to two years, to bring the total sentence in line with “the expectations of the petitioner.” *Paradiso v. United States*, 689 F.2d 28, 30 (2d Cir. 1982).

¹⁴ Consider the statement of Judge Skelly Wright, writing for the majority in upholding the judgments against the “foot soldiers of the Watergate Break-in” : “In sentencing appellants [Judge Sirica] imposed penalties significantly less onerous than those visited upon their co-defendants, their immediate superiors in the enterprise. If further clemency is deemed warranted, a motion to reduce sentence under Rule 35, Fed.R.Crim.P., is always available.” *United States v. Barker*, 514 F.2d 208, 211, 227 (D.C. Cir. 1975) (en banc), *cert. denied*, 421 U.S. 1013 (1975); *see also* United States v. Badolato, 701 F.2d 915, 922 n.6 (11th Cir. 1983) (noting the defendant “still may move to

and courts reassured defendants at sentencing that they could seek reduction later.¹⁵ The Rule could be invoked without a motion of the defendant, *sua sponte*,¹⁶ and did not bar multiple motions to reduce.¹⁷ There was no duty, however, to hold a hearing before denying such a motion.¹⁸

Orders denying reduction of sentence generated many appeals,¹⁹ but were overturned infrequently.²⁰ Trial courts could entertain a motion to reduce sentence before or after, but not during, a pending appeal.²¹ Courts of appeals reviewed government objections to orders granting reductions either by writ of mandamus²² or appellate jurisdiction.²³ Orders granting reduction generally were upheld so long as they did not violate another statutory command.²⁴

reduce his sentence” under Rule 35 “[i]f he feels that the sentencing judge did not give sufficient consideration to what he contends his purposes were”).

¹⁵ See, e.g., *United States v. Pool*, 660 F.2d 547, 554 (5th Cir. 1981) (judge told defendant at sentencing “it’s normally the case that a Rule 35 motion will be made, which is a motion for reduction of sentence. I’m sure your attorney can explain that to you. At that time the court will take that under consideration.”). The prospect of a Rule 35 reduction was also used to encourage compliance by those sentenced for criminal contempt. See, e.g., *In re Liberatore*, 574 F.2d 78, 88, n.9 (2d Cir. 1978) (citations omitted) (“[T]he district court could have imposed a criminal contempt sentence of definite duration and coupled the imposition of such a sentence with ‘(a) promise to consider subsequent compliance in ruling on any Rule 35 motion for reduction of sentence.’”); *United States v. DiMauro*, 441 F.2d 428, 431 (8th Cir. 1971)).

¹⁶ See, e.g., *United States v. Soto*, 793 F.2d 217, 217 (9th Cir. 1986), *cert. denied*, 484 U.S. 833 (1987).

¹⁷ See, e.g., *United States v. Nerren*, 613 F.2d 572, 573 (5th Cir. 1980) (*per curiam*) (defendants filed two motions to reduce and appealed from the second denial).

¹⁸ See, e.g., *United States v. Brummett*, 786 F.2d 720, 723 (6th Cir. 1986).

¹⁹ Claims included that the judge did not exercise any discretion, that by opposing reduction the government breached its agreement not to oppose defense arguments for leniency at sentencing, see *Brooks v. United States*, 708 F.2d 1280, 1282 (7th Cir. 1983), that the judge should have granted a hearing or considered certain evidence, or that the judge did not understand some of the convictions had been vacated.

²⁰ For examples of reversals, see *United States v. Edmonson*, 659 F.2d 549, 550 (5th Cir. 1981) (remanding for reduction where defendants were sentenced for multiple counts for the same offense); *United States v. Warren*, 610 F.2d 680, 685 (9th Cir. 1980) (“The court might have reduced his sentences by the same amount of time which was credited to them. But an order simply crediting time spent in state custody is the functional equivalent of an order imposing a federal sentence to run concurrently with a state sentence: it specifies where a prisoner will serve some or all of a federal sentence. Such an order conflicts with the Attorney General’s authority . . . to designate the place of confinement for federal prisoners and is invalid.”); *Woosley v. United States*, 478 F.2d 139, 143–46 (8th Cir. 1973) (*en banc*) (holding “refusal to consider probation as a reasonable alternative” and mechanical application of maximum sentence for draft violator was error).

²¹ See *United States v. Mack*, 466 F.2d 333, 340 (D.C. Cir. 1972), *cert. denied*, 409 U.S. 952 (1972). In non-contempt cases, some appellate courts would not consider a claim that the sentence was excessive until the defendant first filed a motion to reduce the sentence under Rule 35, but would hear such claims on appeal in contempt cases. See *United States v. Miller*, 588 F.2d 1256, 1259 (9th Cir. 1978).

²² See *United States v. Ferri*, 686 F.2d 147, 155 (3d Cir. 1982).

²³ See *United States v. DeMier*, 671 F.2d 1200, 1204 (8th Cir. 1982); *United States v. Hetrick*, 644 F.2d 752, 755 (9th Cir. 1980) (holding that “the government may appeal, pursuant to section 3731, a district court’s order” granting a Rule 35 motion for reduction of sentence).

²⁴ See *United States v. Cumbie*, 569 F.2d 273, 274–75 (5th Cir. 1978) (“As long as the sentences are within the statutory limits, and are not so arbitrary and capricious as to amount to a gross abuse of discretion, the lower court’s ruling on Rule 35 motions will not be disturbed.”).

3. *Rule 35 Before the Effective Date of the Sentencing Reform Act*

Minor amendments were made in 1979, 1983, and 1985, so that as of 1986, Rule 35 provided:

(a) Correction of Sentence. The court may correct an illegal sentence at any time and it may correct a sentence imposed in an illegal manner within the time provided herein for the reduction of sentence.

(b) Reduction of Sentence. A motion to reduce a sentence may be made, or the court may reduce a sentence without motion, within 120 days after the sentence is imposed or probation is revoked, or within 120 days after receipt by the court of a mandate issued upon affirmance of the judgment or dismissal of the appeal, or within 120 days after entry of any order or judgment of the Supreme Court denying review of, or having the effect of upholding, a judgment of conviction or probation revocation. The court shall determine the motion within a reasonable time. Changing a sentence from a sentence of incarceration to a grant of probation shall constitute a permissible reduction of sentence under this subdivision.²⁵

B. Rule 35 After the Sentencing Reform Act of 1984

Congress fundamentally transformed federal sentencing law and procedure with the Sentencing Reform Act of 1984 (SRA), part of the Comprehensive Crime Control Act of 1984. The SRA, effective November 1, 1987, was the product of decades of dissatisfaction with “[t]he shameful disparity in criminal sentences”²⁶ that judges imposed and offenders served. Congress hoped to bring both more certainty and more consistency to federal sentencing by eliminating the discretion of corrections officials at the back end of the sentencing process and restricting the sentencing discretion of judges at the front end. The Act abolished discretionary parole and substituted determinate sentencing so that the sentence selected by the judge would be the sentence served by the defendant (less good time, which was also regulated by the Act).²⁷ To rein in judicial discretion, Congress created the United States Sentencing Commission and charged it with promulgating sentencing guidelines that judges would be required to follow. Congress reclassified offenses into statutory sentence ranges with minimum terms of incarceration, and restricted probation terms and conditions. The SRA mandated new procedure as well as substance, rewriting Rule 32, regulating presentence investigations and reports, listing factors courts must consider when selecting a sentence, regulating revocation of release, and providing appellate review to enforce judicial compliance with the new laws.

Congress also restricted the ability of judges to reduce the sentences that they initially imposed. 18 U.S.C. § 3582(c) provides that “[t]he court may not modify a term of imprisonment once it has been imposed except” in three circumstances: (1) as permitted by statute or Rule 35, (2) upon motion of the Bureau of Prisons (BOP) Director “if it finds that . . . extraordinary and compelling reasons warrant such reduction” or the prisoner is 70 or older and has served at least 30 years (“compassionate release”), or (3) when the defendant was sentenced to prison based on

²⁵ *United States v. Fowler*, 794 F.2d 1446, 1448–49 (9th Cir. 1986) (quoting FED. R. CRIM. P. 35 (1986)).

²⁶ S. REP. NO. 98-225, at 3248 (1983).

²⁷ *See* *Tapia v. United States*, 131 S. Ct. 2382, 2386–87 (2011); *Barber v. Thomas*, 560 U.S. 474, 481–82 (2010).

a Guidelines range that was subsequently lowered by the Commission.²⁸ According to the Senate Report:

The value of the forms of ‘safety valves’ contained in this subsection lies in the fact that they assure the availability of specific review and reduction of a term of imprisonment for ‘extraordinary and compelling reasons’ and to respond to changes in the guidelines. The approach taken keeps the sentencing power in the judiciary where it belongs, yet permits later review of sentences in particularly compelling situations.²⁹

Congress also rewrote Rule 35 as part of the SRA.³⁰ Except for arithmetic or technical errors (which may be raised within 14 days of sentencing), the Rule no longer provided any remedy for illegal sentences and procedural errors. Such claims had to be raised either on direct appeal or under Section 2255. The rewritten rule also transformed the authority to reduce a sentence from an option for leniency that a judge could exercise at his discretion, into a tool to facilitate government rewards to cooperating defendants. Under the revised rule, a judge could only reduce a sentence (1) on remand after appellate review when resentencing was ordered (language that was eventually deleted in 2002 as unnecessary given other statutory commands) or (2) when granting a motion of the government to reward a defendant's cooperation.³¹

Although Rule 35 has been amended several times since its transformation by the SRA, none of the changes have expanded the authority of a judge to reduce a sentence beyond the power to grant a government motion to reward cooperation.³² Nor has Section 3582(c) been amended to expand the circumstances under which a judge may modify a sentence.

As rewritten by the SRA, Rule 35 also provided that a judge reducing a sentence for cooperation could sentence below the otherwise mandated minimum sentence. The only other existing authority for imposing a below-minimum sentence appears in 18 U.S.C. § 3553(e) and (f). Section 3553(e) permits a sentence less than a mandatory minimum to be imposed upon government motion “to reflect a defendant’s ‘substantial assistance in the investigation or prosecution of another person who has committed an offense.’”³³ Section 3553(f), added in 1994, permits a sentence less than the mandatory minimum in certain drug cases that do not involve violence, serious injury, death, firearms, or other dangerous weapons, as long as “the defendant does not have more than 1 criminal history point,” did not lead or organize the offense,

²⁸ This exception was recently applied to a case involving a Rule 11(c)(1)(C) plea in *Freeman v. United States*, 131 S. Ct. 2685 (2011) (also stating “Federal courts are forbidden, as a general matter, to ‘modify a term of imprisonment once it has been imposed,’ 18 U.S.C. § 3582(c); but the rule of finality is subject to a few narrow exceptions.”).

²⁹ S. REP. NO. 98-225, at 3304 (1983).

³⁰ See Pub. L. No. 98-473, § 215(b), 98 Stat. 1837, 2015–16 (1984).

³¹ Rule 35(b) as amended by the SRA provided that modification must be made “within one year after the imposition of a sentence.” *Id.*

³² In 1991, Rule 35 authorized judges to correct, within 7 days of imposition, obvious “arithmetical, technical, or other clear error,” and extended the year’s deadline for government motions in certain circumstances. Rule 35 was restyled in 2002, and the language regarding correcting sentences on remand was deleted. A provision clarifying that “sentencing” meant the oral imposition of sentence was added in 2004. A reference to the Guidelines was deleted after *Booker* in 2007, and the time to correct technical errors was extended to 14 days in 2009.

³³ *Wade v. United States*, 504 U.S. 181, 182 (1992) (quoting § 3553(e)).

and has provided truthful and complete information about “the offense or offenses that were part of the same course of conduct or a common scheme or plan.”

C. Past Efforts to Restore Judicial Discretion to Reduce Sentences Under Rule 35

In March of 2001, the Director of the American Bar Association, Robert D. Evans, proposed on behalf of the ABA that the Committee consider amending Rule 35 to permit discretionary reduction upon defense motion.³⁴ As support, Mr. Evans attached a record showing that the ABA House of Delegates had approved the following resolution: “That the American Bar Association urges the Congress of the United States to retain Rule 35(b) of the Federal Rules of Criminal Procedure to allow a criminal defendant to move and a federal judge to consider a possible reduction of a sentence.”³⁵ A report, dated February 1987 (before the 1984 amendments to Rule 35 became effective), and authored by Professor Norman Lefstein, Chairperson of the Criminal Justice Section (“ABA Report”), was attached to the proposal. The ABA Report argued that the SRA’s “radical emasculation” of Rule 35 was unjustified and bad policy.³⁶ A copy of the letter and its attachments is appended to this memorandum. The arguments made by the ABA thirteen years ago have not been referenced by the proponents of the current proposal, but are included in this memorandum nonetheless because of their potential relevance to the Subcommittee’s deliberations.

The ABA Report suggested that Congress approved of the change to Rule 35 because it assumed erroneously that sentence reductions could be had through appeal and that a major reason for requesting reductions—rehabilitation—was no longer relevant to sentencing under the new system. Instead, the report argued, “the basic premise underlying Rule 35(b)” had not been altered by the SRA:

District court judges still may make mistakes; reflection still may cause a change of heart; circumstances may still change after sentencing; new information may still be discovered after sentencing; disparities in sentencing may still exist; and both remorse and cooperation may still be withheld on advice of counsel until all appeals are exhausted.³⁷

³⁴ Letter from Robert D. Evans, Director, Am. Bar Ass’n, to Peter G. McCabe, Sec’y, Comm. on Rules of Practice and Procedure (Mar. 2, 2001):

The Association recommends that the Committee consider making further amendments to allow defense counsel to move for reduction and corrections of sentence. Prior to passage of the Comprehensive Crime Control Act of 1984, the Rule provided that defense counsel could make such a motion for the court’s consideration.

Enclosed is the relevant American Bar Association policy on this matter. Although adopted in 1987, the principles it espouses are still valid. The accompanying report, which is not a part of the official ABA policy, may be useful to the Committee in considering this matter.

Id. at 2.

³⁵ SUMMARY OF ACTION TAKEN BY THE HOUSE OF DELEGATES OF THE AM. BAR ASS’N 18 (1987).

³⁶ NORMAN LEFSTEIN, CHAIRMAN, AM. BAR. ASS’N CRIMINAL JUSTICE SECTION, REPORT ON RULE 35 2 (1987).

³⁷ *Id.* at 3.

As to mistakes in sentencing, the report argued that it was not clear that judicial misapprehension would be a basis for relief on appeal under 18 U.S.C. § 3742, or that a reviewing court would entertain new information showing why a sentencing court's assumptions were incorrect. Even under the Guidelines, judges in some cases may have second thoughts about a sentence after time for reflection, the ABA Report asserted. Under the old Rule, it maintained, judges could correct a sentence when, shortly after a sentence was imposed, circumstances relevant to sentencing changed, citing cases in which judges reduced sentences under Rule 35 after a defendant became seriously ill, or a family member became unable to care for children. The new rule, the report stated, "will on occasion permit bitter injustices to occur."³⁸ Judges under the new rule also will be unable to correct disparities in sentencing after other defendants are sentenced for similar conduct, the report stated. Without the option of a motion to reduce sentence, "[t]here will simply be no opportunity for a defendant to admit guilt and express remorse before appeal, unless it is done on the day of sentencing," raising Fifth Amendment problems.³⁹ The report concluded that it is unfair to deprive the defendant of the right to request reconsideration of the sentence, and that by eliminating the option of a motion to reduce, the Rule "guaranteed a vast increase in the number of appeals from guilty pleas," and "lengthened the time necessary to correct . . . a sentence."⁴⁰

At its fall meeting in 2003, the Committee declined to pursue the ABA's proposal, but neither the agenda book nor the minutes for that meeting reveal what the Committee members thought about the proposal.⁴¹

II. The Current Proposal and Its Rationale

The proposed amendment to Rule 35 before the Subcommittee is set out in the letter from the NYCDL. Unlike the 2001 ABA proposal to restore Rule 35(b) to its pre-1987 scope, the present proposal advances a version of the Rule that is both narrower and broader. It is narrower in that it is limited to defendants who have served two thirds of their sentences, and enumerates the authorized grounds for reduction. It is broader in that it places no limit on the time period during which such a motion may be filed, permits reduction of sentence below the otherwise authorized statutory range, and permits reduction as a remedy not only for claims of an illegal

³⁸ *Id.* at 6.

³⁹ *Id.* at 8.

⁴⁰ *Id.* at 4.

⁴¹ The agenda book contained only a very brief cover memorandum from the Reporter describing the proposal, and the minutes of the Committee's consideration state only the following:

In 2001, as part of the public comment period on the restyled Rules of Criminal Procedure, the American Bar Association had recommended that Rule 35 be amended to permit the defendant to move for sentence reduction. The matter had not been specifically addressed since that time, although the proposal appears on the docket as pending. The Reporter indicated that the issue has been raised from time to time, without any formal vote. Following additional discussion, Judge Carnes provided the Committee with an opportunity to move to propose the amendment. When no motion was forthcoming, he stated that the proposal had been considered rejected, for lack of a motion and that the docket should be amended to reflect that the proposal had been "completed."

See Minutes, Advisory Committee on Criminal Rules 12 (Oct. 2003).

sentence, but also for claims attacking the conviction.

In support for the proposal, the Council advances four arguments: (1) it will assist in the effort to reduce the population of incarcerated federal prisoners; (2) it will provide a needed alternative to existing remedies for claims based on newly discovered evidence; (3) it will provide a means for the early release of clearly rehabilitated prisoners; and (4) it will provide a needed alternative to existing regulations for compassionate release. These reasons are examined in turn below.

A. Prison Population Should Be Reduced

A recent report by the Office of Inspector General⁴² found the “Persisting Crisis” in the Federal Prison System” to be the number one challenge for the Department of Justice. It stated:

[D]espite a slight decrease in the total number of federal inmates in fiscal year (FY) 2014, the Department projects that the costs of the federal prison system will continue to increase in the years ahead, consuming a large share of the Department’s budget. . . . [F]ederal prisons remain significantly overcrowded and therefore face a number of important safety and security issues.⁴³

Describing the efforts that the Department of Justice had made to reduce prison costs⁴⁴ and overcrowding,⁴⁵ the Inspector General nevertheless concluded that the Department needs to do

⁴² Memorandum, Top Management and Performance Challenges Facing the Department of Justice, from Michael E. Horowitz, Inspector General, to the Attorney General and the Deputy Attorney General (Nov. 10, 2014) [hereinafter OIG Memorandum], available at <http://www.justice.gov/oig/challenges/2014.htm>.

⁴³ *Id.*

⁴⁴ *See id.* For example:

[T]he Department has recently announced initiatives and changes in prosecution, sentencing, and early release policies that could reduce federal prison costs. These proposed policies target inmates sentenced for drug offenses, a group that accounts for more than half of the current federal prison population. The Department’s FY 2015 budget request includes \$173 million to support the Smart on Crime initiative, which the Department indicates is intended to promote prevention and reentry programs, such as drug courts and veterans courts as alternatives to incarceration, and encourages prosecutors to draft criminal charges for low-level nonviolent drug offenders in ways that will not trigger mandatory minimum sentences. Further, in April 2014, the Department announced a clemency initiative for prisoners already serving long sentences for low-level, non-violent drug offenses.

The Department also has indicated its support for programs that provide alternatives to incarceration, coupled with treatment and supervision, in an attempt to reduce recidivism. In an August 2013 speech, the Attorney General identified state-sponsored initiatives that he said served as effective alternatives to incarceration by providing offenders the treatment and supervision designed to reduce recidivism while also reducing states’ prison populations. The Attorney General also instructed all U.S. Attorneys’ Offices (USAOs) to designate a Prevention and Reentry Coordinator in their respective Districts to expand on existing programs that promote the implementation of the Smart on Crime initiative.

Id.

⁴⁵ *See id.* The report explained:

more. The NYCDL letter quotes Attorney General Holder expressing concern about over-incarceration.⁴⁶

Assuming that the Subcommittee agrees that reducing the prison population is a laudable, even vitally important policy objective, it may wish to consider whether an amendment to the Federal Rules of Criminal Procedure is an appropriate means of addressing this problem.

B. Existing Relief for Claims Based on Newly Discovered Evidence Is Too Difficult to Obtain

The NYCDL proposal authorizes a sentence reduction for defendants who can show that “[s]cientific evidence discovered after the defendant began his term of incarceration creates a substantial question about the validity of the defendant’s conviction.”⁴⁷ The NYCDL argues that relief based on newly discovered evidence

has become more difficult to obtain through the writ of habeas corpus because of the judicial and statutory limitations on the use of the writ, and we submit that this provision will make it easier for the Court to consider meritorious applications for early release from inmates who have a substantial argument that recently discovered evidence tends to exonerate them.⁴⁸

Post-conviction relief for federal prisoners has indeed been restricted in the three decades since the SRA. In 1996, Congress enacted a number of limitations on relief under Section 2255 as part of the Anti-Terrorism and Effective Death Penalty Act (AEDPA), including a new one-year statute of limitations for filing, and new restrictions on successive petitions. The AEDPA includes an exception to the successive petition bar for cases with new evidence of innocence, however. A claim filed in a second or subsequent petition can be heard if it first certified by the court of appeals to involve either:

- (1) newly discovered evidence that, if proven and viewed in light of the evidence as a whole, would be sufficient to establish by clear and convincing evidence that no reasonable factfinder would have found the movant guilty of the offense; or
- (2) a new rule of constitutional law, made retroactive to cases on collateral review by the Supreme Court that was previously unavailable.⁴⁹

Prison overcrowding presents the most significant threat to the safety and security of BOP staff and inmates. . . . As of June 2014, federal prisons operated at 33 percent overcapacity, with 42 percent overcrowding at higher security facilities and 40 percent at medium security facilities.

. . . .

Addressing the challenge of ensuring the safety and security of correctional officers and federal inmates will require the BOP to take several actions. First and foremost, the BOP must pursue strategies to reduce prison overcrowding.

Id.

⁴⁶ See NYCDL Letter, *supra* note 1, at 2 (“As Attorney General Holder himself has noted, ‘widespread incarceration at the federal, state, and local levels is both ineffective and unsustainable.’”).

⁴⁷ *Id.* at 6.

⁴⁸ *Id.* at 3.

⁴⁹ 28 U.S.C. § 2255(h) (2014).

As for the statute of limitations, in 2013, the Court recognized an equitable exception to the filing period for state prisoners with evidence of actual innocence, an exception that is being applied by the lower courts to federal prisoners as well.⁵⁰

In contrast to the equitable exception for late discovered evidence of innocence, which requires a court to take into account unexplained delay in assessing whether the petitioner has made a sufficient showing of innocence,⁵¹ the proposed amendment to Rule 35 suggests no limitation on how soon after discovering the scientific evidence a motion to reduce must be filed. The proposed amendment also places no restrictions on the number of motions that may be made.

The proposed Rule 35 reduction authority could be more advantageous to defendants than Section 2255 in other ways. The Court has not clarified whether relief under Section 2255 is available for a prisoner who is able to demonstrate probable innocence, but unable to demonstrate any procedural violation.⁵² By contrast, the proposed amendment to Rule 35 appears to contemplate relief in this situation. Those lower courts that have considered extending relief for such “bare innocence” claims have not agreed on the standard that the defendant would have to meet in order to demonstrate innocence. The proposal requires “clear and convincing evidence” that newly discovered evidence “creates a substantial question” about the conviction’s “validity.” This is an easier hurdle to clear than at least one lower court’s standard for bare innocence claims.⁵³ It is also easier than the showing of innocence required for merits review of a claim otherwise barred as successive, namely, “clear and convincing evidence that no reasonable factfinder would have found the movant guilty.”⁵⁴

As for other remedies, because the proposal focuses on scientific evidence, mention should be made of 18 U.S.C. § 3600, the federal post-conviction DNA testing statute, enacted as part of the Innocence Protection Act of 2004. Section 3600 provides that the district court shall order DNA testing of evidence in possession of the government that either had not been tested previously or had been tested using an older method, upon a timely application by a federal prisoner who asserts a viable theory of actual innocence that would be confirmed by favorable testing results, and whose identity was an issue if convicted by trial. The judge may, but need not appoint counsel. If the results of testing exclude the prisoner, he may file a motion for new

⁵⁰ See *United States v. Baxter*, 761 F.3d 17, 31 (D.C. Cir. 2014) (citing *McQuiggin v. Perkins*, 133 S. Ct. 1924 (2013)).

⁵¹ *McQuiggin*, 133 S. Ct. at 1935.

⁵² See *id.* at 1931 (“We have not resolved whether a prisoner may be entitled to habeas relief based on a freestanding claim of actual innocence.”). For a useful recent collection of lower court authority on bare innocence claims, see John M. Leventhal, *A Survey of Federal and State Courts' Approaches to a Constitutional Right of Actual Innocence: Is There A Need for A State Constitutional Right in New York in the Aftermath of CPL § 440.10(1)(G-1)?*, 76 ALB. L. REV. 1453 (2013).

⁵³ See *In re Davis*, No. CV409-130, 2010 WL 3385081, at *45 (S.D. Ga. Aug. 24, 2010) (adjudicating bare innocence claim on remand from the Supreme Court exercising its original habeas jurisdiction, concluding petitioner had to “show by clear and convincing evidence that *no reasonable juror would have convicted him* in the light of the new evidence” and was unable to do so) (emphasis added).

⁵⁴ § 2255(h)(2).

trial, which shall be granted if the results along with all of the other evidence establish by “compelling evidence” that a new trial would result in an acquittal.⁵⁵ In 2009, the Supreme Court held that limitations in Alaska’s DNA testing statute, which it noted were similar to those found in Section 3600, did not render the process constitutionally inadequate.⁵⁶

Other avenues of collateral relief are not likely to be available under the current statutory regime. Although the “savings clause” (18 U.S.C. § 2255(e)) permits a person in federal custody to seek habeas corpus relief under Section 2241 instead of Section 2255 in certain circumstances, there is considerable disagreement about the scope of this provision. Accordingly, it is not clear that a prisoner could raise a claim of actual innocence based on newly discovered scientific evidence under Section 2241 (which is not affected by AEDPA’s filing deadlines or successive petition restrictions). The Supreme Court recently suggested that a sentence reduction for “extraordinary and compelling reasons” under 18 U.S.C. § 3582(c)(1)(A)(i) could be available reasons other than declining health (conceivably including new evidence of innocence),⁵⁷ but to our knowledge no court has employed this provision to reduce a sentence based on a showing of innocence.

The Subcommittee may wish to consider whether existing remedies are inadequate for prisoners who obtain scientific evidence suggesting innocence, and if so, whether an amendment to the Federal Rules of Criminal Procedure is an appropriate means of addressing that problem.

C. Existing Law Lacks a Means to Release Clearly Rehabilitated Prisoners

The NYCDL appears to disagree with the policy choice made by Congress in the SRA when it eliminated early release for rehabilitation. It argues that early release on the basis of rehabilitation is consistent with one of the goals of sentencing recognized by the current sentencing regime.⁵⁸ The proposed amendment would permit judges, rather than a paroling authority, to grant early release on this basis.

Discretionary parole release guided by evidence-based practices is enjoying a resurgence of interest. Reliance on risk and needs assessment tools tested by decades of recidivism research has reduced some of the former skepticism about the efficacy and fairness of discretionary release by paroling authorities. There is also considerable support for tempering the rigidity of

⁵⁵ 18 U.S.C. § 3600(g)(2) (2014).

⁵⁶ See *District Attorney’s Office for the Third Judicial District v. Osborne*, 557 U.S. 52, 69 (2009).

⁵⁷ The Supreme Court in *Setser v. United States*, 132 S. Ct. 1463 (2012), rejected the position of both the prisoner and the government that a federal court lacks the authority to run a federal sentence consecutively to an anticipated state sentence. See *id.* at 1473. In dismissing the argument that interpreting the statute at issue to provide this authority would lead to unfairness when the federal judge’s prediction of the state sentence proved later to be inaccurate, the Court quoted Section 3582(c)(1)(A), referring to it as “a mechanism for relief” applicable “when the district court’s failure to ‘anticipat[e] developments that take place after the first sentencing,’ . . . produces unfairness to the defendant.” *Id.* at 1472

⁵⁸ Congress itself recognized one basis for sentence reduction based on post-commitment rehabilitation when it passed 18 U.S.C. § 3621(e)(2), which permits the Bureau of Prisons to reduce for up to one year the sentence of a those convicted of nonviolent offenses upon successful completion of a drug-treatment program. The title of the provision— “[i]ncentive for prisoners’ successful completion of treatment program” —and its limited reach suggest that this provision is not, however, part of a general Congressional acceptance of back-end sentencing adjustments for rehabilitation.

determinate sentencing with a circumscribed opportunity to obtain a second look by the trial judge. For example, the ALI's new *Model Penal Code: Sentencing* includes such a second-look by judges.⁵⁹ The ALI provision affects only prisoners sentenced to two decades or more in prison, and it is intended as “a narrow incursion upon the Code's general preference for determinate sentences,” avoiding “the shortcomings of the parole-release framework.”⁶⁰

The Subcommittee may wish to consider whether it agrees that expanded judicial modification power would be desirable, and, if so whether rulemaking is an appropriate means of achieving this goal.

D. BOP Regulations for “Compassionate Release” Make it Too Difficult for Ill Inmates No Longer Posing a Risk of Recidivism to Obtain Release

The NYCDL presents the third circumstance for reduction—a health condition that eliminates any significant risk of recidivism—as a means of addressing the unnecessarily restrictive regulations for compassionate release under 18 U.S.C. § 3582(c). Following criticism of the compassionate release program, including a 2013 OIG Memorandum concluding “that the program was not well-run,”⁶¹ the BOP expanded the program as part of the Department of Justice’s Smart on Crime initiative.⁶²

The Subcommittee may wish to consider whether, in light of these changes, the compassionate release program is too restrictive, and, if so, whether an amendment to the Federal Rules of Criminal Procedure is an appropriate means of addressing this problem.

III. Issues Raised by the Proposal

The primary concern expressed by Committee members at the November meeting was that the proposed amendment would conflict with existing statutory commands, including (1) the restrictions on judicial modification enacted as part of the SRA and (2) the restrictions on judicial relief from sentencing and conviction under Section 2255. A related concern was that some of the changes proposed would go beyond the authority provided by the Rules Enabling Act, 28 U.S.C. § 2072. Also, members noted that Congress is already considering other legislation to amend some aspects of sentencing law and provide alternative “back-end” reductions. All three of these issues should be considered by the Subcommittee in evaluating the threshold question of whether an amendment expanding judicial authority to reduce sentences under Rule 35 is appropriate at this time. They are discussed in Part III.A, *infra*.

A second set of issues would have to be addressed should the Subcommittee conclude

⁵⁹ See MODEL PENAL CODE: SENTENCING § 305.6, at *1 (T.D. No. 2, 2011).

⁶⁰ *Id.* at *3. The provision notes: “Sentence modification under this provision should be viewed as analogous to a resentencing in light of present circumstances. The inquiry shall be whether the purposes of sentencing in § 1.02(2) would better be served by a modified sentence than the prisoner's completion of the original sentence.” *Id.* at *1. Commentary explains, “[p]risoner rehabilitation remains an eligible concern . . . , but it is far from the only admissible consideration, or the basic underpinning, of the sentence-modification power.” *Id.* at *3.

⁶¹ See OIG Memorandum, *supra* note 44 (referring to earlier 2013 Report).

⁶² See Rafael Lemaitre, *Real #DrugPolicyReform: DOJ's New Criteria on Compassionate Release Requests*, OFFICE OF NATIONAL DRUG POLICY REFORM (Aug. 12, 2013 1:00 AM), <http://www.whitehouse.gov/blog/2013/08/12/real-drugpolicyreform-doj-s-new-criteria-compassionate-release-requests> (summarizing the changes announced in the fall of 2013)

that the proposal should be considered further. These include issues regarding the scope of the proposal itself, its relationship to other aspects of the process, its implementation, and its likely impact. A brief listing of some of these issues appears in Part III.B, *infra*.

A. The Legality and Propriety of Accomplishing These Changes by Rulemaking

1. Conflict with Existing Statutes and the Rules Enabling Act

All three proposed new grounds for sentence reduction reject specific legislative choices embedded in existing law that limit judicial remedies for criminal defendants. Subsection (d)(1)(A) of the proposal—which authorizes sentence reductions on the basis of new scientific evidence of innocence—sidesteps limits Congress adopted for relief under Section 2255 and the Innocence Protection Act. Subsection (d)(1)(B) would reverse, in part, the decision of Congress to drastically limit the authority of judges to reduce sentences and curtail back-end adjustments to sentences for post-commitment rehabilitation under the SRA. Subsection (d)(1)(C) rejects Congress’ decision to condition “compassionate release” upon a request of the Director of the BOP, and to limit that exception to the circumstances specified in 18 U.S.C. § 3582(c).

The NYCDL argues that the Rules Enabling Act would not bar the proposal “because any change in the Rule would ultimately be approved by Congress after judicial review and recommendation, whether by explicit approval or by the rulemaking procedure established by Congress (i.e. Congressional acquiescence).”⁶³ At the Advisory Committee’s November meeting Professor Daniel Coquillette agreed that the Rules Enabling Act’s supersession clause does permit the adoption of rules that supersede existing statutes. Professor Coquillette reminded the Committee, however, that injudicious invocation of that clause may prompt Congress to reconsider it. To avoid this sort of conflict, he explained, Rules Committees have often pursued a different approach, *i.e.*, sponsored legislation.

2. Substance or Procedure and the Rules Enabling Act

A related but separate concern is whether the proposed amendment would run afoul of the Rules Enabling Act. Under that statute, a federal rule must not “abridge, enlarge or modify any substantive right.” 28 U.S.C. § 2072(b). In applying that provision, the Supreme Court has stated “that Rules which incidentally affect litigants’ substantive rights do not violate this provision if reasonably necessary to maintain the integrity of that system of rules.”⁶⁴ In *Hanna v. Plumer*,⁶⁵ the Court explained that “[t]he test must be whether a rule really regulates procedure,—the judicial process for enforcing rights and duties recognized by substantive law and for justly administering remedy and redress for disregard or infraction of them.”⁶⁶ As the Court explained:

Congress’ prohibition of any alteration of substantive rights of litigants was obviously not addressed to such incidental effects as necessarily attend the adoption of the prescribed new rules of procedure upon the rights of litigants who, agreeably to rules of practice and procedure, have been brought before a court

⁶³ NYCDL Letter, *supra* note 1, at 4.

⁶⁴ *Burlington N.R.R. Co. v. Woods*, 480 U.S. 1, 5 (1987).

⁶⁵ 380 U.S. 460 (1965).

⁶⁶ *Id.* at 464 (quoting *Sibbach v. Wilson & Co.*, 312 U.S. 1, 14 (1941)).

authorized to determine their rights.⁶⁷

More recently, writing for a plurality of the Court, Justice Scalia observed that the test under the Rules Enabling Act is not whether a rule affects a litigant's substantive rights; indeed most procedural rules will do so. Instead, the focus is on "what the rule itself regulates: If it governs only 'the manner and the means' by which the litigants' rights are 'enforced,' it is valid; if it alters 'the rules of decision by which [the] court will adjudicate [those] rights,' it is not."⁶⁸

The proposed amendment arguably "enlarges" or "modifies" the substantive rights of certain defendants by expanding post-conviction remedies beyond those provided by existing law, authorizing district judges to reduce their sentences, and to reduce them *below* the minimum otherwise required by statute. The right to seek a reduced punishment, and the right to seek a below-minimum sentence, is narrowly limited by existing statute. The proposed amendment may do more than regulate the manner and means of seeking a sentence reduction, providing a new right to sentence reductions that does not now exist.

3. *Pending Legislation and Potential Conflict with Judicial Conference Position*

Legislation introduced in the 113th Congress and still pending would authorize judges to determine whether early release is appropriate for certain offenders who have been found to be at a low risk of reoffending. Section 2(b) of the Recidivism Reduction and Public Safety Act of 2014⁶⁹ requires the BOP to develop, expand, and make available to all eligible inmates "appropriate recidivism reduction programming or productive activities." Section 3 of the bill requires the Attorney General to develop for use by the BOP an offender risk and needs assessment system to determine the recidivism risk level of all prisoners. Section 4 creates a system of "prerelease custody." It authorizes the BOP Director to transfer inmates who have completed a BOP recidivism reduction program and who have a low to moderate risk assessment to "prerelease custody," which includes home confinement or community supervision. For inmates sentenced to a term of imprisonment of more than 3 years, the Director's decision to transfer an inmate to prerelease custody is subject to review by the sentencing court.

As described by the Criminal Law Committee, the bill provides:

For inmates who were sentenced to three years or more, the BOP Director would be required to give six months' notice of a release decision to the sentencing court. The notice would include the amount of earned credit, the anticipated date of transfer, the prerelease custody plan, the prisoner's behavioral record, and the prisoner's most recent risk assessment. *The bill would authorize the court to conduct a hearing on its own motion or on the government's motion, which the prisoner would have the right to attend. After the hearing, the court would be able to deny the transfer to home confinement or community supervision if the court found by a preponderance of the evidence that the transfer is contrary to public safety or to the earned credit system established by the new bill. Certain prisoners would be excluded from eligibility for transfer altogether*

⁶⁷ *Id.* at 465.

⁶⁸ *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 407 (2010) (plurality opinion).

⁶⁹ S. 1675, 113th Cong. (2014).

. . . [I]nmates on home confinement or on “community supervision” would remain under BOP custody but would be supervised by probation officers.⁷⁰

The bill was reported out of the Senate Judiciary Committee on March 6, 2014.

Prior to the March 6 vote, Judge Bates, the Director of the Administrative Office of U.S. Courts, wrote to the Senate Judiciary Committee noting the Criminal Law Committee’s opposition to that portion of the bill that would involve judges in deciding whether to release an inmate to a community setting. Judge Bates noted that “serious questions have been raised within the judiciary . . . about the proposed amendment to S. 1675.”⁷¹ The Criminal Law Committee’s concerns are summarized in its report to the Judicial Conference, which is attached to this memorandum. The Criminal Law Committee objected that judges are not in the position to perform this function—a function traditionally performed by the executive branch:

[T]he executive branch . . . is in the best position to determine where an inmate should serve a sentence, the type of security classification an inmate is assigned, and whether an inmate is making appropriate progress in his or her correctional treatment. Authorizing judges to make release decisions raises public safety concerns due to judges’ lack of direct contact with inmates and the most accurate and up-to-date information about their conduct and condition.⁷²

Unlike the defendants whose terms of probation and supervised release the judge sets with the assistance of a probation officer who knows something about the person, inmates seeking early release from a judge under the proposed legislation may “have no relationship with the probation officers working for the court.”⁷³ Authorizing judges to make release decisions is also inconsistent with both the goals of “truth in sentencing,” and avoiding unwarranted sentencing disparities, the report continued.⁷⁴ Moreover, because the proposal would involve probation officers in monitoring those still in BOP custody, the proposed legislation would transfer costs of monitoring from the executive to the judiciary.⁷⁵

The Subcommittee may wish to consider whether the proposed amendment to Rule 35 raises any of the concerns that prompted the Criminal Law Committee to object to portions of S. 1675.

The Subcommittee may also wish to consider whether—as an alternative to amending Rule 35—it recommends that the Committee explore options for legislation that would address any gaps in existing law. For example, regarding compassionate release, the Judicial Conference is seeking an amendment to 18 U.S.C. § 3583(e)(1), that would permit the early termination of supervision terms for an inmate who is compassionately released from prison under 18 U.S.C. § 3582(c). The Judicial Conference agreed that there are cases where earlier termination would

⁷⁰ Report from the Judicial Conference Committee on Criminal Law Committee to the Chief Justice of the U.S. and Members of the Judicial Conference of the U.S. 12–13 (Sept. 2014) (emphasis added).

⁷¹ *Id.* at 13 (quoting Letter from the Hon. John D. Bates, Director, Administrative Office of the U.S. Courts, to the Senate Judiciary Committee (Mar. 5, 2014)).

⁷² *Id.* at 14.

⁷³ *Id.*

⁷⁴ *Id.* at 15.

⁷⁵ The House version is H.R. 2656, the “Public Safety Enhancement Act of 2013,” which has been referred to the House Judiciary Committee. *See id.* at 13.

be appropriate based on factors independent of the offender's conduct. For example, where defendants are physically incapacitated, dying, or aged to the point that they are no longer a risk to the community and cannot meaningfully engage in the supervision process, it makes little policy or financial sense to keep such cases under supervision.⁷⁶

B. Other Issues Raised by the Proposed Amendment

Given the formidable controversies discussed above, it seemed prudent to postpone a detailed discussion of questions of scope and application of the proposal. Some idea of the range of questions is suggested by the case law that developed under the former Rule 35(b) motion for reduction of sentence. Those potential questions would include:

- (1) How would the motion for reduction interact with appeal, and with the other post-conviction remedies available to a defendant, including motions for new trial, and applications for relief under Section 2255? Must one remedy be exhausted before another? Must a prisoner seek relief under Section 3582(c) before moving for reduction under Rule 35? Can a prisoner raise the same claim in both?
- (2) Could more than one ground for reduction be raised by the same prisoner? More than one motion regarding the same sentence? Or more than one motion when a prisoner is serving multiple sentences concurrently?
- (3) Could the terms be more precisely defined? What is included in the term "scientific evidence"? What is meant by the phrase "substantial question about the validity of the defendant's conviction"? Is this only factual innocence or something more?
- (4) What procedural protections would accompany such a motion, particularly one raising new scientific evidence? When could a judge proceed without a hearing or without appointing counsel?
- (5) What standard would the court of appeals apply to a judge's ruling on a Rule 35 motion to reduce?
- (6) Is one particular ground for reduction of sentence more acceptable or desirable than others?
- (7) Are there additional restrictions that should be required, such as a time limit like the one in the former Rule 35(b)?

⁷⁶ Email from Julie Wilson to Reporters (Nov. 14, 2014) (on file with authors).

TAB 6C

RECEIVED
IN CHAMBERS OF
HON. REENA RAGGI

NEW YORK COUNCIL OF DEFENSE LAWYERS ★ **DEC 11 2014** ★

c/o Alexandra A.E. Shapiro, Esq.
Shapiro, Arato & Isserles LLP
500 Fifth Avenue, 40th Floor, New York, New York 10110
TELEPHONE: 212.257.4880 FAX: 212.202.6417
E-MAIL: ashapiro@shapiroarato.com

AM _____
PM _____

Alexandra A. E. Shapiro
President
Roland G. Riopelle
Vice President
Susan Necheles
Secretary-Treasurer

Board of Directors
James J. Benjamin, Jr
David E. Brodsky
Marc Greenwald
Sean Hecker
Linda Imes
Jane W. Parver
Marjorie J. Pearce
Jodi Misher Peikin
Patricia A. Pileggi
Jill Shellow

Ex Officio
Alan Kaufman

December 8, 2014

Hon. Reena Raggi
United States Circuit Judge
United States Court of Appeals,
Second Circuit
United States Courthouse
225 Cadman Plaza East
Brooklyn, NY 11201-1818

Re: Proposed Amendment to Fed. R. Crim. P. 35

Dear Judge Raggi:

I am writing regarding the New York Council of Defense Lawyers' proposal to amend Federal Rule of Criminal Procedure 35. It has come to our attention that some members of the Advisory Committee are concerned that sub-paragraph (d)(3) of our proposal would permit a judge to impose a sentence below an otherwise applicable statutory minimum and that such a change must be formally passed by Congress. In order to avoid an objection on this basis, we are willing to withdraw sub-paragraph (d)(3) of our proposal, and limit our proposal to the other changes to Rule 35 described in my letter of October 17, 2014.

Hon. Reena Raggi
December 8, 2014

Page 2

Please let us know if you have any questions.

Very truly yours,

A handwritten signature in black ink, consisting of three distinct, stylized characters that appear to be 'A', 'S', and 'S'.

Alexandra A.E. Shapiro

cc: Michael Grudberg, Esq.
Roland Riopelle, Esq.

TAB 6D

NEW YORK COUNCIL OF DEFENSE LAWYERS

c/o Alexandra A.E. Shapiro, Esq.
 Shapiro, Arato & Isserles LLP
 500 Fifth Avenue, 40th Floor, New York, New York 10110
 TELEPHONE: 212.257.4881 FAX: 212.202.6417
 E-MAIL: ashapiro@shapiroarato.com

Alexandra A.E. Shapiro
 President
 Roland G. Riopelle
 Vice President
 Susan Necheles
 Secretary-Treasurer

Board of Directors

James J. Benjamin, Jr.
 David E. Brodsky
 Marc Greenwald
 Sean Hecker
 Linda Imes
 Jane W. Parver
 Marjorie J. Pearce
 Jodi Misher Peikin
 Patricia A. Pileggi
 Jill Shellow

Ex Officio

Alan Kaufman

October 17, 2014

Hon. Reena Raggi
 United States Circuit Judge
 United States Court of Appeals,
 Second Circuit
 United States Courthouse
 225 Cadman Plaza East
 Brooklyn, NY 11201-1818

RECEIVED
 IN CHAMBERS OF
 HON. REENA RAGGI

★ OCT 20 2014 ★

AM _____
 PM _____

Re: Proposed Amendment to Fed. R. Crim. P. 35

Dear Judge Raggi:

This letter is submitted on behalf of the New York Council of Defense Lawyers (the "NYCDL"). We write to you in your capacity as Chairperson of the Advisory Committee on the Federal Rules of Criminal Procedure, to propose an amendment to Federal Rule of Criminal Procedure 35. A copy of the proposed amendment is enclosed. The proposed amendments to Rule 35 are black-lined.

The NYCDL is a professional association comprised of approximately 250 experienced attorneys whose principal area of practice is the defense of white collar criminal cases in federal court. Among its members are former Assistant United States Attorneys, including previous Chiefs of the Criminal Divisions in the Southern and Eastern Districts of New York. Its membership also includes current and former attorneys from the Office of the Federal Defender.

The NYCDL's members thus have gained familiarity with the Federal Rules of Criminal Procedure both as prosecutors and as defense lawyers.

A. The Terms of the Proposed Amendments

The proposed amendment would allow a defendant to make a motion to reduce his sentence after serving two thirds of his sentence. Such a motion would be limited to those cases in which the defendant could prove, by clear and convincing evidence, that the post-sentence discovery of scientific evidence justifies his release; his substantial rehabilitation justifies his release; or the defendant's changed medical condition justifies his release. In addition, before granting any motion to reduce a defendant's sentence, the Court would be required to solicit the opinion of any victim who submitted a victim impact statement in connection with the defendant's original sentencing.

B. The Merits of the Proposed Amendments

The grounds on which the motion could be made are circumscribed, and clear and convincing evidence will be required. This proposed amendment will not result in an "open floodgate" of meritless applications that would substantially burden the District Courts. Given the manner in which the amendments are drafted, there will be relatively few applications for relief.

Nor will the proposed amendments result in a "get out of jail free" card for defendants that would effectively negate their original sentences. At the present time, through the accrual of "good time," a federal inmate typically serves approximately 85% of his or her sentence, and is eligible for release to a "halfway house" with approximately six months remaining on his or her original term of incarceration (or 10% of the term if the original sentence is less than 60 months). Thus, at the present time, an inmate serves approximately 80% of his or her sentence "behind bars." For example, on a 10 year sentence (120 months) an inmate now serves 96 months "behind bars" before being released to a halfway house, where he or she may reside for a period of up to six months.

In rare cases, the proposed amendments will permit a federal inmate to serve as little as 67% of his or her original sentence "behind bars." Under the proposed amendment to Rule 35, an inmate who receives a 120 month sentence will be eligible to make a motion for a sentencing reduction only after he or she has served 80 months of his sentence. Thus, even if his or her motion is granted without delay, the inmate will only save himself or herself 16 months "behind bars" -- although the inmate will also be spared the time in the halfway house that is presently required by the Bureau of Prisons.

In short, the proposed amendments provide a limited form of relief in a defined group of appropriate cases.

C. Why the Amendments Are Needed

It is apparent to everyone that federal incarceration has become an epidemic, and is, in some cases, unnecessary. As Attorney General Holder himself has noted, "widespread incarceration at the federal, state and local levels is both ineffective and unsustainable." Hon. Eric Holder, Address at the Annual Meeting of the American Bar Association's House of

Delegates, August 12, 2013. It is appropriate to find ways to reduce our prison population, because the burden of incarceration sometimes outweighs its benefit. To quote former Attorney General Janet Reno, “there are a great many people who are in prison for very good reasons. But many are behind bars for sentences that are too long” Hon. Janet Reno, Forward, Federal Prosecution for the 21st Century, Published by the Brennan Center for Justice, 2014.

The Department’s tacit support in some cases for the general approach advanced by this rule proposal is supported by a draft bill that we understand it submitted to the Senate Judiciary Committee that would permit a “second look” for defendants convicted of committing homicides when they were juveniles. For the moment, we have not been able to find a copy of it in the public domain.

Congress has also recognized the need to release prisoners held longer than necessary. For example, it has specifically authorized the release of certain elderly prisoners who have served a substantial portion of their sentence when they present no danger to others. *See* 18 U.S.C. § 3582(c)(1)(A); U.S.S.G. § 1B1.13.

The proposed rule amendments will help to ease the problems of lengthy and unnecessary incarceration in some cases, by permitting defendants to obtain release from prison somewhat earlier than they can under the current sentencing regime. We respectfully submit that this is an appropriate reason to amend Rule 35.

The first proposed basis for the early termination of a defendant’s sentence is newly discovered scientific evidence that calls into question the validity of the conviction. We certainly believe that a serious question as to the validity of a conviction is an appropriate reason to terminate an inmate’s sentence early. Relief of this sort has become more difficult to obtain through the writ of habeas corpus because of the judicial and statutory limitations on the use of the writ, and we submit that this provision will make it easier for the Court to consider meritorious applications for early release from inmates who have a substantial argument that recently discovered evidence tends to exonerate them.

The second proposed basis for the early termination of a defendant’s sentence is a showing of substantial rehabilitation. As the Court knows, under the old sentencing regime, defendants were eligible for parole after serving a part of their sentences. While the proposed amendments are far less likely to result in early release than parole, they will serve a similar function by permitting some defendants – those who can demonstrate by clear and convincing evidence that they have rehabilitated themselves – to exit the prison system after serving a substantial portion of their sentences. We submit that early release on this basis is appropriate, given the goals of sentencing, which include the rehabilitation of defendants. *See* United States Sentencing Guidelines Manual, Chapter 1, Section 1, Sub-section 2 “The Statutory Mission” as stated in 1987 (“the basic purposes of criminal punishment [include]: ... rehabilitation.”).

The last proposed basis for the early termination of a defendant’s sentence is a showing that the defendant’s medical condition has deteriorated, and that it is unlikely he will commit further crimes. At the present time, the criteria for “compassionate release” on medical grounds under the Bureau of Prisons’ regulations are so stringent that it is very difficult to obtain compassionate release. We believe the cost of incarcerating ill inmates who are often elderly is unnecessary where clear and convincing evidence shows that the defendant is unlikely to commit

further crimes. We submit there is a real benefit to the defendant, the defendant's family, and society, in releasing such defendants.

We do not believe the number of applications for release under these proposed amendments will present a burden on the courts. Currently, prisoners seeking release on these bases can make a request for "compassionate release" from the Bureau of Prisons. The best available historical data reflect that, from 2006 to 2011, only 211 such requests were approved by a Warden or Regional Director, and only 273 were denied and then appealed by the prisoner. *See* U.S. Dep't of Justice, Office of the Inspector General, *The Federal Bureau of Prisons' Compassionate Release Program 34-38* (April 2013). While additional requests may have been denied and not appealed in that five-year period, these numbers do not remotely present a "floodgates" problem.

We recognize that crime victims play an important role in sentencing proceedings. Therefore, the proposed amendment to Rule 35 explicitly provides that the Court must solicit and consider the opinion of any victim who submitted a victim impact statement at the time of the defendant's original sentencing before granting any motion for a sentencing reduction. By including this provision, we believe that adequate provision has been made to ensure that victims are heard in connection with any application to reduce a defendant's sentence.

Finally, the proposed amendments permit a court to reduce a defendant's sentence to a level below the minimum required by statute. We do not believe that this provision presents any significant jurisdictional issue for the Committee, because any change in the Rule would ultimately be approved by Congress after judicial review and recommendation, whether by explicit approval or by the rulemaking procedure established by Congress (i.e. Congressional acquiescence). *See* 28 U.S.C. §2072, 2074. So this provision of the Rule would ultimately be approved by Congress if adopted by the Committee and the Courts. Accordingly, there should be no bar to expanding, in the limited way proposed here, the grounds on which the Courts may reduce a defendant's sentence pursuant to Rule 35.

Please let us know if you have any questions. We look forward to hearing from Advisory Committee concerning this proposal.

Very truly yours,



Alexandra Shapiro

PROPOSED MODIFICATIONS TO RULE 35

RULE 35. CORRECTING OR REDUCING A SENTENCE

(a) Correcting Clear Error. Within 14 days after sentencing, the court may correct a sentence that resulted from arithmetical, technical or other clear error.

(b) Reducing a sentence for Substantial Assistance.

(1) In General. Upon the government's motion made within one year of sentencing, the Court may reduce a sentence if the defendant, after sentencing, provided substantial assistance in investigating or prosecuting another person.

(2) Later Motion. Upon the government's motion made more than one year after sentencing, the court may reduce a sentence if the defendant's substantial assistance involved:

(A) information not known to the defendant until one year or more after sentencing;

(B) information provided by the defendant to the government within one year of sentencing, but which did not become useful to the government until more than one year after sentencing; or

(C) information the usefulness of which could not reasonably have been anticipated by the defendant until more than one year after sentencing and which was promptly provided to the government after its usefulness was reasonably apparent to the defendant.

(3) Evaluating Substantial Assistance. In evaluating whether the defendant has provided substantial assistance, the court may consider the defendant's presentence assistance.

(4) Below Statutory Minimum. When acting under Rule 35(b), the court may reduce the sentence to a level below the minimum sentence established by statute.

(c) "Sentencing" Defined. As used in this rule, "sentencing" means the oral announcement of the sentence.

(d) Sentencing Reduction on the Application of a Defendant.

(1) In General. A defendant may make a motion to reduce his sentence after he has served two thirds of the total term of incarceration imposed on him by the District Court, if he can demonstrate by clear and convincing evidence any of the following grounds for a reduction in his sentence:

(A) Scientific Evidence. Scientific evidence discovered after the defendant began his term of incarceration creates a substantial question about the validity of the defendant's conviction;

(B) Substantial Rehabilitation. The defendant has substantially rehabilitated himself while incarcerated;

(c) The Defendant's Medical Condition. The defendant's medical condition has deteriorated to a degree that justifies his release, even if the defendant does not qualify for a "compassionate" release pursuant to the applicable Bureau of Prisons regulations. To qualify for this reduction, the defendant must demonstrate that the deterioration in his medical condition and his criminal history make it unlikely that he will commit further crimes.

(2) Role of Crime Victims. Before granting any reduction in sentence pursuant to this subsection, the Court must solicit and consider the opinion of any victim of the defendant's crime who submitted a statement in connection with the sentencing at which the defendant was sentenced to the term of incarceration which the defendant moves to reduce.

(3) Below Statutory Minimum. When acting under Rule 35(d), the court may reduce the sentence to a level below the minimum sentence established by statute.

TAB 7A

MEMO TO: Members, Criminal Rules Advisory Committee

FROM: Professors Sara Sun Beale and Nancy King, Reporters

RE: CM/ECF

DATE: February 25, 2015

The CM/ECF Subcommittee met twice by telephone to consider a draft amendment to Civil Rule 5 concerning e-filing that will be considered by the Civil Rules Committee at its Spring 2015 meeting. A draft of the agenda materials for the Civil Rules Committee is Tab B.

Because Criminal Rule 49 now provides that “Service must be made in the manner provided for a civil action,” and that “[a]paper must be filed in a manner provided for in a civil action,” changes in the Civil Rules 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 too incorporate Civil Rules. *See* 2254 Rule 12 (providing that “The Federal Rules of Civil Procedure, to the extent that they are not inconsistent with any statutory provisions or these rules, may be applied to a proceeding under these rules.”); 2255 Rule 12 (providing that “The Federal Rules of Civil Procedure and the Federal Rules of Criminal Procedure, to the extent that they are not inconsistent with any statutory provisions or these rules, may be applied to a proceeding under these rules.”)

Thus, it is possible that amendments to Criminal Rule 49 and Rules 12 of the 2254 and 2255 rules may be necessary, depending upon whether any changes made in the Civil Rules are appropriate for criminal, habeas, and 2255 cases. The Standing Committee has indicated a preference that changes and updates in the rules be uniform to the degree possible and appropriate. It would of course be ideal if changes to interlocking filing and service rules from more than one Committee were published together and considered at the same time. It appears, however, that Civil is farther along in their consideration of these issues than Criminal is.

As noted in Tab B, Professor Cooper has drafted two alternative drafts of the proposed amendment to Civil Rule 5(d)(3) for consideration at the Civil Rules Committee’s spring meeting (which will be held after this Committee’s spring meeting). Both require that all filings be made by electronic means subject to certain exceptions, but they differ on the issue of signing.

Alternative 1: All filings must be made and signed by electronic means that are consistent with any technical standards established by the Judicial Conference of the United States. But paper filing must be allowed for good cause, and may be required or allowed for other reasons by local rule. A paper filed electronically is a written paper for purposes of these rules.

Alternative 2: All filings must be made by electronic means that are consistent with any technical standards established by the Judicial Conference of the United States. But paper filing must be allowed for good cause, and may be required or allowed for other reasons by local rule. The act of electronic filing constitutes the signature of the person who makes the

filing. A paper filed electronically is a written paper for purposes of these rules.

Both versions also depart from current Criminal Rule 49(e), which states (emphasis added):

A court may, by local rule, allow papers to be filed, signed, or verified by electronic means that are consistent with any technical standards established by the Judicial Conference of the United States. *A local rule may require electronic filing only if reasonable exceptions are allowed.* A paper filed electronically in compliance with a local rule is written or in writing under these rules.

After its first telephone conference evaluating a prior draft of a possible civil rule, the CM/ECF Subcommittee asked Professors Beale and King to communicate to the reporters of the other Rules Committees the Subcommittee's preference for exempting pro se defendants from the rule requiring electronic filing in criminal cases, and to ask for a parallel exemption in the Civil Rules. Professor Cooper, the other reporters, and the Civil Rules liaison members discussed the Subcommittee's suggestion, but rejected that approach. Their tentative conclusion was that it would be best to handle pro se filers through the good cause exception, including a discussion of pro se filers in the committee note. Among the reasons offered were arguments that programs in some districts already mandate or allow e-filing by prisoners, that some pro se litigants want to e-file, and that a provision exempting pro se filers could become outdated quickly as more courts adapt CM/ECF for a wider non-attorney audience. Thus the current draft of the alternative amendments to Rule 5 contain no carve out for pro se filers in the text.

In its latest meeting, the Subcommittee noted that the latest drafts of the amendments to the Civil Rule would permit districts to exempt pro se filers from the e-filing mandate through local rule, but agreed unanimously it was not ready to endorse any new mandatory e-filing rule for either criminal cases or 2254 and 2255 cases, at least not one that lacked an express exemption for pro se and inmate filers in the text of the rule. Members recognized that there are some districts and circuits that allow pro se parties to file electronically, but there are also districts and circuits that require paper filing, and do not allow e-filing by pro se parties in criminal, 2254, and 2255 cases. Subcommittee members expressed a preference for a rule that mirrors present practice in most districts with which members were familiar: a practice that presumes such filers can use paper filing without having to make any special showing of need, or having to secure a local rule exempting them from e-filing. Members noted that at this time too little is known about the experiences of the few districts that have permitted e-filing in these cases, and the risks and benefits they have encountered. Members also raised concerns about the scope and reliability of access to technology by incarcerated filers. In addition, members had significant concerns about electronic filings under seal in criminal cases, signatures, as well as filings by unrepresented victims, law enforcement officers, material witnesses. All of these issues require more time to examine than is available before the Criminal Rules spring meeting.

The Subcommittee recommends to the Committee that it take more time to gather and evaluate additional information about past and present experiences with e-filing and e-service in criminal, 2254, and 2255 cases. Depending upon what that information reveals, it is possible the Committee may decide that rather than a uniform rule that governs e-filing in all cases, it would be more appropriate to specify different rules for electronic filing in criminal, 2254, and 2255 cases. The differences between criminal and civil cases may be so significant that different rules are warranted. In criminal cases where pro se defendants are incarcerated, for example, there are critical issues of their rights to self-representation and

access to the court that do not exist for other pro se filers in civil cases.

The Subcommittee has yet to discuss other issues raised by the pending proposals for mandatory electronic filing or for electronic service, including whether they would have any effect on the issues related to the amendment to Rule 4 presently under consideration, the impact of an electronic signing rule, or the recognition of a notice of electronic filing as proof of service. An electronic service rule may raise special problems for pro se inmates because of the frequency with which prisoners are moved between institutions and the variations in technology available at different institutions.

TAB 7B

RULES PROPOSED FOR PUBLICATION

Electronic Filing and Service

The Standing Committee Subcommittee on matters electronic has suspended operations. The several advisory committees, however, are cooperating in carrying forward consideration of the ways in which the several sets of rules should be revised to reflect the increasing dominance of electronic means of preserving and communicating information.

Earlier work has considered an open-ended rule that would equate electrons with paper in two ways. The first provision would state that a reference to information in written form includes electronically stored information. The second provision would state that any action that can or must be completed by filing or sending paper may also be accomplished by electronic means. Each provision would be qualified by an "unless otherwise provided" clause. Discussion of these provisions recognized that they might be suitable for some sets of rules but not for others. For the Civil Rules, many different words that seem to imply written form appear in many different rules. The working conclusion has been that at a minimum, several exceptions would have to be made. The time has not come to allow electronic service of initiating process as a general matter – the most common example is the initial summons and complaint, but Rules 4.1, 14, and Supplemental Rules B, C, D, E(3) and G also are involved. And a blanket exception might not be quite right. Rule 4 incorporates state grounds of personal jurisdiction; if state practice recognizes e-service, should Rule 4 insist on other modes of service?

Determining what other exceptions might be desirable would be a long and uncertain task. Developing e-technology and increasingly widespread use of it are likely to change the calculations frequently. And there is no apparent sense that courts and litigants are in fact having difficulty in adjusting practice to ongoing e-reality.

The conclusion, then, has been that the time has not come to propose general provisions that equate electrons with paper for all purposes in all Civil Rules. The Evidence Rules already have a provision. It does not appear that the Appellate, Bankruptcy, or Criminal Rules Committees will move toward proposals for similar rules in the immediate future.

A related general question involves electronic signatures. Many local rules address this question now. A proposal to amend the Bankruptcy Rules to address electronic signatures was published and then withdrawn. There did not seem to be much difficulty with treating an electronic filing by an authorized user of the court e-filing system as the filer's signature. But difficulty was encountered in dealing with papers signed by someone other than the authorized filer. Affidavits and

declarations are common examples, as are many forms of discovery responses.

It seems to have been agreed that it is too early to attempt to propose a national rule that addresses electronic signatures other than the signature of an authorized person who makes an e-filing.

The draft rules set out below do address the signature of an authorized e-filer. The alternative drafts of Rule 5(d) (3) deserve careful consideration.

The proposals set out below are advanced for consideration of a recommendation that they be published for comment in August, 2015. They cover e-filing, e-service, and recognizing a notice of electronic filing as proof of service.

e-Filing and Service; NEF as Proof of Service

INTRODUCTORY NOTES

The draft Committee Notes are new. They are designed in part to identify issues that may prompt further discussion and changes in the draft rule texts.

e-Filing

To be complete, alternative versions of this proposal have been carried forward. But as noted with Alternative 2, at least most participants favor Alternative 2. Discussion may well begin with Alternative 2 unless Alternative 1 wins new fans.

Civil Rule 5(d) (3)

(d) Filing. * * *

Alternative 1

- (3) ~~Electronic Filing, and Signing, or Verification. A court may, by local rule, allow papers to be filed~~ All filings must be made and, signed, or verified¹ by

¹ Deletion of verification by electronic means seems a conservative choice, but may be wrong. Is there any experience with local rules that might help? Verification is required for the complaint in a derivative action, Rule 23.1, a petition to perpetuate testimony, Rule 27(a), and is allowed as an alternative to an affidavit to support a motion for a temporary restraining order, Rule 65(b) (1) (A). Verification or an affidavit may be required in receivership proceedings, Rule 66. Supplemental Rule B(1) (A) requires a verified complaint to support attachment in an in personam action in admiralty. Rule C(2) requires verification of the complaint in an in rem action. Those are the only rules provisions that come to mind at the

electronic means that are consistent with any technical standards ~~or standards of form~~² established by the Judicial Conference of the United States. ~~A local rule may require electronic filing only if reasonable exceptions are allowed. But paper filing must be allowed for good cause, and may be required or allowed for other reasons by local rule.~~ A paper filed electronically ~~in accordance with a local rule~~ is a written paper for purposes of these rules.

COMMITTEE NOTE

Electronic filing has matured. Most districts have adopted local rules that require electronic filing, and allow reasonable exceptions as required by the former rule. The time has come to seize the advantages of electronic filing by making it mandatory in all districts. But exceptions continue to be available. Paper filing must be allowed for good cause. Many courts now have local rules that provide for paper filing by pro se litigants, and may carry those rules forward. And a local rule may allow or require paper filing for other reasons.³

The means of electronic signing are left open; local rules can specify appropriate means. If the Judicial Conference adopts standards that govern the means or form of electronic signing, they may displace local rules.⁴

The amended rule applies directly to the filer's

moment. Statutes also may require verification. There may be circumstances in which a federal court will adopt a state-law verification requirement, although that seems uncertain.

If verification is accomplished by the filer, the signature would have to be accompanied by some sort of statement that the paper is verified. Perhaps it is better, after all, to retain "verified" in rule text?

² This phrase likely should be omitted. It was included to recognize that Judicial Conference standards might go beyond the electronic technology to address such issues as whether a machine signature should be preceded by /s/ or some such (L.S.? locus sigilli?).

³ Examples could be given of good cause, or other exceptions, but this may be a case where a terse Note is better.

⁴ Civil Rule 11(a) provides that every pleading, written motion, and other paper must be signed. Rule 5(d)(3) already provides that a paper filed electronically in accordance with a local rule is a written paper for purposes of the Civil Rules. It seems useful to carry this provision forward in this place, not Rule 11, omitting only the reference to local rules.

signature.⁵ It does not address others' signatures. Many filings include papers signed by someone other than the filer. Examples include affidavits and declarations and, when filed, discovery materials. Provision for these signatures may be made by local rule, as many courts do now, unless the Judicial Conference adopts a preemptive national standard.⁶

[The former provision for verification by electronic means is omitted. Verification is not often required by these rules. The special policies that justify a verification requirement suggest that it is better to defer electronic verification **pending further experience; local rules may provide useful experience.**]⁷

Alternative 2

Alternative 2 has become the preferred version of at least most of the reporters and the Civil Rules Committee members who have participated in the subcommittee work.

- (3) ~~*Electronic Filing, and Signing, or Verification. A court may, by local rule, allow papers to be filed*~~ All filings must be made, signed, or verified by electronic means that are consistent with any technical standards established by the Judicial Conference of the United States. But paper filing must be allowed for good cause, and may be required or allowed for other reasons by local rule. The act of electronic filing constitutes the signature of the person who makes the filing. A paper filed electronically in accordance with a local rule is a written paper for purposes of these rules.

COMMITTEE NOTE

Electronic filing has matured. Most districts have adopted local rules that require electronic filing, and allow reasonable exceptions as required by the former rule. The time has come to seize the advantages of electronic filing by making it mandatory in all districts. But exceptions continue to be available. Paper filing must be allowed for good cause. And a local rule may allow **or require paper filing for other reasons. Many courts now have**

⁵ Should this proposition be asserted more directly in rule text? E.g., "must be made and signed by the filer"?

⁶ Alternative 2, below, avoids the questions raised by attempting to address non-filer signatures in a Committee Note to a rule that does not directly address the question.

⁷ See footnote 1.

local rules that provide for paper filing by pro se litigants,
and may carry those rules forward.

The act of electronic filing by an authorized user of the court's system counts as the filer's signature. Under current technology, the filer must log in and present a password. Those acts satisfy the purposes of requiring a signature without need for an additional electronic substitute for a physical signature. But the rule does not make it improper to include an additional "signature" by any of the various electronic means that may indicate an intent to sign.

The amended rule applies directly to the filer's signature. It does not address others' signatures. Many filings include papers signed by someone other than the filer. Examples include affidavits and declarations and, when filed, discovery materials. Provision for these signatures may be made by local rule, but if the Judicial Conference adopts standards that govern the means or form of electronic signing, they may displace local rules.

[The former provision for verification by electronic means is omitted. Verification is not often required by these rules. The special policies that justify a verification requirement suggest that it is better to defer electronic verification **pending further experience. Local rules may address verification by electronic means.**]

e-Service

Civil Rule 5(b) (2) (E)

(b) Service: How Made. * * *

(2) Service in General. A paper is served on the person to be served⁸ under this rule by:

(A) handing it to the person * * *

⁸ This provision is included to address the question that arises when readers confront "the person" in (E). The stylists chose to use "the person" throughout (A), (B), (C), (D), (E), and (F). We cannot simply add "the person to be served" in (E) and leave the others untouched.

Adding "to be served" to all the other subparagraphs is awkward because "the person's" appears in (B) (i), (B) (ii), and (C).

But it works to add "on the person to be served" in the introduction. Do we want to second-guess the style choice?

- (E) sending it by electronic means ~~if the person consented in writing, unless the person shows good cause to be exempted from such service or is exempted by local rule. -in which event~~ Electronic service is complete upon transmission, but is not effective if the serving party learns that it did not reach the person to be served; or * * *

COMMITTEE NOTE

Provision for electronic service was first made when electronic communication was not as widespread or as fully reliable as it is now. Consent of the person served to receive service by electronic means was required as a safeguard. Those concerns have substantially diminished. The amendment makes electronic service the standard. But it also recognizes that electronic service is not always effective. Some litigants lack access to suitable electronic devices. Exceptions are available on showing good cause in a particular case. And local rules may establish other exceptions [that reflect local experience].

Notice of Filing as Proof of Service

Civil Rule 5(d) (1)

(d) Filing.

- (1) Required Filings; Certificate of Service. Any paper after the complaint that is required to be served—~~together with a certificate of service—~~ must be filed within a reasonable time after service; a certificate of service also must be filed, but a notice of electronic filing constitutes a certificate of service on any party served through the court's transmission facilities [unless the serving party learns that it did not reach the party to be served].

COMMITTEE NOTE

The amendment provides that a notice of electronic filing generated by the court's CM/ECF system is a certificate of service on any party served through the court's transmission facilities. But if the serving party learns that the paper did not reach the party to be served, there is no service under Rule 5(b)(2)(E) and there is no certificate of the (nonexistent) service.

[When service is not made through the court's transmission facilities, a certificate of service must be filed and should specify the date as well as the manner of service.]

Rule 5(d)(1) addresses the certificate of service only. It does not address electronic service or a failure of electronic service.⁹

⁹ This brief sentence seems better than any attempt to explore what the person who attempted electronic service should do on learning that service failed. Information about the failure may be provided when the person to be served asks whether it will be receiving such a paper. More often, it will be provided when the attempted service is bounced back through the system. A study in the Southern District of Indiana found that most often the "bounceback" reflected failure of service on a secondary target, an assistant to the attorney or a paralegal, at the same time as the attorney was in fact served. There may be little point in requiring a renewed effort to serve a duplicate on the assistant, along with a certificate of service.

Alternatively, this paragraph could be dropped. Rule 5(b)(2)(E) addresses failure of electronic service. Why bother to state the obvious – that proposed Rule 5(d)(1) does not?

TAB 8A

MEMO TO: Members, Criminal Rules Advisory Committee

FROM: Professors Sara Sun Beale and Nancy King, Reporters

RE: Rule 35, 15-CR-A

DATE: February 25, 2015

Kevin Bennardo, Visiting Associate Clinical Professor of Law at the Robert H. McKinney School of Law, Indiana University at Indianapolis, has submitted a proposal to amend Rule 35 to provide authority for a district court to reduce a sentence based on the defendant's "acceptance of punishment," if the parties make a joint motion within 14 days and the defendant promises "not to appeal her punishment either in whole or in part." The proposal is explained further in a law review article, "Post-Sentencing Appellate Waivers," 48 U. MICH. L. REF. 347 (2015). Professor Bennardo's letter proposing this amendment appears as Tab B.

Because the proposal was submitted shortly before the agenda book was being compiled, a more detailed evaluation of the proposal by the Reporters has not been prepared.

TAB 8B



**ROBERT H. MCKINNEY
SCHOOL OF LAW**

INDIANA UNIVERSITY
Indianapolis

Kevin Bennardo
Visiting Associate Clinical Professor of Law
(317) 278-8574 • kbennard@iupui.edu

February 17, 2015

Committee of Rules of Practice and Procedure
Advisory Committee on Criminal Rules

Re: Proposed Amendment to Fed. R. Crim. P. 35 to permit sentence
reductions for acceptance of punishment

Judge Raggi and Members of the Advisory Committee on Criminal Rules,

I write to propose an amendment to Rule 35 of the Federal Rules of Criminal Procedure. The overarching idea behind the proposal is that appellate waiver agreements in which a defendant promises not to appeal her sentence should occur *after* sentencing rather than as part of the plea agreement. In order for such a system to work, a defendant's sentence must be susceptible to a reduction to reflect the post-sentencing appellate waiver through Rule 35.

Broadly speaking, the current system of plea agreement appellate waivers is inefficient and skews incentives. First, by removing the threat of reversal from sentencing hearings, it removes an important incentive to ensure that district court judges properly conduct sentencing hearings according to the procedure laid out in federal law. Second, bargaining over appellate waivers is inefficient at the pre-plea stage because neither the defendant nor the Government can properly value the defendant's right to an appeal at that stage. This bargaining inefficiency wastes resources and leads to aborted appellate waivers and plea bargains. Third, the current system fails to adequately deter defendants from breaching their appellate waivers. Defendants currently face no sanction for breach aside from the dismissal of their appeal; thus breaching defendants end up in no worse position than defendants who abide by their promise not to appeal.

Making the appellate waiver a stand-alone agreement that takes place *after* the sentencing hearing would significantly reduce these problems. First, the threat of reversal would be re-injected into the sentencing hearing because no one would know whether an appellate waiver would be consummated until after sentencing. Second, bargaining over appellate waivers would be much more efficient at the post-sentencing stage because the procedure and outcome of the sentencing hearing would be known, and therefore both parties could fairly accurately value the

defendant's right to appeal and intelligently decide whether to barter over it. Lastly, by moving the appellate waiver into a stand-alone agreement supported by separate consideration, a breaching defendant would suffer a known and easily-imposed consequence and would therefore be deterred from breach.

As consideration for the post-sentencing appellate waiver, I envision that the Government would offer some incremental reduction of punishment. If the defendant agreed, the Government and the defendant would file a joint "Motion for Reduction of Sentence for Acceptance of Punishment" within fourteen days of the sentencing hearing. The motion would automatically stay the appeal period. The district court would have discretion to accept or reject the motion and the sentence reduction. If accepted by the district court, the defendant would receive the sentence reduction. If the defendant then breached by appealing, the Government could move to have the incremental sentence reduction removed and the original sentence reinstated.

I've set forth a much deeper analysis of the flaws of the current appellate waiver system and my proposal for a post-sentencing appellate waiver system in the attached article, *Post-Sentencing Appellate Waivers*, which was recently published by the University of Michigan Journal of Law Reform. I am certainly not tied to any particular text for the amendment, but what follows is a rough proposal:*

FEDERAL RULE OF CRIMINAL PROCEDURE 35. CORRECTING OR REDUCING A SENTENCE

(d) REDUCING A SENTENCE FOR ACCEPTANCE OF PUNISHMENT.

(1) Within fourteen days after sentencing, the parties may jointly move the court for a reduction of sentence based on the defendant's acceptance of punishment. Such a motion automatically stays the appeal period provided by Fed. R. App. P. 4(b)(1)(A) until the court rules on the motion.

(2) The court has discretion to grant or deny the motion. In exercising that discretion, the court should consider whether granting the motion would further the interests of justice, including the purposes of punishment set forth in 18 U.S.C. § 3553(a).

(3) For purposes of Rule 35(d), a defendant's acceptance of punishment must be evidenced by a promise not to appeal her punishment either in whole or in part. The court's denial of a motion under Rule 35(d) relieves the defendant of her promise not to appeal her punishment.

(4) When acting under Rule 35(d), the court may not reduce the sentence to a level below the minimum sentence established by statute unless the sentence being reduced was already below the minimum sentence established by statute.

* Although I've styled my proposal as subsection (d) to Rule 35, it would likely make more sense to insert the proposed amendment as subsection (c) and to move the current subsection (c) defining "sentencing" to a new subsection (d).

I very much appreciate the committee's consideration of my proposal. If adopted, I believe a system of stand-alone post-sentencing appellate waivers would lead to more efficient bargaining, better adherence to proper procedure in sentencing hearings and therefore more substantively reasonable sentences, and fewer breaching defendants. Aside from these incentive-based reasons, a defendant who accepts her sentence displays respect for the justice system that counsels in favor of a shorter period of incapacitation and a reduced need for deterrence and rehabilitation. In short, I believe the proposed amendment would lead to a more just and fair system of federal punishment.

Please let me know if you have any questions or if I can be of any service to the committee during the consideration process.

Best regards,



Kevin Bennardo

2015

Post-Sentencing Appellate Waivers

Kevin Bennardo

Indiana University Robert H. McKinney School of Law

Follow this and additional works at: <http://repository.law.umich.edu/mjlr>



Part of the [Courts Commons](#), and the [Criminal Procedure Commons](#)

Recommended Citation

Kevin Bennardo, *Post-Sentencing Appellate Waivers*, 48 U. MICH. J. L. REFORM 347 (2015).

Available at: <http://repository.law.umich.edu/mjlr/vol48/iss2/2>

This Article is brought to you for free and open access by the Journals at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in University of Michigan Journal of Law Reform by an authorized administrator of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

POST-SENTENCING APPELLATE WAIVERS

Kevin Bennardo*

A sentencing appellate waiver is a criminal defendant's promise not to appeal her sentence. These provisions routinely appear in federal defendants' plea agreements. With a few narrow exceptions, a knowing and voluntary sentencing appellate waiver bars a defendant from appealing all issues within the waiver's scope. Using models of judicial behavior and empirical studies, this Article argues that the inclusion of sentencing appellate waivers in plea agreements creates bargaining inefficiencies and removes important incentives from the sentencing process. As a solution, the Article proposes that sentencing appellate waivers should take the form of separate post-sentencing agreements.

INTRODUCTION

Since their popular inception approximately twenty years ago, sentencing appellate waivers have become more prevalent than ever in the federal courts. These waivers, executed as part of a defendant's plea agreement, relinquish the defendant's right to appeal her yet-to-be-imposed sentence. This Article argues that the timing of these waivers is problematic. By pre-dating sentencing by months, these waivers are inefficient and skew the incentives of the stakeholders in the sentencing process in troubling ways: the parties cannot accurately value their rights during the bargaining process; district courts know the sentence is virtually unreviewable and therefore lack incentives to observe proper sentencing practices; and the government cannot impose meaningful consequences on a breaching defendant, thereby reducing the likelihood that defendants will adhere to their waiver agreements.

Postponing sentencing appellate waiver agreements until after sentencing would rectify these ills and conserve appellate resources. Under this proposed system, the defendant and the government could negotiate over a separate post-sentencing appellate waiver in exchange for a sentence reduction subject to the approval of the district court.

* Visiting Associate Clinical Professor of Law, Indiana University Robert H. McKinney School of Law. The research for this Article was completed during the author's tenure as a Teaching Fellow at the Louisiana State University Paul M. Hebert Law Center, and the author extends great appreciation to that institution for its support. The author is especially thankful to Bill Corbett, Mark Glover, and Ken Levy for their thoughtful comments.

Part I of this Article sets forth the mechanics of the current system of plea agreement sentencing appellate waivers. Part II recounts the numerous criticisms of the current appellate waiver system and the federal courts of appeals' refutation of these critiques. Part III uses models of judicial decision-making to hypothesize the likely effect of sentencing appellate waivers on the sentencing process. That Part concludes that a district court's knowledge that a sentencing appellate waiver exists influences sentencing procedures and outcomes. Part IV establishes the mechanics of the proposed post-sentencing appellate waiver system, describes its advantages compared to the current system, and responds to anticipated criticisms. Instead of permitting "a lawless district court"¹ to deviate from proper sentencing practices, the proposed post-sentencing appellate waiver system incentivizes lawfulness while vindicating the parties' freedom to engage in self-interested bargaining.

I. MECHANICS OF SENTENCING APPELLATE WAIVERS

Appellate waiver provisions rose to popularity in the 1990s² and are today common components of plea agreements in many federal districts.³ The garden-variety appellate waiver is a provision in a defendant's plea agreement that waives the defendant's right to appeal her conviction, her sentence, or both.⁴ The parties are free to customize these waivers on a case-by-case basis, and, as a result, the waivers vary widely in scope from broad blanket waivers of "all"

1. Memorandum from Acting Ass't Att'y Gen. John C. Keeney for all United States Attorneys (Oct. 4, 1995), *reprinted in* 10 FED. SENT'G REP. 209, 210 (1998).

2. Noted reasons for the rise of appellate waivers include (1) the high number of sentencing appeals in the wake of the Sentencing Reform Act of 1984, (2) the federal appellate courts' positive reception of appellate waivers, and (3) the above-cited Keeney memorandum advising federal prosecutors to consider including appellate waivers in plea agreements. Catharine M. Goodwin, *Summary: 1996 Committee on Criminal Law Memo on Waivers of Appeal and Advise of the Rights to Appeal*, 10 FED. SENT'G REP. 212, 212 (1998); *see also* Memorandum from Acting Ass't Att'y Gen. John C. Keeney for all United States Attorneys, *supra* note 1, at 210 (urging that "the use of these waivers in appropriate cases can be helpful in reducing the burden of appellate and collateral litigation involving sentencing issues.").

3. An empirical study of 971 federal plea agreements in 2003 found that almost two-thirds contained an appellate waiver provision. Nancy J. King & Michael E. O'Neill, *Appeal Waivers and the Future of Sentencing Policy*, 55 DUKE L.J. 209, 212 (2005); *see also* Robert K. Calhoun, *Waiver of the Right to Appeal*, 23 HASTINGS CONST. L.Q. 127, 211 (1995) (labeling appellate waivers "a dominant feature of the plea bargaining landscape").

4. An empirical study found that a little less than two-thirds of appellate waivers include the right to appeal both the sentence and conviction, while a little more than one third barred review of the sentence only. King & O'Neill, *supra* note 3, at 242-43. Pressure to waive appellate rights is reportedly most intense in the area of sentencing appeals. *See* Calhoun, *supra* note 3, at 135.

appellate rights to individually-tailored waivers in which the defendant retains the right to appeal specified aspects of the sentence under particular conditions.⁵

The plea-bargaining and guilty-plea processes predate the sentencing hearing by weeks if not months. At the plea hearing, also known as the “Rule 11 hearing,” the parties are required to disclose to the district court that a plea agreement exists.⁶ Federal plea agreements may take one of three forms: (1) binding on the government to dismiss or forego charges, (2) binding on the government to recommend (or not oppose) a particular sentence or calculation under the U.S. Sentencing Guidelines, and (3) binding on the court to impose a particular sentence or reach a particular calculation under the U.S. Sentencing Guidelines.⁷ Under the first type, the district court is free to accept or reject the plea agreement, and the defendant can withdraw her guilty plea if the government does not uphold its end of the bargain.⁸ Under the second type, the defendant is again free to withdraw the plea if the

5. Roger W. Haines, Jr., *Waiver of the Right to Appeal Under the Federal Sentencing Guidelines*, 3 FED. SENT'G REP. 227, 229 (1991) (describing various limitations the parties could elect to put on the waiver, such as “retaining the right to appeal if the court departs upward, or if the court refuses to give credit for acceptance of responsibility”); Kevin Bennardo, *A Frank Look at Appellate Waiver in the Seventh Circuit*, 36 S. ILL. U. L.J. 531, 531–32, 532 n.4 (2012) (listing examples of restrictive waivers); see Goodwin, *supra* note 2, at 212–13 (providing examples of “relatively narrow” waivers, “such as where a defendant waives the right to appeal only if he or she receives a sentence within the range which both parties agree is appropriate”); see also King & O’Neill, *supra* note 3, at 244 (finding that only twenty-one percent of appellate waivers place no limitations on the waiver, while the most common limitations are the retention of the right to appeal an upward departure from the Guidelines range (36.5% of waivers), a sentence above the statutory maximum (28.9%), ineffective assistance of counsel (28.6%), and a sentence above a specified range (22.8%)). Companion provisions to an appellate waiver may include waivers of the defendant’s right to collaterally attack her conviction or sentence through habeas corpus or the right to move for a later reduction of sentence pursuant to 18 U.S.C. § 3582(c) (2012). In the same study noted above, almost eighty percent of the defendants who had waived the right to appeal had also waived collateral review. King & O’Neill, *supra* note 3, at 242–43. The federal appellate courts have similarly held collateral attack waivers enforceable. See, e.g., *DeRoo v. United States*, 223 F.3d 919, 923 (8th Cir. 2000) (“As a general rule, we see no reason to distinguish the enforceability of a waiver of direct-appeal rights from a waiver of collateral-attack rights in the plea agreement context.”). A pleading defendant may also waive the right to seek relief through a section 3582(c) motion, which seeks a reduction of sentence based on the reduction of a sentencing range under the U.S. Sentencing Guidelines Manual. See *United States v. Gordon*, 480 F.3d 1205, 1208 (10th Cir. 2007) (plea agreement contained an explicit waiver of right to move for a sentence reduction under section 3582(c)); cf. *United States v. Monroe*, 580 F.3d 552, 558–59 (7th Cir. 2009) (without a specific provision addressing section 3582(c), appellate and collateral attack waivers did not bar motion under section 3582(c)); *United States v. Chavez-Salais*, 337 F.3d 1170, 1173 (10th Cir. 2003).

6. FED. R. CRIM. P. 11(c)(2).

7. See FED. R. CRIM. P. 11(c)(1).

8. FED. R. CRIM. P. 11(c)(1)(A), (3)(A), (4), (5).

government breaches by failing to make the agreed-upon recommendation. The court is, however, free to ignore the recommendation, and the defendant may not withdraw her guilty plea merely because the court imposed a harsher punishment than was recommended.⁹ Under the third type, known as a “C” plea because of its home in subpart C of Rule 11, the district court is bound to adhere to the parties’ recommendation if it accepts the plea agreement.¹⁰ The defendant is free to withdraw her plea if the district court rejects the plea agreement.¹¹

At the plea hearing, the district court must ensure that the defendant understands the host of rights that she is foregoing by pleading guilty, a process known as the plea colloquy.¹² If the plea agreement contains an appellate waiver provision, the district court must specifically question the defendant about the appellate waiver during the plea colloquy.¹³ Only upon finding that the defendant is entering her guilty plea knowingly and voluntarily may the district court accept the defendant’s guilty plea.¹⁴

District courts are not bound to accept any plea agreements. Thus, district court judges are free to categorically reject plea agreements that contain appellate waiver provisions.¹⁵ Moreover, district courts may reject appellate waiver provisions in specific cases if either the defendant fails to understand the significance of the

9. FED. R. CRIM. P. 11(c)(1)(B), (3)(B).

10. FED. R. CRIM. P. 11(c)(1)(C), (3)(A), (4).

11. FED. R. CRIM. P. 11(c)(5), (d)(2).

12. FED. R. CRIM. P. 11(b)(1).

13. FED. R. CRIM. P. 11(b)(1)(N).

14. FED. R. CRIM. P. 11(b)(2). The court must also determine the existence of a factual basis for the guilty plea, but that determination need only precede the entry of judgment. FED. R. CRIM. P. 11(b)(3).

15. See Douglas A. Berman, *Windows into Sentencing Policy and Practice: The Crack/Cocaine Ratio and Appeal Waivers*, 10 FED. SENT’G REP. 179, 181 (1998); see also FED. R. CRIM. P. 11(c) (granting district courts the authority to reject plea agreements). Judges Greene and Friedman of the District Court for the District of Columbia categorically refused to accept plea agreements containing waivers of the right to appeal unknown and yet-to-be-imposed sentences. See, e.g., *United States v. Johnson*, 992 F. Supp. 437, 438–40 (D.D.C. 1997); *United States v. Raynor*, 989 F. Supp. 43, 48–49 (D.D.C. 1997). In the District of Massachusetts, Judge Gertner found appellate waivers unacceptably violative of public policy. *United States v. Perez*, 46 F. Supp. 2d 59, 64–72 (D. Mass. 1999). Although the Fifth Circuit held appellate waivers enforceable, it explicitly noted that “there may be sound policy reasons for refusing to accept such waivers, and that district courts might disagree with the policy choice made by the court in this case to accept a plea agreement appeal waiver.” *United States v. Melancon*, 972 F.2d 566, 568 (5th Cir. 1992).

provision¹⁶ or the district court believes that the provision does not serve the interests of justice.¹⁷

After a defendant enters a guilty plea, a probation officer creates a presentence investigation report.¹⁸ This report contains a calculation of the defendant's advisory sentencing range from the U.S. Sentencing Guidelines Manual.¹⁹ The defendant can object to information contained in the presentence investigation report, including the probation officer's Guidelines calculation.²⁰ At the sentencing hearing, the district court must resolve any disputes regarding the presentence investigation report²¹ and calculate the defendant's advisory Guidelines range of imprisonment on the record.²² The court may receive evidence and witness testimony at the sentencing hearing,²³ and the resulting factual determinations may bear heavily on the Guidelines calculation.²⁴ Although the district court is not bound to impose a sentence within the Guidelines range,²⁵ a sentence within the Guidelines range receives a presumption of reasonableness on appeal in the majority of circuits.²⁶ The district court often enters judgment on the same day as sentencing. A defendant has fourteen days following the entry of judgment to file a notice of appeal.²⁷

The federal courts of appeals have uniformly held that appellate waiver provisions are enforceable,²⁸ including waiver of the right to

16. *See, e.g.*, *United States v. Soon Dong Han*, 181 F. Supp. 2d 1039, 1045 (N.D. Cal. 2002) (finding the specific defendant's waiver was not knowing and voluntary).

17. *See, e.g.*, *United States v. Vanderwerff*, No. 12-cr-00069, 2012 WL 2514933, at *5–6 (D. Colo. June 28, 2012) (rejecting plea agreement because the court found that the defendant's circumstances did not justify the appellate waiver provision contained therein).

18. FED. R. CRIM. P. 32(c), (d).

19. *See* FED. R. CRIM. P. 32(d)(1).

20. *See* FED. R. CRIM. P. 32(f).

21. FED. R. CRIM. P. 32(i)(3).

22. 18 U.S.C. § 3553(a)(4) (2012); *Gall v. United States*, 552 U.S. 38, 49 (2007) (“[A] district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range.”).

23. FED. R. CRIM. P. 32(i)(2).

24. Many Guidelines calculations turn on factual findings, such as the degree of bodily injury the victim suffered, the dollar amount of the victim's loss, or whether a firearm was discharged, brandished, possessed, or otherwise used in the course of the offense. *E.g.*, U.S. SENTENCING GUIDELINES MANUAL § 2B3.1(b)(2), (3), (7) (2013) (robbery offense guideline).

25. The Guidelines were downgraded to “advisory” status in *United States v. Booker*, 543 U.S. 220, 245 (2005).

26. *See United States v. Carty*, 520 F.3d 984, 993–94 & n.9 (9th Cir. 2008) (listing cases of other circuits but declining to adopt such a presumption of reasonableness); *see also Rita v. United States*, 551 U.S. 338, 347 (2007) (permitting the federal courts of appeal to apply a presumption of reasonableness to a sentence within a properly-calculated Guidelines range).

27. FED. R. APP. P. 4(b)(1)(A).

28. *See, e.g.*, *United States v. Guillen*, 561 F.3d 527, 529–31 (D.C. Cir. 2009); *United States v. Hahn*, 359 F.3d 1315, 1318, 1324–28 (10th Cir. 2004) (en banc) (per curiam); *United States v. Andis*, 333 F.3d 886, 889–92 (8th Cir. 2003) (en banc); *United States v.*

appeal sentencing error.²⁹ Because an appellate waiver only precludes a defendant from appealing issues that fall within the scope of the waiver,³⁰ a defendant does not violate an appellate waiver agreement until she files an opening brief raising a waived issue as the basis for her appeal. Although the mechanics vary by circuit, a common system of appellate waiver enforcement requires a government motion to dismiss the defendant's appeal once the defendant-appellant files her opening brief.³¹ After permitting the defendant-appellant to respond to the motion, the appellate court will generally rule on the motion to dismiss before requiring the government to file a response to the defendant's appellate brief.³²

Appellate waivers are generally enforced as long as the appealed issue is within the scope of the waiver and the defendant entered

Teeter, 257 F.3d 14, 21–23 (1st Cir. 2001); *United States v. Khattak*, 273 F.3d 557, 560–62 (3d Cir. 2001); *United States v. Schmidt*, 47 F.3d 188, 190–92 (7th Cir. 1995); *United States v. Ashe*, 47 F.3d 770, 775–76 (6th Cir. 1995); *United States v. Yemitan*, 70 F.3d 746, 747–48 (2d Cir. 1995); *United States v. Melancon*, 972 F.2d 566, 567 (5th Cir. 1992); *United States v. Wiggins*, 905 F.2d 51, 52–53 (4th Cir. 1990); *United States v. Navarro-Botello*, 912 F.2d 318, 321–22 (9th Cir. 1990).

29. See Calhoun, *supra* note 3, at 143 (describing the federal courts' approach to sentencing appellate waivers as "very expansive").

30. Matters that fall outside of the scope of an appellate waiver are not waived. See, e.g., *United States v. Corso*, 549 F.3d 921, 927 (3d Cir. 2008). Courts construe appellate waivers narrowly and resolve any ambiguities "in favor of a defendant's appellate rights." *Andis*, 333 F.3d at 890 (8th Cir. 2003); see also *Khattak*, 273 F.3d at 562 ("[W]aivers of appeals should be strictly construed."); *Hahn*, 359 F.3d at 1325; *United States v. Ready*, 82 F.3d 551, 556 (2d Cir. 1996). But see *United States v. Quintero*, 618 F.3d 746, 750 (7th Cir. 2010) ("[W]e will enforce a waiver only if the disputed appeal falls within the *general ambit* of the waiver.") (emphasis added).

31. For example, the Sixth Circuit "strongly encourage[s] the government to promptly file a motion to dismiss the defendant's appeal where the defendant waived his appellate rights as part of a plea agreement." *United States v. McGilvery*, 403 F.3d 361, 363 (6th Cir. 2005). Other circuits have established similar procedures. See, e.g., *Hahn*, 359 F.3d at 1328 (evaluating appellate waiver enforcement before the filing of substantive briefs); *United States v. Marin*, 961 F.2d 493, 494 (4th Cir. 1992) (granting the government's motion to dismiss the appeal on the basis of an appellate waiver).

32. Rather than entering an order of dismissal, some appellate courts take the more questionable step of affirming the district court's judgment when enforcing an appellate waiver. E.g., *Khattak*, 273 F.3d at 563 (enforcing appellate waiver and affirming on basis of lack of jurisdiction); *Navarro-Botello*, 912 F.2d at 319.

The *sua sponte* enforcement of appellate waivers on the court's own initiative is a similarly questionable practice because appellate waivers are not properly regarded as jurisdictional. But see *Schmidt*, 47 F.3d at 190 (dismissing appeal on the basis of appellate waiver even though the government did not seek enforcement of the waiver). Some courts improperly consider appellate waivers as jurisdictional. E.g., *Khattak*, 273 F.3d at 563 (stating that enforcement of defendant's appellate waiver deprived the court of "jurisdiction to consider the merits of his appeal"). But see *Schmidt*, 47 F.3d at 194 (Ripple, J., dissenting) ("It is not our task to insist on a bargain that the government, the only party which might benefit from it, does not want to enforce."); *Nunez v. United States*, 546 F.3d 450, 452 (7th Cir. 2008) ("[T]he United States, as the waiver's beneficiary, may freely give up its protection."); *Hahn*, 359 F.3d at 1320–24 (asserting jurisdiction despite a valid appellate waiver).

into the waiver knowingly and voluntarily. The federal appellate courts have, however, carved out narrow exceptions to the operation of appellate waivers. Notwithstanding a valid appellate waiver, the appellate courts will entertain an appeal on the grounds that the defendant was sentenced in excess of the statutory maximum³³ or based on an impermissible factor, such as race.³⁴ Additionally, some circuits will refuse to enforce an appellate waiver if enforcing the waiver would constitute a “miscarriage of justice.”³⁵ The Fourth Circuit declined to enforce an otherwise valid appellate waiver

33. See, e.g., *United States v. Gibson*, 356 F.3d 761, 765 (7th Cir. 2004); *Teeter*, 257 F.3d at 25 n.10; *Marin*, 961 F.2d at 496. Further, a sentence below the statutory minimum can provide for an appeal despite a valid appellate waiver. Cf. *United States v. Cieslowski*, 410 F.3d 353, 363 (7th Cir. 2005) (noting that an agreed-upon sentence “must comply with the maximum (and minimum, if there is one) provided by the statute of conviction”); *Andis*, 333 F.3d at 891–92 (describing illegal sentences as those that fall outside the statutory limits).

34. See, e.g., *United States v. Guillen*, 561 F.3d 527, 531 (D.C. Cir. 2009); *United States v. Brown*, 232 F.3d 399, 403 (4th Cir. 2000); see also Goodwin, *supra* note 2, at 212 (“[C]ertain issues are never waived, such as sentences which are plainly illegal because they . . . [are] based on a factor such as race, gender or religion.”) (internal footnotes omitted).

35. *Teeter*, 257 F.3d at 25–26 (stating that what constitutes a miscarriage of justice “is more a concept than a constant” and identifying non-exclusive factors: “the clarity of the error, its gravity, its character (e.g., whether it concerns a fact issue, a sentencing guideline, or a statutory maximum), the impact of the error on the defendant, the impact of correcting the error on the government, and the extent to which the defendant acquiesced in the result.”); *Khattak*, 273 F.3d at 563 (adopting the *Teeter* factors); cf. *Andis*, 333 F.3d at 891 (cautioning that the miscarriage of justice exception is a “narrow one” and listing non-exhaustive examples such as a sentence that exceeds the statutory maximum or fails to comply with the plea agreement); *Hahn*, 359 F.3d at 1327 (limiting the miscarriage of justice exception to: (1) a sentence imposed on account of an impermissible factor such as race, (2) ineffective assistance of counsel in connection with the negotiation of the waiver, (3) a sentence that exceeds the statutory maximum, or (4) a waiver that is otherwise unlawful such that the error seriously affects the fairness, integrity, or public reputation of judicial proceedings).

Courts and scholars have critiqued the miscarriage of justice exception for its vagueness and inconsistent administration. See *Andis*, 333 F.3d at 895–96 (Arnold, J., concurring) (stating that the difficulty of applying the vague miscarriage of justice exception on a case by case basis creates inefficiencies that undermine the purpose of appellate waivers); *Hahn*, 359 F.3d at 1344 n.9 (Murphy, J., dissenting) (criticizing the miscarriage of justice exception because its vagueness encourages defendants with appellate waivers to appeal and discourages the government from entering into appellate waiver agreements); Kristine Malmgren Yeater, Note, *Third Circuit Appellate Waivers: The Mysterious Miscarriage of Justice Standard*, 1 DUQ. CRIM. L.J. 94, 94, 103 (2010) (criticizing the Third Circuit’s application of the miscarriage of justice exception as ill-defined and inconsistent); Derek Teeter, Comment, *A Contracts Analysis of Waivers of the Right to Appeal in Criminal Plea Bargains*, 53 U. KAN. L. REV. 727, 728 (2005) (labeling the miscarriage of justice exception “unworkable, unpredictable, and unfair to defendants and prosecutors”). One troubling formulation is the D.C. Circuit’s statement that a miscarriage of justice occurs “[i]f, for example, the district court utterly fails to advert to the factors in 18 U.S.C. § 3553(a).” *Guillen*, 561 F.3d at 531. This broad formulation devalues appellate waivers. Defendants often allege that the district court failed to adhere to the statutory sentencing factors of subsection 3553(a). Resolution of this issue would require the appellate court to fully consider the sentencing record to determine whether a miscarriage of justice occurred, thereby nullifying the resource-saving benefit of the appellate waiver.

where the defendant claimed a denial of the right to assistance of counsel at sentencing.³⁶ Other circuits have not been so charitable and have routinely found that appellate waivers bar a later claim of ineffective assistance of counsel at sentencing.³⁷ Appellate claims of other constitutional violations—such as violation of the Eighth Amendment’s prohibition against cruel and unusual punishment or the Fifth Amendment’s double jeopardy clause—are not recognized as exceptions to appellate waivers.³⁸

The defendant can always appeal issues concerning the validity of the plea agreement or of the waiver itself because such issues relate to the knowing and voluntary nature of the agreement.³⁹ For example, the waiver agreement cannot relinquish a claim that the plea agreement itself was the product of ineffective assistance of counsel because, if the claim is successful, the plea agreement—including the waiver—is itself invalid.⁴⁰ Likewise, an appellate waiver does not preclude a claim that the sentence imposed violated the terms of the plea agreement⁴¹ or that the government breached its obligations under the plea agreement.⁴² These matters are not exceptions to the waiver but rather are considerations bearing on a waiver’s effectiveness. Thus, unless an exception or a

36. *United States v. Attar*, 38 F.3d 727, 732–33 (4th Cir. 1994) (holding that an appellate waiver did not preclude challenge to the sentence where the district court permitted the defense attorney to withdraw at the beginning of the sentencing hearing and defendant proceeded *pro se*).

37. *See, e.g., United States v. White*, 307 F.3d 336, 343 (5th Cir. 2002) (“[A]n ineffective assistance of counsel argument survives a waiver of appeal only when the claimed assistance directly affected the validity of that waiver or the plea itself.”); *Mason v. United States*, 211 F.3d 1065, 1069 (7th Cir. 2000); *United States v. Djelevic*, 161 F.3d 104, 107 (2d Cir. 1998) (*per curiam*) (“emphatically reject[ing]” the defendant’s contention that claims of ineffective assistance of counsel relating to sentencing cannot be waived).

38. *United States v. Davey*, 550 F.3d 653, 658 (7th Cir. 2008) (“We see no reservation in that waiver for constitutional arguments.”); *see also King & O’Neill, supra* note 3, at 249 & n.131 (finding cases in ten circuits enforcing appellate waivers against defendants’ claims that their sentences violated their Fifth and Sixth Amendment rights).

39. *See Calhoun, supra* note 3, at 140–41; Kevin Bennardo, *supra* note 5, at 534–35, 535 n.14 (listing Seventh Circuit cases).

40. *See, e.g., Guillen*, 561 F.3d at 530 (“[B]ecause the defendant’s attorney failed to ensure the defendant understood the consequences of his waiver, the waiver was not knowing, intelligent, and voluntary.”).

41. *See, e.g., United States v. Teeter*, 257 F.3d 14, 25 n.10 (1st Cir. 2001); *United States v. Michelsen*, 141 F.3d 867, 872 & n.3 (8th Cir. 1998); *United States v. Navarro-Botello*, 912 F.2d 318, 321 (9th Cir. 1990).

42. *See, e.g., United States v. Gonzalez*, 16 F.3d 985, 990 (9th Cir. 1993) (“By opposing the acceptance of responsibility adjustment, the government by its breach of the agreement released [the defendant] from his promise in paragraph 11 not to appeal.”); *United States v. Schwartz*, 511 F.3d 403, 405 (3d Cir. 2008). *But see Bennardo, supra* note 5, at 541–44 (noting inconsistent precedent in the Seventh Circuit regarding the effect of the government’s breach of the plea agreement on a defendant’s appellate waiver).

meritorious claim of invalidity exists, a knowing and voluntary appellate waiver will bar the appellate court from considering any claims within its scope.⁴³

II. PREVIOUS CRITIQUES AND JUSTIFICATIONS OF SENTENCING APPELLATE WAIVERS

In upholding the enforceability of appellate waivers, numerous courts have pointed to the statutory origin of criminal defendants' appellate rights.⁴⁴ Criminal defendants possessed no right to appeal in the federal system until the end of the nineteenth century.⁴⁵ The right to meaningful appellate review of sentencing extends back only as far as the Sentencing Reform Act of 1984.⁴⁶ According to these courts, if a defendant can waive constitutional rights such as the right to a jury trial, she can surely waive a statutory right such as the right to appeal. This syllogism is demonstrably flawed: an individual's ability to waive a right does not depend on whether the right's origins are constitutional or statutory.⁴⁷ Effective waivers of

43. Although the government is capable of waiving its appellate rights along with the defendant, no mutuality of waiver is generally required. See King & O'Neill, *supra* note 3, at 255–56 (reporting that both the defendant and the government waive appeal in only 12.5% of appellate waiver cases). *But see* United States v. Guevara, 941 F.2d 1299, 1299–1300 (4th Cir. 1991) (interpreting a defendant's appellate waiver to implicitly bar the government from appealing).

Scholars have criticized non-mutual appellate waivers. See D. Randall Johnson, *Giving Trial Judges the Final Word: Waiving the Right to Appeal Sentences Imposed Under the Sentencing Reform Act*, 71 NEB. L. REV. 694, 723–24 (1992) (advocating that appellate waivers should be explicitly mutual to be enforceable). A significant drawback of requiring mutuality of appellate waivers is that it forces the defendant to accept the government's appellate waiver as part (or all) of the consideration received in exchange for the defendant's appellate waiver. The defendant may value some other concession by the government more highly, and imposing a mutuality requirement on appellate waivers would diminish the value of a defendant's right to appeal as a bargaining chip.

44. See, e.g., *Teeter*, 257 F.3d at 22 (“Since the Supreme Court repeatedly has ruled that a defendant may waive constitutional rights as part of a plea agreement, it follows logically that a defendant ought to be able to waive rights that are purely creatures of statute.”) (internal citation omitted); United States v. Melancon, 972 F.2d 566, 567 (5th Cir. 1992) (finding that because a defendant may waive constitutional rights in a plea bargain, “[i]t follows that a defendant may also waive statutory rights, including the right to appeal.”); United States v. Wiggins, 905 F.2d 51, 53 (4th Cir. 1990) (“[I]f defendants can waive fundamental constitutional rights such as the right to counsel, or the right to a jury trial, surely they are not precluded from waiving procedural rights granted by statute.”) (internal quotation marks and citation omitted).

45. See *Carroll v. United States*, 354 U.S. 394, 400 & n.9 (1957) (providing a historical account of the right to appeal in federal criminal cases).

46. See Johnson, *supra* note 43, at 695 n.1.

47. *Melancon*, 972 F.2d at 570 (Parker, J., concurring) (deriding this “faulty syllogism”); United States v. Perez, 46 F. Supp. 2d 59, 65–67 (D. Mass. 1999) (“[S]ince not all rights are

statutory rights must be knowing and voluntary, cannot violate public policy, and must comply with due process. The federal appellate courts have rejected challenges to appellate waivers on all three of these grounds. These challenges, as well as the accepted rebuttals to these challenges, are set forth below.

A. *Knowing and Voluntary Waiver*

The federal appellate courts have held that criminal defendants can knowingly and voluntarily waive their prospective sentencing appellate rights.⁴⁸ In the wake of these rulings, modern defendants are left to argue on a case-by-case basis that their individual appellate waivers were uninformed or coerced.

1. Per Se Challenges to Knowledge and Voluntariness

Some courts and commentators have maintained that a waiver of a defendant's right to appeal her sentence is inherently uninformed because the sentence has yet to be imposed or calculated.⁴⁹ A central part of this argument is that a knowing waiver must be

waivable, the syllogism falls short in failing to distinguish, in some principled and contextually sensitive way, between those waivers which are acceptable, and those which are not."); *see also* Johnson, *supra* note 43, at 706 (noting, in due process analysis, that the statutory nature of the right to appeal "has, at most, marginal relevance to whether or not a per se rule of involuntariness is justified with respect to waiver of that right."); Gregory M. Dyer & Brendan Judge, Note, *Criminal Defendants' Waiver of the Right to Appeal—An Unacceptable Condition of a Negotiated Sentence or Plea Bargain*, 65 NOTRE DAME L. REV. 649, 661–63 (1990).

Some individual rights are inherently unwaivable despite their non-constitutional provenance. *See, e.g.*, *United States v. Olano*, 507 U.S. 725, 742 (1993) (Kennedy, J., concurring) (suggesting that a defendant is unable to waive the operation of the federal rule provision that disallows the presence of alternate jurors in the jury room during deliberations); *United States v. Greatwalker*, 285 F.3d 727, 730 (8th Cir. 2002) (holding that parties cannot waive statutory limits on sentencing "[e]ven when a defendant, prosecutor, and court agree").

48. *See, e.g.*, *United States v. Hahn*, 359 F.3d 1315, 1325 (10th Cir. 2004) (en banc) (per curiam); *United States v. Woolley*, 123 F.3d 627, 632 (7th Cir. 1997); *Melancon*, 972 F.2d at 567; *see also* Ginger K. Gooch, Note, *The Message to Criminal Defendants—Waive at Your Own Risk: The Eighth Circuit Enforces Waivers of Appellate Rights*, 64 MO. L. REV. 459, 464 & n.37 (1999).

49. *United States v. Raynor*, 989 F. Supp. 43, 44 (D.D.C. 1997) ("Such a waiver is by definition uninformed and unintelligent and cannot be voluntary and knowing."); *United States v. Johnson*, 992 F. Supp. 437, 439 (D.D.C. 1997); *Melancon*, 972 F.2d at 571 (Parker, J., concurring); Calhoun, *supra* note 3, at 205 ("There is simply no way the accused can be viewed as knowing what he is giving up as a part of his waiver because it has not been determined at the time the plea is entered . . . waivers of this sort simply cannot withstand scrutiny."); Lynn Fant & Ronit Walker, *Reflections on a Hobson's Choice: Appellate Waivers and Sentencing Guidelines*, 11 FED. SENT'G REP. 60, 61 (1998).

grounded in a high level of outcome certainty. For example, a defendant who pleads guilty and waives her right to a jury trial is certain that she will be convicted of a particular count.⁵⁰ A defendant entering into a sentencing appellate waiver is situated differently: “she is freed of none of the uncertainties that surround the sentencing process in exchange for giving up the right to later challenge a possibly erroneous application or interpretation of the Sentencing Guidelines or a sentencing statute.”⁵¹

As a proposed remedy, commentators have suggested that courts should only regard sentencing appellate waivers as “knowing” when the defendant’s guilty plea is conditioned on the imposition of a specific sentence and when the defendant actually receives that sentence.⁵² Under the federal rules, “C” pleas permit the parties to submit a plea agreement to the district court with a binding sentencing recommendation that requires the court either to accept the agreement along with the sentencing recommendation or to refuse it completely.⁵³ According to some appellate waiver critics, precise foreknowledge of the impending sentence negates the otherwise unknowing nature of the sentencing appellate waiver.⁵⁴ Others have suggested that binding a district court to an exact sentence is not necessary, but rather that defendant’s appellate waiver

50. See *Melancon*, 972 F.2d at 572 (Parker, J., concurring) (“While one cannot fully know the consequences of confessing or pleading guilty, one does know what is being yielded up at the time he or she yields it.”).

51. *Raynor*, 989 F. Supp. at 44; see also *Melancon*, 972 F.2d at 572 (Parker, J., concurring) (“This right [to appeal sentencing error] cannot come into existence until after the judge pronounces sentence; it is only then that the defendant knows what errors the district court has made—i.e., what errors exist to be appealed, or waived.”).

52. *Raynor*, 989 F. Supp. at 47–48; Jesse Davis, Note, *Texas Law Rides to the Rescue: A Lone Star Solution for Dubious Federal Presentence Appeal Waivers*, 63 BAYLOR L. REV. 250, 267 (2011); Calhoun, *supra* note 3, at 206 (“When the defendant gets precisely what is bargained for it offends our basic notions of fairness to allow that same defendant to try to improve upon the deal by means of an appeal.”); Comment, *Second Circuit Upholds Plea Provision that Waives Appeal Without Fixed Sentence Range*, 111 HARV. L. REV. 1116, 1119 (1998); David E. Carney, Note, *Waiver of the Right to Appeal Sentencing in Plea Agreements with the Federal Government*, 40 WM. & MARY L. REV. 1019, 1044–45 (1999).

53. FED. R. CRIM. P. 11(c)(1)(C). These so-called “C” pleas are discussed more in depth at text accompanying note 10, *supra*. Empirical research has shown that plea agreements containing appellate waiver provisions are more likely to limit the court’s sentencing options in some way. See King & O’Neill, *supra* note 3, at 239–42; see also *id.* at 251 n.135 (describing one federal public defender’s policy of only entering into a plea agreement containing an appellate waiver provision if it was a Rule 11(c)(1)(C) plea).

54. See, e.g., *Raynor*, 989 F. Supp. at 47–48; Davis, *supra* note 52, at 267; Carney, *supra* note 52, at 1044–45.

is sufficiently knowing as long as the defendant is permitted to appeal a sentence outside of some predetermined range, such as a maximum cap on the term of incarceration.⁵⁵

Courts have rejected this argument, holding that a defendant can knowingly waive her right to appeal her sentence despite the fact that the sentencing hearing has not yet occurred.⁵⁶ Although a defendant is ignorant of the outcome of the sentencing hearing at the time of the waiver, she is aware of the nature of the right she is waiving.⁵⁷ The waiver inquiry focuses on the defendant's understanding of the appellate right that she is waiving, not her knowledge of the sentencing proceeding's outcome.⁵⁸ Thus, courts enforce sentencing appellate waivers as long as the defendant understands the nature of the waiver.⁵⁹

55. For example, Judge Charles Roberts Breyer has proposed limiting appellate waivers in scope to permit the defendant to appeal a sentence above a specified upper limit. *United States v. Soon Dong Han*, 181 F. Supp. 2d 1039, 1044–45 (N.D. Cal. 2002). It is unclear how limited of a ceiling is necessary to satisfy this recommendation because appellate waivers are already not enforceable against claims that the punishment exceeded the statutory maximum. *See supra* note 33. For one commentator's view, see Calhoun, *supra* note 3, at 209–11. Even assuming that commentators could agree upon a precise enough ceiling on a defendant's imprisonment to render the appellate waiver knowing with respect to the term of incarceration, it remains unclear whether similar issues of lack of knowledge would arise with respect to the noncustodial portion of the sentence, such as the terms of the defendant's supervised release.

56. *See United States v. Hahn*, 359 F.3d 1315, 1326–27 (10th Cir. 2004) (en banc) (per curiam); *United States v. Teeter*, 257 F.3d 14, 21–23 (1st Cir. 2001); *Melancon*, 972 F.2d at 567–68; *United States v. Navarro-Botello*, 912 F.2d 318, 320 (9th Cir. 1990); *see also* Calhoun, *supra* note 3, at 202 n.461 (listing cases).

57. *See Haines, Jr.*, *supra* note 5, at 229 (comparing the waiver of the right to appeal a future sentence to the decision to plead guilty under the previously indeterminate sentencing regime); *see also United States v. Guillen*, 561 F.3d 527, 529 (D.C. Cir. 2009) (“An anticipatory waiver—that is, one made before the defendant knows what the sentence will be—is nonetheless a knowing waiver if the defendant is aware of and understands the risks involved in his decision.”); *United States v. Khattak*, 273 F.3d 557, 561 (3d Cir. 2001) (“Waivers of the legal consequences of unknown future events are commonplace.”); *Melancon*, 972 F.2d at 567–68; *United States v. Rutan*, 956 F.2d 827, 830 (8th Cir. 1992); *Navarro-Botello*, 912 F.2d at 320.

58. The choice to plead guilty always involves a calculated risk; appellate waivers are but one dimension of this calculation:

By signing a waiver, defendants gamble that the deals they have negotiated are better than the dispositions they might ultimately receive if they preserved their right to review. Some win this bet, others do not. . . . We simply do not know what proportion of defendants end up worse off because of their waivers.

King & O'Neill, *supra* note 3, at 250.

59. A 1999 amendment to the Federal Rules of Criminal Procedure that required district courts to discuss any applicable appellate waiver with the defendant during the plea colloquy bolstered this interpretation. *See* FED. R. CRIM. P. 11(b)(1)(N). Although the rules advisory committee explicitly stated that it took “no position on the underlying validity” of appellate waivers, FED. R. CRIM. P. 11 advisory committee's notes (referring to the 1999

Others argue that appellate waivers are inherently involuntary or coercive because of the unequal balance of power between the government and the defendant in a criminal prosecution.⁶⁰ Rather than viewing appellate waivers as additional bargaining chips in the defendant's arsenal,⁶¹ these commentators complain that the government extracts appellate waivers as the proverbial ante to participate in plea negotiations and that it offers no consideration in exchange for the waivers.⁶² Some have gone so far as to label appellate waivers "one-sided contract[s] of adhesion."⁶³

The Supreme Court has repeatedly rejected arguments based on the coerciveness of the plea-bargaining process.⁶⁴ Because defendants have no right to a plea agreement, the government is free to

Amendments), the rule amendment solidified appellate waivers as an established component of plea agreements and plea colloquies.

60. See Calhoun, *supra* note 3, at 153–59 (calling for a reevaluation of the constitutionality of plea agreements in general and of the Supreme Court's "central assumption that the defendant and the prosecutor are coequal adversaries in the plea bargaining context" in particular).

Notably, as a basis for revisiting the fairness of the plea-bargaining process, Professor Calhoun identifies the sharply increased penalty ranges the federal determinate sentencing system created and the concomitant increase in the power of the government in defining the sentence at the charging stage. *Id.* at 154–56, 158; see also *United States v. Raynor*, 989 F. Supp. 43, 45 (D.D.C. 1997); *United States v. Johnson*, 992 F. Supp. 437, 439–40 (D.D.C. 1997) (calling the government's bargaining power "utterly superior" to that of criminal defendants "because the precise charge or charges to be brought—and thus the ultimate sentence to be imposed under the guidelines scheme—is up to the prosecution."). Others have likewise argued that the sentencing reforms of the 1980s, including mandatory sentencing guidelines, increased the power of the government at the expense of defendants' ability to voluntarily decline to plea bargain. See Fant & Walker, *supra* note 49, at 61. However, since then, that pressure has abated, at least somewhat, because the Guidelines were downgraded from mandatory to advisory status. See *United States v. Booker*, 543 U.S. 220 (2005).

61. Some courts view enforcing appellate waivers as adding to the reserve of "goods" that a willing defendant may use to entice the government to enter into a favorable plea bargain. See, e.g., *Guillen*, 561 F.3d at 530; *Teeter*, 257 F.3d at 22; *United States v. Yemitan*, 70 F.3d 746, 748 (2d Cir. 1995); see also notes 89–90, *infra*.

62. See Steven L. Chanenson, *Guidance from Above and Beyond*, 58 STAN. L. REV. 175, 182 (2005) ("[T]here is reason to question how much real trading occurs."); Fant & Walker, *supra* note 49, at 60 ("[M]any United States Attorney's Offices require defendants to waive the right to appeal as part of a plea agreement."); Calhoun, *supra* note 3, at 167 ("[A]ppeal waivers look . . . more like the price of admission to engage in the plea bargaining process at all.").

63. *Raynor*, 989 F. Supp. at 49; see also *Johnson*, 992 F. Supp. at 439.

64. See, e.g., *Brady v. United States*, 397 U.S. 742 (1970) (finding a guilty plea to be voluntary even though it was calculated to minimize the likelihood of receiving the death penalty); see also *Johnson*, *supra* note 43, at 707 ("There simply is no reason to believe the Court is inclined to revisit the issue anytime soon."); *Mabry v. Johnson*, 467 U.S. 504, 508 (1984) (stating that plea bargains are "no less voluntary than any other bargained-for exchange" despite the defendant's interest in minimizing punishment); Calhoun, *supra* note 3, at 152 (identifying the "core assumption" in the Supreme Court's plea-bargaining jurisprudence as "a negotiating process characterized by arms-length transactions between parties who enjoy 'relatively equal bargaining power.'") (internal citation omitted).

make a plea agreement contingent on an appellate waiver.⁶⁵ Moreover, empirical research has shown that, on the whole, plea agreements that contain appellate waiver agreements confer some extra benefits on the defendant when compared to plea agreements in which the defendant does not waive the right to appeal.⁶⁶ Although the decision to waive the right to appeal future unknown errors is understandably a difficult one for defendants, courts have found that it does not rise to the level of coerciveness necessary to overcome a defendant's will and overbear her volition.⁶⁷ Thus, *per se* challenges to the enforceability of sentencing appellate waivers are unlikely to gain much traction in the federal courts.

2. Case-by-Case Analysis of Knowledge and Voluntariness

Finding nothing inherently unknowable or involuntary in the appellate waiver process, federal courts test the knowing and voluntary nature of individual appellate waivers on a case-by-case basis. The defendant bears the burden of demonstrating that she did not knowingly and voluntarily waive her appellate rights.⁶⁸ A district court's adherence or non-adherence to the federal rule requiring the discussion of appellate waiver provisions during the

65. Although criminal defendants and the government often see utility in plea agreements, neither is obligated to bargain. Indeed, "a common response" of criminal defendants to the introduction of appellate waiver agreements was an "open plea"—a guilty plea without the benefit of any agreement with the government. King & O'Neill, *supra* note 3, at 233 n.87; *see also id.* at 250 n.133 (recounting one federal prosecutor's view that the overall plea agreement inures to the benefit of the defendant in the end and "that's why they sign the agreement at all.").

66. King & O'Neill, *supra* note 3, at 232–38 (2005). Appreciable differences were observed in the rate of downward departures and the application of the safety valve in plea agreements containing appellate waivers versus those that did not. *Id.* at 236–38.

More than one of every five waiver cases received a downward departure other than substantial assistance, compared to one of every ten nonwaiver cases in our sample [of 971 cases]. And nearly one in five waiver cases received a safety valve adjustment, compared to less than one in eight nonwaiver cases.

Id. at 238. *But see id.* at 244–45 (noting that defendants in some districts do not appear to receive independent consideration in exchange for appellate waivers).

67. *See United States v. Navarro-Botello*, 912 F.2d 318, 320–21 (9th Cir. 1990) ("Just because the choice looks different to [the defendant] with the benefit of hindsight, does not make the choice involuntary."); *see also Haines, Jr.*, *supra* note 5, at 229 (finding the decision to accept a waiver to be "no more the product of 'coercion' than the standard plea bargain.") (internal citation omitted).

68. *See United States v. Hahn*, 359 F.3d 1315, 1329 (10th Cir. 2004) (en banc) (per curiam).

plea colloquy⁶⁹ does not conclusively demonstrate whether the defendant knowingly entered into the appellate waiver. A district court's proper questioning of the defendant during the plea colloquy only creates a presumption that the appellate waiver was knowing and voluntary; a defendant could demonstrate otherwise by introducing other particularized evidence.⁷⁰ Conversely, even if the district court failed to mention the appellate waiver during the plea colloquy, courts of appeals will enforce the appellate waiver as long as other indicia demonstrate that the defendant understood the waiver and freely assented to it.⁷¹

Relatedly, a district court's instruction at the conclusion of the sentencing hearing that the defendant has fourteen days to note an appeal does not render an appellate waiver unenforceable. Such a statement is undeniably true—some issues, including all issues outside of the scope of the appellate waiver, remain appealable despite the presence of an appellate waiver.⁷² Moreover, such a belated statement made weeks after the acceptance of the plea has no effect on whether the defendant knew and understood the appellate waiver at the time of the agreement.⁷³

When individual defendants successfully demonstrate that they did not understand the appellate waiver provision to which they agreed, courts naturally decline to enforce the waivers. Still, appellate courts have not taken a uniform approach to dealing with uninformed or involuntary appellate waivers. While some courts invalidate the entire plea agreement and send the parties back to

69. FED. R. CRIM. P. 11(b)(1)(N).

70. See *United States v. White*, 366 F.3d 291, 295–96 (4th Cir. 2004) (although a defendant's statements during a Rule 11 colloquy “‘carry a strong presumption of verity,’” they are not categorically immune from later challenge (quoting *Blackledge v. Allison*, 431 U.S. 63, 74 (1977))).

71. See *United States v. Loutos*, 383 F.3d 615, 619 (7th Cir. 2004) (finding that defendant, who was an attorney, made a knowing waiver of his right to appeal despite failure of the district court to mention it in the plea colloquy); *United States v. Teeter*, 257 F.3d 14, 24 (1st Cir. 2001).

72. See *supra* notes 33–36 and accompanying text.

73. See, e.g., *United States v. Azure*, 571 F.3d 769, 774 (8th Cir. 2009); *United States v. Fisher*, 232 F.3d 301, 304–05 (2d Cir. 2000) (“If enforceable when entered, the waiver does not lose its effectiveness because the district judge gives the defendant post-sentence advice inconsistent with the waiver. No justifiable reliance has been placed on such advice.”) (internal footnote omitted). *But see* *United States v. Felix*, 561 F.3d 1036, 1040–41 (9th Cir. 2009) (holding that the district court's advisement of the right to appeal during sentencing hearing can limit the scope of an appellate waiver if the government does not object) (citing *United States v. Buchanan*, 59 F.3d 914, 917–18 (9th Cir. 1995)).

square one,⁷⁴ other courts simply sever the appellate waiver from the plea agreement and forge ahead with the merits of the appeal.⁷⁵

B. Public Policy Considerations

Numerous public policy considerations exist both for and against sentencing appellate waivers. In general terms, the policy rationales in favor of appellate waivers are finality, efficiency, and freedom of bargaining. Critics of appellate waivers generally point to the potential for uncorrected sentencing errors and negative impacts on the perceived integrity of the criminal justice system. As of now, the federal appellate courts have not found that the negative policy consequences of sentencing appellate waivers merit their invalidation.

1. Finality and Efficiency

Some courts and commentators claim that enforcing sentencing appellate waivers furthers the related public policies of finality and efficiency.⁷⁶ Sentencing appellate waivers promote the finality of sentences in the sense that a valid appellate waiver makes it almost impossible to disturb these judgments. By increasing finality and curtailing the appellate process, appellate waivers reduce the workload of the appellate courts, prosecutors, and state-funded defense attorneys.⁷⁷ This reduced workload permits reallocation of governmental and judicial resources to other areas, such as additional prosecutions. These additional prosecutions reduce crime, promote justice, and generally benefit the public.

74. See, e.g., *United States v. Ogden*, 102 F.3d 887, 888 (7th Cir. 1996); *United States v. Wenger*, 58 F.3d 280, 282 (7th Cir. 1995) (“Waivers of appeal must stand or fall with the agreements of which they are a part.”). But see *Bennardo*, *supra* note 5, at 541 (noting inconsistency in Seventh Circuit jurisprudence on this issue).

75. See, e.g., *Teeter*, 257 F.3d at 27 (“[T]he proper remedy, given the circumstances, is to sever the waiver of appellate rights from the remainder of the plea agreement, allowing the other provisions to remain in force.”); *United States v. Bushert*, 997 F.2d 1343, 1353 (11th Cir. 1993) (“By imposing the severance remedy, [the defendant] will get the benefit of the deal he thought he struck.”).

76. See, e.g., *United States v. Navarro-Botello*, 912 F.2d 318, 322 (9th Cir. 1990) (describing finality as “perhaps the most important” benefit of plea bargaining); see also *Teeter*, 257 F.3d at 22 & n.5; *Calhoun*, *supra* note 3, at 137–38.

77. See *Teeter*, 257 F.3d at 22; *Navarro-Botello*, 912 F.2d at 322; *Goodwin*, *supra* note 2, at 212 (noting that appellate waiver supporters “contend that waivers help to decrease the enormous amount of guideline sentencing litigation”); *Haines, Jr.*, *supra* note 5, at 229 (“If waivers of appeal were forbidden, courts would continue to bear the burden of many marginal appeals that hinder and devalue the appellate process.”).

Not all commentators believe this brand of finality is positive.⁷⁸ Although appellate waivers bolster the finality of judgments, that finality comes at the expense of the error-correcting function of the appellate process.⁷⁹ Finality of erroneous judgments and sentences is a negative. Moreover, some have questioned whether appellate waivers actually conserve significant resources given the costs of enforcement.⁸⁰

When a defendant requests an appeal despite a valid appellate waiver, defense counsel often files an *Anders* brief.⁸¹ In an *Anders* brief, defense counsel references “anything in the record that might arguably support the appeal,” but states that the attorney could not find any non-frivolous issues for appeal.⁸² The defendant is then permitted to file a supplemental brief raising additional grounds for appeal or expounding upon the arguments raised in the *Anders* brief.⁸³ When deciding an *Anders* appeal, the appellate court is duty-bound to independently review the entire trial record to determine whether the appeal is “wholly frivolous.”⁸⁴ If a valid appellate waiver is present in an *Anders* appeal, the appellate court may dismiss the issues the appellate waiver covers, but the court must still independently review the trial record to ascertain whether the defendant possesses any non-frivolous appellate arguments that are unwaivable or fall outside of the scope of the waiver.⁸⁵ Thus, the

78. See Chanenson, *supra* note 62, at 183 (“[J]udicial resource questions should largely be beside the point.”); see also *United States v. Vanderwerff*, No. 12-cr-00069, 2012 WL 2514933, at *4 (D. Colo. June 28, 2012) (“Prioritizing efficiency at the expense of the individual exercise of constitutional rights applies to the guilty and the innocent alike, and sacrificing constitutional rights on the altar of efficiency is of dubious legality.”).

79. See Johnson, *supra* note 43, at 710 (“While the wholesale enforcement of appeal-of-sentence waivers would achieve sentence finality, it would do so only at unwarranted expense to sentencing accuracy.”).

80. See *United States v. Perez*, 46 F. Supp. 2d 59, 71 (D. Mass. 1999) (“[I]t is not at all clear that there is a tide of appeals from pleas that needs to be stemmed.”); *United States v. Melancon*, 972 F.2d 566, 579 (5th Cir. 1992) (Parker, J., concurring) (predicting that it is “wishful thinking at best and self-delusion at least” to think that appellate waivers will stem the tide of sentencing appeals); see also Johnson, *supra* note 43, at 711 (estimating that the “processing of sentence appeals is generally less costly than the processing of other types of appeals” and cautioning that the burden imposed by processing frivolous sentencing appeals “should not be overstated”).

81. Also called a “no-merit” brief, the *Anders* brief takes its name from *Anders v. California*, 386 U.S. 738 (1967).

82. See *Anders*, 386 U.S. at 744.

83. *Id.*

84. *Id.*

85. See, e.g., *United States v. Widdows*, 477 F. App’x 143 (4th Cir. 2012) (per curiam) (dismissing majority of *Anders* appeal as precluded by appellate waiver but reviewing record and affirming as to unwaivable issues).

enforcement of a valid appellate waiver often consumes a considerable amount of appellate resources, especially where *Anders* appeals are involved.⁸⁶

2. Freedom of Bargaining

Public policy favors permitting the government and the defendant to each enter into an enforceable bargain that they believe will further their self-interest.⁸⁷ Diffuse public interests should rarely outweigh a criminal defendant's freedom to bargain in the way that she believes best protects her liberty interests.⁸⁸ Any restriction on the enforceability of appellate waivers reduces the number of bargaining chips available to criminal defendants,⁸⁹ undermines their ability to safeguard their own interests, and ultimately makes successful bargaining less likely.⁹⁰

An individual may always waive or forfeit appeal simply by declining to file a notice of appeal,⁹¹ voluntarily dismissing an appeal

86. Cf. King & O'Neill, *supra* note 3, at 227 (finding a probable connection between the proliferation of appellate waivers and a decline in the rate of appellate filings). *But see id.* at 228 & n.78 (noting other factors likely contributed to the decline).

87. Johnson, *supra* note 43, at 712.

88. Cf. *Town of Newton v. Rumery*, 480 U.S. 386, 395 (1987) (enforcing an agreement releasing the right to file a civil action against the town in exchange for the dismissal of criminal charges). *But see United States v. Ready*, 82 F.3d 551, 555–56 (2d Cir. 1996) (finding that waivers of appellate rights implicate “institutional and societal values” that transcend individuals' bargaining interests).

89. See, e.g., *United States v. Andis*, 333 F.3d 886, 895 (8th Cir. 2003) (Arnold, J., concurring) (“One of the few things that a criminal defendant has to trade with his or her accuser is the right to appeal, and so the court, far from improving the lot of criminal defendants with its interventionist rule, actually deprives them of their property and the wherewithal with which to bargain.”); *United States v. Khattak*, 273 F.3d 557, 562 (3d Cir. 2001); *United States v. Behrman*, 235 F.3d 1049, 1051 (7th Cir. 2000); see also *United States v. Mezzanatto*, 513 U.S. 196, 208 (1995) (“A defendant can ‘maximize’ what he has to ‘sell’ only if he is permitted to offer what the prosecutor is most interested in buying.”); Calhoun, *supra* note 3, at 138.

90. See *United States v. Guillen*, 561 F.3d 527, 530 (D.C. Cir. 2009); *Andis*, 333 F.3d at 895 (Arnold, J., concurring); *United States v. Teeter*, 257 F.3d 14, 22 (1st Cir. 2001); Teeter, *supra* note 35, at 749; see also *Mezzanatto*, 513 U.S. at 209 (noting that limitations on what may be plea bargained may have the effect of curtailing plea bargaining); Calhoun, *supra* note 3, at 138.

91. See *United States v. Wenger*, 58 F.3d 280, 282 (7th Cir. 1995) (“Our legal system makes no appeal the default position.”); see also *Yakus v. United States*, 321 U.S. 414, 444 (1944) (noting that “a constitutional right may be forfeited in criminal as well as civil cases by the failure to make timely assertion of the right.”).

once filed,⁹² dying,⁹³ going on the lam,⁹⁴ or failing to call the trial court's attention to the alleged error.⁹⁵ A necessary ingredient in the appellate process is a willing and diligent defendant. If an individual defendant decides not to file a timely appeal and freely waives her appellate rights, it is counterintuitive that society would bar the defendant from extracting a price for that same waiver.

3. Sentencing Disparity

A major goal of the Sentencing Reform Act of 1984 (SRA) was to reduce the imposition of dissimilar sentences on similarly-situated defendants.⁹⁶ Reformers saw incongruent sentences based on individual judges' preferences as a major problem of the pre-SRA era.⁹⁷ To reduce sentencing disparity, the SRA created federal sentencing guidelines, which were initially mandatory but were later downgraded to advisory,⁹⁸ and meaningful appellate review of sentences.⁹⁹ Numerous courts and commentators have argued that the enforcement of sentencing appellate waivers undermines the SRA's goal of consistency by allowing erroneous sentences to go uncorrected and inhibiting the articulation of a common law of sentencing.¹⁰⁰

92. See, e.g., *Johnson v. United States*, 838 F.2d 201 (7th Cir. 1988) (appellant's voluntary dismissal of appeal surrendered all future claims that could have been raised on appeal).

93. The death of an appealing criminal defendant typically results in either dismissal of the appeal or setting aside the conviction. WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, *CRIMINAL PROCEDURE* § 27.5(a) (2d ed. 1999).

94. Under the fugitive disentitlement doctrine, "an appellate court may dismiss the appeal of a defendant who is a fugitive from justice during the pendency of his appeal." *Ortega-Rodriguez v. United States*, 507 U.S. 234, 239 (1993); see also LAFAVE, ISRAEL & KING, *supra* note 93, § 27.5(c); Martha B. Stolley, Note, *Sword or Shield: Due Process and the Fugitive Disentitlement Doctrine*, 87 J. CRIM. L. & CRIMINOLOGY 751 (1997).

95. LAFAVE, ISRAEL & KING, *supra* note 93, § 27.5(c). But see *id.* at § 27.5(d) (discussing appellate courts' authority "to reverse on the basis of plain error even though the error was not properly raised and preserved at the trial level").

96. See Stephen Breyer, *The Federal Sentencing Guidelines and the Key Compromises Upon Which They Rest*, 17 HOFSTRA L. REV. 1, 4–5, 7 (1988); KATE STITH & JOSE A. CABRANES, *FEAR OF JUDGING: SENTENCING GUIDELINES IN THE FEDERAL COURTS* 51 (1998) (identifying the primary objective of the SRA as the elimination of "unwarranted disparity" in federal sentencing) (internal quotation marks omitted).

97. See, e.g., MARVIN E. FRANKEL, *CRIMINAL SENTENCES: LAW WITHOUT ORDER* 5 (1973) ("As to the penalty that may be imposed, our laws characteristically leave to the sentencing judge a range of choice that should be unthinkable in a 'government of laws, not of men.'").

98. See *United States v. Booker*, 543 U.S. 220, 245 (2005); see also STITH & CABRANES, *supra* note 96, at 38–77 (chronicling the advent of the U.S. Sentencing Commission and the promulgation of the Guidelines); Breyer, *supra* note 96, at 5–8.

99. 18 U.S.C. § 3742 (2012).

100. In the words of Judge Paul L. Friedman:

By making sentences virtually unreviewable, the widespread use of enforceable sentencing appellate waivers results in a functional return to the pre-SRA system.¹⁰¹ The appellate system exists “to correct errors; to develop legal principles; and to tie geographically dispersed lower courts into a unified, authoritative legal system.”¹⁰² Once a broad appellate waiver is executed, a sentencing court can impose virtually any sentence within the statutory limits without the fear of appellate intermeddling. Circumventing appellate review increases the risk that district courts will break with national trends in sentencing, ignore the recommendations of the Guidelines, and impose sentences that are out of alignment with other sentences in comparable prosecutions. Without the specter of an appellate court vacating the sentence as unreasonable, the district court commands almost free rein over the sentence.¹⁰³ Such lack of oversight results in a greater likelihood of idiosyncratic sentences.¹⁰⁴

Absence of appellate review also results in a dearth of precedential case law.¹⁰⁵ Thus, district courts that seek to impose within-Guidelines sentences or otherwise follow the dictates of the sentencing statutes have fewer common law guideposts to follow. With fewer guideposts, well-meaning district courts are more likely to inadvertently deviate from acceptable sentencing practices and outcomes. Coupled with the potential inability of the appellate court to correct an error because of an appellate waiver, the lack of

What the government seeks to do through the appeal waiver provision is inconsistent with the goals and intent of Congress and the goals and intent of the Sentencing Commission. It will insulate from appellate review erroneous factual findings, interpretations and applications of the Guidelines by trial judges and thus, ultimately, it will undermine uniformity.

United States v. Raynor, 989 F. Supp. 43, 48 (D.D.C. 1997); *see also* United States v. Melancon, 972 F.2d 566, 574 (5th Cir. 1992) (Parker, J., concurring); United States v. Bolinger, 940 F.2d 478, 483 (9th Cir. 1991) (Nelson, J., dissenting); United States v. Johnson, 992 F. Supp. 437, 439 (D.D.C. 1997); Douglas A. Berman, *The fate and future of appeal waivers?*, SENTENCING LAW AND POLICY BLOG (Mar. 4, 2005, 12:05 PM), http://sentencing.typepad.com/sentencing_law_and_policy/2005/03/the_fate_and_fu.html; Goodwin, *supra* note 2, at 212; Calhoun, *supra* note 3, at 201, 206; Chanenson, *supra* note 62, at 182–84; Comment, *supra* note 52, at 1120.

101. *See* United States v. Perez, 46 F. Supp. 2d 59, 68 (D. Mass. 1999); *see Melancon*, 972 F.2d at 574 (Parker, J., concurring).

102. Harlon Leigh Dalton, *Taking the Right to Appeal (More or Less) Seriously*, 95 YALE L.J. 62, 69 (1985).

103. *See* United States v. Vanderwerff, No. 12-cr-00069, 2012 WL 2514933, at *5 (D. Colo. June 28, 2012).

104. *But see* Johnson, *supra* note 43, at 718 (arguing that appellate “intermeddling” can create sentencing irrationality and disparity).

105. *See* Perez, 46 F. Supp. 2d at 68 (“[A]llowing appeals waivers would have a cost in terms of the development of appellate law necessary to clarify how the guidelines should be applied.”); Dyer & Judge, *supra* note 47, at 663; Comment, *supra* note 52, at 1121; Chanenson, *supra* note 62, at 183; *see also* Johnson, *supra* note 43, at 712.

appellate sentencing case law compounds the likelihood of non-uniform sentences.

Appellate waiver supporters argue that developing the common law is not an established public policy, but rather “seems directly in conflict with doctrines of judicial restraint that suggest that courts should avoid crafting public policy unless forced to do so.”¹⁰⁶ Others have noted that adequate sentencing common law is developed through the significant number of cases without appellate waivers, including all of the prosecutions that go to trial.¹⁰⁷ Additionally, the U.S. Sentencing Commission’s constant oversight of the Guidelines diminishes the need for judicial review of all sentences.¹⁰⁸ Empirical research demonstrates that an early concern that the widespread use of non-mutual appellate waivers would lead to a disproportionate number of government-initiated sentencing appeals¹⁰⁹ has not come to fruition because defendants continue to initiate a significant number of sentencing appeals.¹¹⁰ Additionally, as noted above, defendants have always possessed the ability to forgo appeal, which similarly compromises society’s interests in error correction and the reduction of disparate sentences.¹¹¹

4. Integrity of the Criminal Justice System

Judges and commentators have voiced concerns that prosecutors, defense attorneys, and district court judges are self-interested in obtaining a defendant’s appellate waiver because the waiver insulates their actions from later review.¹¹² When it comes to judges, some worry that this insulation erodes judicial integrity.¹¹³ When it comes to defense attorneys, some claim that the lawyer’s personal interest in the execution of an appellate or collateral attack waiver rises to the level of a conflict of interest that compromises the attorney’s ability to competently represent the defendant.¹¹⁴

106. Teeter, *supra* note 35, at 741 & n.97.

107. Haines, Jr., *supra* note 5, at 229.

108. *Id.*

109. *See, e.g., Perez*, 46 F. Supp. 2d at 69 (voicing concern that widespread use of appellate waivers would lead to “skewed case law” based on the disproportionate number of appeals by the government); *United States v. Raynor*, 989 F. Supp. 43, 46 (D.D.C. 1997).

110. *See King & O’Neill, supra* note 3, at 256.

111. *See supra* Part II.B.2.

112. *See Calhoun, supra* note 3, at 138–39 & nn.58–59 (listing cases); *King & O’Neill, supra* note 3, at 223 (citing letter from National Association of Criminal Defense Lawyers).

113. *See Dyer & Judge, supra* note 47, at 663–65.

114. *King & O’Neill, supra* note 3, at 245–47 (labeling appellate waiver provisions “an obvious conflict of interest”).

These concerns certainly have some validity. An aversion to reversal or a desire to reduce the likelihood of continued proceedings after remand may motivate a judge to accept a plea agreement containing an appellate waiver. Concern over questionable practices in the prosecution may motivate a prosecutor to offer a plea bargain at a significant discount as long as the defendant agrees to an appellate waiver. Finally, a desire to avoid a later charge of ineffective assistance of counsel may motivate a defense attorney to counsel her client to accept a plea agreement containing appellate and collateral attack waivers. These concerns, however, have not rendered appellate waivers unenforceable.

Despite an otherwise enforceable waiver, defendants may attack the plea agreement or the waiver itself with a claim of ineffective assistance of counsel in acceptance of the plea agreement or the waiver.¹¹⁵ In most circuits, however, a defendant who has waived appeal and collateral review may not raise any ineffective assistance claims based on her attorney's actions after the execution of the waiver (such as during sentencing).¹¹⁶ Some commentators take solace in the plea colloquy to ensure that defendants enter into such waivers knowingly and with an opportunity to discuss the waiver provision with both the court and counsel.¹¹⁷ With full knowledge of the ramifications of their waivers, defendants ostensibly agree to waive their rights to challenge errors and ineffectiveness only when the plea agreement makes it worthwhile to do so. Thus, federal courts continue to enforce sentencing appellate waivers despite concerns of abuse by the bench and the bar.

C. An Impermissible Chill and Unconstitutional Condition

Constitutional due process prohibits a court from putting a price on a defendant's right to appeal or otherwise chilling it.¹¹⁸ The Constitution does not require an avenue for criminal appeals;¹¹⁹

115. See *id.* at 247 n.122; see also *supra* text accompanying note 40.

116. See, e.g., *Nunez v. United States*, 495 F.3d 544, 548 (7th Cir. 2007), *vacated* 554 U.S. 911 (2008) (“[I]neffective assistance *after* the plea . . . cannot retroactively make the plea invalid.”). *But see* *United States v. Attar*, 38 F.3d 727, 732–33 (4th Cir. 1994) (holding that appellate waiver did not preclude challenge that the sentencing hearing and presentation of motion to withdraw plea were conducted in violation of the Sixth Amendment where the district court permitted the defense attorney to withdraw at the beginning of the sentencing hearing and defendant proceeded *pro se*). See also *supra* notes 36–37 and accompanying text.

117. Teeter, *supra* note 35, at 741.

118. See, e.g., *Chaffin v. Stynchcombe*, 412 U.S. 17, 24 n.11 (1973); *North Carolina v. Pearce*, 395 U.S. 711, 724 (1969); see also *Calhoun*, *supra* note 3, at 146; *Dyer & Judge*, *supra* note 47, at 655.

119. *Jones v. Barnes*, 463 U.S. 745, 751 (1983).

“[o]nce a system of appellate courts is put into place, however, a criminal defendant’s ability to appeal may not be unduly burdened.”¹²⁰ Demonstrating a sufficient chill, nevertheless, presents a significant hurdle for criminal defendants. The Supreme Court has declined to find that offers of benefits by the government, up to and including avoiding the death penalty, impermissibly chilled other rights.¹²¹ Offers to drop charges or otherwise minimize a defendant’s punishment in exchange for the waiver of a defendant’s appellate rights do not impermissibly chill the exercise of those rights any more than the same sorts of offers in a greater plea agreement chill a defendant’s exercise of her right to a jury trial.¹²² Thus, courts have roundly rejected the impermissible chill argument when raised against plea bargaining in general¹²³ and against appellate waivers specifically.¹²⁴ An individual defendant would have an easier time showing that her particular circumstance was so devoid of options that the government’s offer rendered her appellate waiver involuntary.¹²⁵ Thus, arguments involving the impermissible chilling effects of appellate waivers are rarely raised and unlikely to succeed.

III. AN INCENTIVE AND EFFICIENCY-BASED CRITIQUE OF SENTENCING APPELLATE WAIVERS

The current plea agreement sentencing appellate waiver system suffers from three major drawbacks because these waivers (1) remove much of the incentive for district courts to adhere to established procedural and substantive sentencing law, (2) create

120. *United States v. Ready*, 82 F.3d 551, 555 (2d Cir. 1996); *see also* *United States v. Melancon*, 972 F.2d 566, 577 (5th Cir. 1992) (Parker, J., concurring) (“Even if the Due Process and Equal Protection Clauses of the Constitution do not require the government to create a statutory system of appellate rights, these constitutional clauses do require the government, once it has decided voluntarily to create such a system (as it has), to allow unfettered and equal access to it.”) (citing *Griffin v. Illinois*, 351 U.S. 12 (1956)).

121. *See* *Brady v. United States*, 397 U.S. 742, 755 (1970) (“[A] plea of guilty is not invalid merely because entered to avoid the possibility of a death penalty”).

122. *See* *Teeter*, *supra* note 35, at 740; *see also* *Calhoun*, *supra* note 3, at 153.

123. *See* *Calhoun*, *supra* note 3, at 153.

124. *See* *United States v. Navarro-Botello*, 912 F.2d 318, 321 (9th Cir. 1990); *Calhoun*, *supra* note 3, at 149 (concluding that the evolution of Supreme Court precedent no longer supports invalidation of appellate waivers on this basis). *But see* *United States v. Perez*, 46 F. Supp. 2d 59, 67–68 (D. Mass. 1999) (finding that appellate waivers are an undue burden on the right to appeal in violation of due process); *Dyer & Judge*, *supra* note 47, at 655 (arguing that appellate waivers create an unreasonable deterrent to a defendant’s exercise of her statutory right to appeal in violation of due process).

125. *See supra* Part II.A.2.

inefficiencies in the bargaining process, and (3) lack the “bite” necessary to deter defendants from breaching the agreement. These first two concerns are not wholly divorced from previous criticisms already described. Removing incentives from the district courts is an extension of the argument that sentencing appellate waivers undermine the Sentencing Reform Act and the discussion of the inefficiencies of the bargaining structure builds upon previous criticisms that appellate waivers impair plea bargaining.

A. Hypothesizing Judicial Response to Appellate Waivers

Anecdotes abound of district court judges who appear to alter their behavior at sentencing hearings based on the existence of an appellate waiver.¹²⁶ Some judges appear to give short shrift to explaining the basis of their sentences.¹²⁷ Others perhaps arrive at different sentencing outcomes. But anecdotes, however interesting, prove little. This Article therefore employs existing models of judicial behavior and the available data to support the hypothesis that the absence of appellate review affects sentencing behavior. This analysis assumes that district court judges are rational (although not hyper-rational) actors,¹²⁸ who seek to maximize utility. However, federal district court judges number in the hundreds¹²⁹ with as many individual definitions of utility. Some value being a “good” judge, others prioritize avoiding reversal, others seek promotions, and others maximize their leisure. No single formula can describe all judges, but both behavioral models and empirical data support the conclusion that the absence of appellate review affects the sentencing behavior of the “ordinary” district court judge.

126. See, e.g., King & O’Neill, *supra* note 3, at 247–48 & n.123.

127. The transcript of one sentencing hearing abruptly ends after the district court judge pronounces the sentence without any supporting explanation and confirms with the assistant U.S. attorney that the plea agreement includes an appellate waiver. United States v. Powell, No. 7:09-CR-114-1-BO (E.D.N.C. Feb. 25, 2010).

128. The fact that humans are not hyper-rational does not void rational-choice theory. See RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW § 1.4 (8th ed. 2011); see also Richard A. Posner, *Rational Choice, Behavioral Economics, and the Law*, 50 STAN. L. REV. 1551, 1552–54 (1998).

129. In fiscal year 2013, there were 677 authorized judgeships in the federal district courts. See United States Courts, U.S. District Courts (last visited Dec. 5, 2014), <http://www.uscourts.gov/Statistics/JudicialBusiness/2013/us-district-courts.aspx>.

1. Dalton's Trial Judges Archetypes

Nearly thirty years ago, Professor Harlon Dalton described three archetypes of trial judges: bench warmers, bench climbers, and bench builders.¹³⁰ The bench warmer is a team player—she is unlikely to take chances or stretch precedents, is “willing to pull her weight, so long as others pull theirs,” and “is, if anything, a little too appreciative” of her judicial position, as she did not actually expect to obtain it.¹³¹ The bench climber seeks to advance through the judicial ranks. To rise through the ranks, she seeks “to make few mistakes while doing a few things really well.”¹³² Finally, in contrast, the bench builder takes her position in the trial court very seriously because that is where justice is achieved (if at all). She trusts her own rulings, “does not regard precedent as particularly instructive,” and “views appellate review as a necessary evil”—necessary to rectify the mistakes of colleagues but a roadblock that she must sidestep to achieve justice.¹³³

Professor Dalton used these archetypes to argue that appeal as of right is not necessary for a variety of civil cases. The bench warmer, although not the most capable of judges, would never actively attempt to disobey the teachings of the appellate court. She is unlikely to employ the precedents creatively and will likely attempt to insulate her decisions from reversal.¹³⁴ The bench warmer, though, would act no differently under a system that permitted appeal as of right versus one that permitted discretionary appeals. Her goal is to apply the precedents, move the cases, and avoid the humiliation of reversal.

Similarly, the bench climber seeks to minimize reversal, second-guessing, or negative treatment in the press.¹³⁵ Unlike the bench warmer, however, she may attempt to anticipate shifts in the higher court's thinking rather than just apply precedent. If she senses that a precedent will be overruled, she may challenge the unpopular precedent to demonstrate that she was out in front of the shift. To attract the attention of the court above (which she would like to join), she may craft especially well-written or “splash[y]” opinions.¹³⁶

130. Dalton, *supra* note 102, at 87.

131. *Id.*

132. *Id.*

133. *Id.*

134. *Id.*

135. *See id.* at 88.

136. *See id.*

Appellate review has the greatest effect on the bench builder.¹³⁷ Finding appellate review of her own work a nuisance, the bench builder goes to great lengths to insulate her decisions from reversal. She knows the just outcome and does not want her work undone by the appellate court. Thus, she may hide the ball or otherwise distort her true reasoning to avoid reversal and preserve what she views as a just outcome.¹³⁸

Dalton questioned whether the threat of appellate review actually induces trial judges to self-correct and reach more just results.¹³⁹ Reversals may not motivate some judges if the percentage of reversals is small and, in those judges' eyes, arbitrary. Appellate review only motivates some judges to better insulate their opinions from reversal, but not to alter their outcomes. Other judges are unmoved by the prospect of reversal because they simply lack the aptitude to accurately forecast how the appellate court would have them rule.¹⁴⁰

None of these three judicial archetypes would substantially alter their modus operandi under a system that provides an appeal of right versus a discretionary appeal. Appellate review is not guaranteed even in an appeal of right system, because the losing party may simply elect not to appeal. Rather, it is the *threat* of appeal that motivates trial judges to act the way they do, and a system of discretionary appeals does not significantly dissipate that threat. The question appellate waivers pose is what effect an *assurance of no appellate review* has on the cast of judicial archetypes. The bench warmer may get a little sloppy. Although she seeks to accurately apply precedents, much of her motivation stems from her desire to avoid reversals. Her other main interest is to pull her weight as part of the trial court team and move the cases. Although she would not purposefully ignore the precedents, removing the possibility of reversal starkly diminishes her incentive to rigorously attempt to research and understand the law. Appellate waiver grants the bench warmer the license to expeditiously move cases without fear of reversal. This recipe is ripe to produce oversights.

Appellate waiver similarly disincentivizes the bench climber by removing the case from the appellate conversation. Assured that the appellate court will not review her rulings, she lacks an outlet to engage and impress the appellate court. She will devote her time

137. *Id.*

138. *Id.* at 88–89.

139. *Id.* at 92.

140. *Id.* at 92 & n.101.

and effort to decisions that are likely to be reviewed at the expense of those that assuredly will not move on to a higher court.

On the other hand, producing just outcomes is the primary incentive of the bench builder, not upward ambitions or fear of reversal. Appellate waiver will rarely affect the bench builder's outcomes; it may, however, affect the presentation. Instead of crafting well-insulated opinions in order to evade meaningful appellate review, appellate waiver frees the bench builder to plainly state her true rationale without fear of appellate intermeddling and, in certain cases, to brazenly flaunt appellate teachings in areas of disagreement.

Thus, foreknowledge that its decisions will be insulated from appellate review reduces a trial court's motivation to closely adhere to the law of the circuit, whether from lack of effort spent on researching the law, from a decreased aspiration to get it right, or from seizing an opportunity to achieve the judge's view of justice even if that view runs counter to appellate precedent. Appellate waivers decrease the likelihood that trial judges will systematically exercise fidelity to appellate teachings by informing the trial judge at the outset that her sentencing decisions are virtually unreviewable. In short, appellate waivers incentivize lawless sentencing in the district courts.

2. Posner's Judge as "Labor-Market Participant"

Judge Richard Posner describes judges through a comprehensive labor-market participant model.¹⁴¹ This model "find[s] that judges are not moral or intellectual giants (alas), prophets, oracles, mouthpieces, or calculating machines. They are all-too-human workers, responding as other workers do to the conditions of the labor market in which they work."¹⁴² Judges desire the same basic goods as other workers, and their behavior is designed to maximize the attainment of these desires.¹⁴³

Prospective federal judges are sellers in the labor market, and the President, with the approval of the Senate, is the buyer. The

141. This model of decision-making integrates nine incomplete theories of judicial behavior: the attitudinal, strategic, sociological, psychological, economic, organizational, pragmatic, phenomenological, and legalist theories. RICHARD A. POSNER, *HOW JUDGES THINK* 19-56 (2008); *see also* LEE EPSTEIN, WILLIAM M. LANDES & RICHARD A. POSNER, *THE BEHAVIOR OF FEDERAL JUDGES: A THEORETICAL AND EMPIRICAL STUDY OF RATIONAL CHOICE* 30-47 (2013).

142. POSNER, *supra* note 141, at 7.

143. *Id.* at 11; *see generally* Richard A. Posner, *What Do Judges and Justices Maximize? (The Same Thing Everybody Else Does)*, 3 *SUP. CT. ECON. R.* 1 (1993); RICHARD A. POSNER, *OVERCOMING LAW* 109-44 (1995).

buyer seeks to appoint “good” judges, but also judges ideologically tilted in favor of the Administration’s political goals.¹⁴⁴ Once appointed, though, federal judges are well insulated from both the carrots and the sticks that motivate most workers.¹⁴⁵ Judges have few avenues for promotion¹⁴⁶ and no monetary rewards for “superior” work.¹⁴⁷ Likewise, judges have life tenure, and the prospect of impeachment is so small that it has little effect on judicial behavior.¹⁴⁸

Judges desire a salary, but are not primarily motivated by salary because they could presumably find more lucrative employment elsewhere.¹⁴⁹ Many enjoy the respect federal judges receive and the opportunity to exert power over others. Most federal judges “derive more utility from leisure and public recognition, relative to income, and are more risk averse, than the average practicing lawyer.”¹⁵⁰ Judges also, on the whole, appear to derive intrinsic satisfaction from being a “good” judge.¹⁵¹ Otherwise federal judges would simply avoid hard work, given the few true external constraints on their behavior, and would retire with full pay at the earliest possible moment.¹⁵² Of course, judges may be working for some other goal such as celebrity or power, but Posner estimates that the attainment of those goals does not necessarily depend on hard work.¹⁵³

In short, judges value income and leisure but do not seek to maximize either to the exclusion of all else. Most judges want to do a “good” job, and some aspire to promotion or celebrity. Judicial competence varies, and less able judges face a more difficult road to

144. POSNER, *supra* note 141, at 57–58.

145. *Id.* at 37, 58.

146. *But see id.* at 142 (conceding that the odds of promotion for judges within the pool of viably promotable judges may be “short enough . . . to induce a judge to do whatever he could to rise within the pool”); EPSTEIN, LANDES & POSNER, *supra* note 141, at 35–36, 337–83 (finding inconclusive evidence that some judges alter their behavior in order to increase their chances of promotion).

147. EPSTEIN, LANDES & POSNER, *supra* note 141, at 33.

148. *See id.*; *see also* Posner, *supra* note 143, at 4–5 (“A federal judge can be lazy, lack judicial temperament, mistreat his staff, berate without reason the lawyers who appear before him, be reprimanded for ethical lapses . . . and misbehave in other ways that might get even a tenured civil servant or university professor fired; he will retain his office.”).

149. *See* EPSTEIN, LANDES & POSNER, *supra* note 141, at 30–31.

150. *See* POSNER, *supra* note 141, at 59–60; *see also* EPSTEIN, LANDES & POSNER, *supra* note 141, at 36.

151. POSNER, *supra* note 141, at 174; POSNER, *supra* note 143, at 131, 133 (“The pleasure of judging is bound up with compliance with certain self-limiting rules that define the ‘game’ of judging.”); *see also* RICHARD A. POSNER, *THE FEDERAL COURTS: CHALLENGE AND REFORM* 335–36 (1996).

152. *See* POSNER, *supra* note 141, at 60–61 & n.7.

153. *Id.* at 62; POSNER, *supra* note 143, at 118 (“[P]restige inheres in the whole judiciary. Free-rider problems make it unlikely that any one judge will exert himself strenuously to raise the prestige of all.”).

achieving distinction and promotion.¹⁵⁴ Diminished opportunities for promotion or recognition may cause less able judges to substitute leisure for work and delegate a substantial amount to law clerks.¹⁵⁵ More able judges can be expected to work harder because they face fewer barriers to distinction and promotion.¹⁵⁶

Regardless of ability, reversal is a disutility for judges.¹⁵⁷ Reversal is a form of criticism and results in more work and less leisure.¹⁵⁸ Indeed, “when the heavier constraints of termination or demotion are inoperative with respect to an employee, the lighter constraint of criticism can weigh heavily.”¹⁵⁹ Judges, therefore, may consciously or unconsciously alter their behavior to avoid reversal even if that behavior does not align with the judge’s reading of the precedents or sense of justice.¹⁶⁰ In lawless areas, where district courts have little fear of appellate reversal (such as criminal sentencing before the Sentencing Reform Act), individual judges’ preferences and preconceptions are more likely to play a role in decision-making because these preferences are not tempered by reversal aversion.¹⁶¹ Anything from personal background and traits to previous employment and experiences can shape such preferences and preconceptions.¹⁶² A similar reliance on individual judges’ histories and biases emerge when formalist judges are faced with a lack of guidance from the “orthodox materials of decisions.”¹⁶³ Relatively minor influences are more likely to affect decision-making when workers’ overall incentives and constraints decrease.¹⁶⁴ In the

154. See POSNER, *supra* note 141, at 65.

155. *Id.* at 65; see also EPSTEIN, LANDES & POSNER, *supra* note 141, at 36–37.

156. POSNER, *supra* note 141, at 65.

157. See *id.* at 70, 141; POSNER, *supra* note 143, at 118–19. For studies supporting the existence of reversal aversion, see EPSTEIN, LANDES & POSNER, *supra* note 141, at 83–85, 215. See also discussion *infra* Part III.A.3.

158. See EPSTEIN, LANDES & POSNER, *supra* note 141, at 48–49.

159. *Id.* at 35. *But see id.* at 83 (noting that judges who do not respect their judicial superiors “might consider reversal a badge of honor and revel in their defiance of superior judicial authority”).

160. POSNER, *supra* note 141, at 70–71.

161. *Id.* at 71–72.

162. *Id.* at 72–75; see also RICHARD A. POSNER, REFLECTIONS ON JUDGING 129–30, 306 (2013).

163. To “fill the void,” judges’ decisions may be influenced by “life experience, personal-identity characteristics such as race and sex, temperament, ideology (often influenced by personal-identity characteristics, religion, and party loyalties), ideas of sound public policy whether or not ideologically inflected, considerations of administrability and workload, moral beliefs, collegial pressures, public opinion, family background, reading, sentiment and aversions, [or] even indifference.” *Id.* at 115.

164. POSNER, *supra* note 141, at 76; see also EPSTEIN, LANDES & POSNER, *supra* note 141, at 30–47.

case of district court judges, the removal of the possibility of reversal increases the likelihood that the judge will act based on personal preferences.

Aside from reversal aversion, backlog pressure from growing dockets also motivates judges.¹⁶⁵ Judges must, at some point, prioritize efficiency over perfection, especially at the district court level.¹⁶⁶

Judge Posner labels judges' failure to "converge on sentencing" a "serious problem" and identifies a need for judicial education in "a coherent, evidence-based theory of criminal punishment."¹⁶⁷ By enhancing the finality of the district court's rulings, appellate waivers alleviate both the threat of reversal and docket pressures. Removing the constraint of reversal, appellate waivers increase the likelihood that personal preferences will play a greater role in sentencing. In this way, appellate waivers return district courts to the pre-SRA era of effectively unreviewable sentencing discretion.¹⁶⁸ As discussed above, this period was marked by the perception that similarly-situated defendants received unacceptably disparate sentences.¹⁶⁹ Thus, structuring sentencing appellate waivers so that district courts know up front that their sentencing rulings are unreviewable increases the likelihood that personal biases will play a greater role in the sentencing process and decreases the likelihood that different judges will arrive at similar sentencing outcomes.

3. Empirical Research on Judicial Sentencing Behavior

Max Schanzenbach's empirical research supports the hypothesis that appellate review and the political composition of the reviewing court affect the sentencing behavior of district court judges. A study

165. POSNER, *supra* note 141, at 141.

166. According to Judge Friendly, "[t]he district courts know what their business is—disposing of cases by trial or settlement with fairness and with the optimum blend of prompt decision and rightness of result; they also have the responsibility of demonstrating the quality of federal justice to ordinary citizens—parties, witnesses and jurors." Henry J. Friendly, *The "Law of the Circuit" and All That*, 46 ST. JOHN'S L. REV. 406, 406–07 (1972) (internal footnote omitted); *see also id.* at 407 n.6 (opining that the "greatest district judges [are not] those who stew for months and then write a long opinion on a novel point of law concerning which they are almost certain not to have the last word"); POSNER, *supra* note 151, at 336–37 (quoting Judge Friendly); POSNER, *supra* note 162, at 288.

167. POSNER, *supra* note 162, at 314; *see also generally* Mary Kreiner Ramirez, *Into the Twilight Zone: Informing Judicial Discretion in Federal Sentencing*, 57 DRAKE L. REV. 591 (2009) (urging the use of cultural-competence and social-cognition training to reduce the influence of implicit biases and associations in federal sentencing).

168. *See supra* Part II.B.3.

169. *See supra* note 97 and accompanying text.

by Schanzenbach and Emerson Tiller analyzed variations in district court sentencing behavior based on whether the district court was politically aligned with the court of appeals.¹⁷⁰ The Schanzenbach-Tiller study found that Democrat-appointed district court judges gave shorter sentences for street crimes than Republican-appointed district court judges.¹⁷¹ District court judges of both parties used fact-based, offense-level adjustments, which are deferentially reviewed, to bring the Guidelines sentence in closer alignment with their sentencing preferences.¹⁷² However, Democrat-appointed district court judges were more likely to use Guidelines departures, which are subject to stricter appellate review, to further shorten the sentence in circuits with majority Democrat-appointed circuit court judges than in circuits with majority Republican-appointed circuit court judges.¹⁷³ The political orientation of the circuit court did not meaningfully affect the Republican-appointed district court judges' frequency of upward departures.¹⁷⁴ The authors deemed the lack of increased frequency of upward departures by Republican-appointed district court judges in aligned circuits unsurprising because upward departures are quite rare, Guidelines sentences for street-level crimes are already quite harsh, longer sentences can be achieved by manipulating adjustments, and defendants almost always appeal upward departures, which, therefore, make them unattractive to district court judges.¹⁷⁵

A second Schanzenbach-Tiller study using the actual identities of sentencing judges confirmed the results of the earlier study.¹⁷⁶ The first study used a larger sample size, but only approximated the political alignment of the district court based on the political composition of the judges in the district.¹⁷⁷ Using a smaller sample,

170. Max M. Schanzenbach & Emerson H. Tiller, *Strategic Judging Under the U.S. Sentencing Guidelines: Positive Political Theory and Evidence*, 23 J.L. ECON. & ORG. 24 (2007).

171. *Id.* at 43.

172. *Id.*

173. *Id.* at 47–52. A later study similarly found that an increase in Republican-appointed judges on the court of appeals results in longer sentences and reduces the frequency of below Guidelines sentences. EPSTEIN, LANDES & POSNER, *supra* note 141, at 246, 253; *see also* Joshua B. Fischman & Max M. Schanzenbach, *Do Standards of Review Matter? The Case of Federal Criminal Sentencing*, 40 J. LEGAL STUD. 405, 422–24 (2011) (“Moving from a circuit with 25 percent Democrats to a circuit with 75 percent Democrats . . . increases departures by about 6 percentage points.”).

174. Schanzenbach & Tiller, *supra* note 170, at 49.

175. *Id.*

176. *See* Max M. Schanzenbach & Emerson H. Tiller, *Reviewing the Sentencing Guidelines: Judicial Politics, Empirical Evidence, and Reform*, 75 U. CHI. L. REV. 715, 723, 724 (2008).

177. The Sentencing Commission does not publicly release the identity of the sentencing judge in its statistics. *See id.* at 728–29, 740–43.

the second study matched sentencing decisions to individual district court judges. Using this “judge-level data,” Schanzenbach and Tiller found that Democrat-appointed judges imposed approximately ten percent shorter sentences than Republican-appointed judges for “serious offenses.”¹⁷⁸ However, Democratic appointees were more likely to employ departures in circuits where the majority of appellate judges were themselves Democratic appointees.¹⁷⁹ They were also more likely to employ fact-based offense level adjustments, which are reviewed under a less searching standard of review, in circuits where the majority of appellate judges were Republican appointees.¹⁸⁰ This evidence suggests that district court judges strategically alter their calculations to avoid reversal. This behavior strongly demonstrates that reversal acts as a sentencing constraint.

A later study by Joshua Fischman and Schanzenbach found that “district judges are meaningfully constrained by the prospect of appellate reversal” when sentencing.¹⁸¹ The Fischman-Schanzenbach study analyzed the differential between sentences imposed by Democrat-appointed district court judges and those imposed by Republican-appointed district court judges across time periods in which appellate courts applied different levels of scrutiny to sentencing decisions.¹⁸² The study found that interparty sentencing disparity was significant only during periods of deferential review.¹⁸³ District court judges’ sensitivity to the changing standards of review for sentencing decisions suggests “that these judges are strategically modifying their behavior in response to the likelihood of reversal.”¹⁸⁴ In other words, district court judges are averse to reversal and modify their behavior—including the severity of an offender’s sentence—to minimize the risk of reversal. The study found, however, that district court judges who were appointed before the implementation of the Guidelines in 1987 did not modify their behavior as a consequence of changing standards of review.¹⁸⁵ The study hypothesized that these judges were likely less averse to reversal because they did not respect the Guidelines and, therefore, faced lower legitimacy costs when appellate courts reversed their

178. *Id.* at 734.

179. *Id.* at 735.

180. *Id.* at 736.

181. Fischman & Schanzenbach, *supra* note 173, at 405.

182. The party of the appointing president is significantly correlated with sentencing preferences; district court judges appointed by Democratic presidents favor shorter sentences than district court judges appointed by Republican presidents. *See id.* at 406, 422.

183. *Id.* at 424.

184. *Id.* at 407.

185. *See id.* at 426.

sentencing decisions.¹⁸⁶ The study concluded that although “aversion to reversal acts as a constraint on the behavior of district judges, its impact may be heterogeneous and depend upon the perceived legitimacy of the guidelines.”¹⁸⁷

These studies confirm that district court judges who respect the legitimacy of the Guidelines are averse to reversal of their sentencing decisions and modify their behavior accordingly.¹⁸⁸ Stephanos Bibas, Schanzenbach, and Tiller identified the threat of reversal as a “key component” of the Guidelines system that “constrains sentencing courts *ex ante*.”¹⁸⁹ In order to temper the effect of judges’ ideological beliefs on sentencing, the authors proposed a system in which a diversity of political viewpoints is institutionalized into the appellate review of sentences.¹⁹⁰ The essay specifically identified the proliferation of appellate waivers as a barrier to policing district courts’ sentencing practices because broad waivers “signal to sentencing judges that they can sentence without regard to sentencing law or policy.”¹⁹¹

Although no one has precisely measured the effect of appellate waivers on sentencing behavior, these studies confirm that removing the realistic possibility of reversal almost certainly affects sentencing practices. District court judges have sentencing preferences, strategically manipulate Guidelines calculations to further those preferences, and labor under an aversion to reversal. These findings support the hypothesis that district court judges, when

186. *Id.* at 418, 431.

187. *Id.* at 431.

188. See Christina L. Boyd & James F. Spriggs II, *An Examination of Strategic Anticipation of Appellate Court Preferences by Federal District Court Judges*, 29 WASH. U. J.L. & POL’Y 37, 51–53 (2009). One study appears to undermine claims that reversal aversion shapes judicial behavior. See Donald R. Songer, Martha Humphries Ginn & Tammy A. Sarver, *Do Judges Follow the Law When There Is No Fear of Reversal?*, 24 JUST. SYS. J. 137 (2003). This study, however, analyzed federal appellate court decisions in diversity tort actions (which are categorically unlikely to be reviewed by the Supreme Court) and found that law and precedent constrained the appellate courts’ decisions despite the low likelihood of reversal. Federal appellate courts—which operate in three judge panels—have institutional constraints that engender adherence to precedent that are absent at the district court level. In effect, “somebody” is always watching appellate decision makers. See VIRGINIA A. HETTINGER, STEPHANIE A. LINDQUIST & WENDY L. MARTINEK, *JUDGING ON A COLLEGIAL COURT: INFLUENCES ON FEDERAL APPELLATE DECISION MAKING* (2006) (claiming that the likelihood of arbitrary or extreme decisions is reduced at the appellate level by the moderating influence of alternative points of view); see also FRANK M. COFFIN, *THE WAYS OF A JUDGE: REFLECTIONS FROM THE FEDERAL APPELLATE BENCH* 58–59 (1980). The moderating influence of judicial panels is not present at the district court level. See POSNER, *supra* note 151, at 340 (noting that the isolation of district court judges creates the temptation for lawlessness and tyranny).

189. Stephanos Bibas, Max M. Schanzenbach & Emerson H. Tiller, *Policing Politics at Sentencing*, 103 NW. U. L. REV. 1371, 1371 (2009).

190. *Id.* at 1391–94; see also Schanzenbach & Tiller, *supra* note 176, at 743–47.

191. Bibas, Schanzenbach & Tiller, *supra* note 189, at 1395.

faced with the prospect of virtually no chance of appellate review, are more likely to impose sentences on the basis of personal preferences to the detriment of uniformity in sentencing.

B. Pre-Plea Bargaining for Sentencing Appellate Waivers is Inefficient

Both the government and the defendant lack valuable information at the plea-bargaining stage. Neither knows whether the district court will adhere to the statutory procedure for imposing the sentence, and neither knows the outcome of the sentencing hearing. Thus, the defendant cannot accurately gauge her contentment with the sentence. Likewise, the government cannot accurately gauge the likelihood that the defendant will appeal the sentence, the likelihood such an appeal would succeed, or the resources that an appeal would consume. If the defendant has only frivolous grounds for appeal, both parties may set a low price on the defendant's appellate waiver. If the defendant has potentially meritorious grounds for appeal, both parties will likely value the defendant's appellate waiver more dearly. At the time of the plea agreement, however, the parties lack critical information about the procedure and substantive outcome of the defendant's sentencing hearing.

Uncertainty impedes using cost-benefit analysis to efficiently bargain unless both parties view the relevant probabilities similarly.¹⁹² If the parties can accurately predict the likelihood of some future event, then they can set the price of the good based on the likelihood of its occurrence. If both parties know that there is a fifty percent probability that a painting is a worthless forgery and a fifty percent probability that the painting is a masterpiece worth \$10,000, the parties can apply a discount based on the likelihood that the work is a forgery and strike a deal to sell the painting for \$5,000. Conversely, a deal may be impossible if the parties estimate the probabilities differently. If the seller believes that there is only a twenty percent chance that the painting is a forgery, and the buyer believes that there is a fifty percent chance that the painting is a forgery, the parties will not be able to reach an agreement. The seller will insist on at least \$8,000 for the painting, but the buyer will not pay more than \$5,000. Moreover, even if both parties place the

192. POSNER, *supra* note 128, § 1.1; *see also* Frank H. Easterbrook, *What's So Special About Judges?*, 61 U. COLO. L. REV. 773, 780 (1990) ("Cases can be settled when parties agree on the likely outcome. When there are no rules of law, when the judge must apply his own weights to inconsistent factors, agreement is less likely."); Teeter, *supra* note 35, at 746 ("Uncertainty is the enemy of the plea bargaining system.").

likelihood that the painting is a forgery at fifty percent, they still may not agree on a price depending on their relative aversions to risk. Most people are risk averse and, as buyers, would rather keep \$5,000 than gamble it on an equal probability of ending up with either \$10,000 or nothing.¹⁹³

For the defendant, the downside of judicial error at sentencing is quite high. An error that increases the defendant's sentence results in a very real cost. An individual defendant has relatively little experience in federal sentencing and likely no experience with the particular sentencing judge.¹⁹⁴ Thus, the defendant has little information about the likelihood for sentencing error and associates a high cost with such error. A high level of uncertainty about a high stakes outcome will lead a cautious defendant to place a higher price on her appellate rights than is warranted.

The government likely has a long history of observing the sentencing behavior of an individual judge. Assuming that the judge is not especially prone to sentencing error or abuse, the government will predict that the defendant is unlikely to have a meritorious basis for a sentencing appeal. Therefore, from the government's perspective, appellate rights are not especially valuable, and most defendants should barter them cheaply and almost as a matter of course.

Because of the inherent uncertainty in the value of future appellate rights, bargaining over sentencing appellate waivers at the pre-plea stage results in inefficient or aborted appellate waiver bargains.¹⁹⁵ During plea bargaining, the parties are merely guessing at the probable value of the defendant's appellate rights given the scant information available. Moreover, the plea agreement does not increase certainty in any particular outcome—the plea agreement only ensures conviction, not the amount of punishment.¹⁹⁶ Drawing a parallel to civil litigation, it would be as if the parties settled the liability aspect of a lawsuit, but left the issue of damages to the court's unreviewable discretion. Uncertainty is greatly diminished after the sentencing hearing, however, and both parties should be able to fairly accurately value the defendant's appellate rights at

193. See POSNER, *supra* note 128, § 1.2; see also Oren Gazal-Ayal & Avishalom Tor, *The Innocence Effect*, 62 DUKE L.J. 339, 374–75 (2012).

194. Even if the defendant's attorney has a wealth of sentencing experience before the judge, the defendant is likely to discount such secondhand information.

195. The inability to reach an appellate waiver agreement may inhibit the parties from striking a plea bargain at all.

196. "C" pleas, discussed *supra* note 10 and accompanying text, are an exception. In these pleas the parties bargain for a particular sentencing outcome that is binding on the court if the court accepts the plea agreement. FED. R. CRIM. P. 11(c)(1)(C).

that time. Thus, negotiations should be quick and efficient, whether or not the parties reach an appellate waiver agreement, based on knowledge of the actual procedure and outcome of the sentencing hearing.

C. Lack of Meaningful Enforcement Fails to Disincentivize Breach

Another significant drawback of folding sentencing appellate waivers into the larger plea agreement is the difficulty in imposing consequences for the breach of the appellate waiver. A defendant who appeals in violation of her appellate waiver faces the prospect that the appellate court will dismiss her appeal. Dismissal places the defendant in a position no worse than if she had abided by her appellate waiver agreement and withheld filing a notice of appeal; the defendant has lost nothing. In the meantime, judicial and government resources are expended in docketing the appeal, moving to dismiss the appeal, and ruling on the motion to dismiss. Even if dismissed, an appeal in violation of an appellate waiver destroys many of the resource-saving benefits that motivate the government to enter into appellate waivers. Additionally, future defendants' appellate waivers lose value every time a defendant appeals in violation of her appellate waiver as the government loses faith that defendants will abide by their agreements. To deter defendants from appealing in violation of their appellate waiver agreements, some sanction is necessary beyond mere dismissal of the appeal.

Some appellate opinions have invited the government to rescind the plea agreement upon finding that a defendant violated the appellate waiver provision.¹⁹⁷ Rescinding the plea agreement allows the government to reinstate dismissed charges, but also requires it to start the prosecution over at square one. That result is unpalatable to many prosecutors, who would rather let sunk costs stay sunk and move forward with new prosecutions. Thus, defendants face no

197. Judge Easterbrook has authored opinions that, on several occasions, have invited the government to reinstate dismissed charges in response to a defendant's breach of an appellate waiver provision. *See, e.g.*, *United States v. Whitlow*, 287 F.3d 638, 640–41 (7th Cir. 2002); *United States v. Hare*, 269 F.3d 859, 862–63 (7th Cir. 2001). But Judge Easterbrook's invitations have drawn criticism. *See Whitlow*, 287 F.3d at 642–43 (Diane P. Wood, J., concurring); *see also* Bennardo, *supra* note 5, at 544–45. The First Circuit has likewise stated that by appealing in violation of an appellate waiver provision, "defendants will risk giving the government an option to disclaim a plea agreement, if it wishes to do so." *United States v. Teeter*, 257 F.3d 14, 26 (1st Cir. 2001); *see also* *United States v. Erwin*, 765 F.3d 219, 228–32 (3d Cir. 2014) (remanding for resentencing in case where the government alleged that the defendant's violation of the appellate waiver in his plea agreement alleviated it of its obligation to move for a downward departure for substantial assistance under an intertwined cooperation agreement).

realistic downside to breaching appellate waiver provisions, and the government and judiciary must expend significant resources to dispose of breaching defendants' appeals.

IV. A PROPOSED POST-SENTENCING APPELLATE WAIVER SYSTEM

Sentencing appellate waivers do not need to be abolished or made contingent on the sentencing court imposing a particular sentence. Procedural reform, however, would improve the system. A post-sentencing appellate waiver system where the defendant and the government enter into a sentencing appellate waiver agreement only *after* the imposition of the sentence would rectify many of the problems that beleaguer current sentencing appellate waivers:¹⁹⁸ concerns about the defendant's voluntariness and knowledge when deciding whether to waive her appeal, fear of lawless district court judges ignoring proper sentencing practices, and the lack of meaningful incentives to deter defendants from breaching their appellate waivers. Although post-sentencing appellate waivers will consume additional trial-level resources, the proposed system will save appellate-level resources and increase efficiency in the broader plea-bargaining process.

A. *The Mechanics of a Post-Sentencing Appellate Waiver System*

After the sentencing hearing, the district court enters its judgment into the record.¹⁹⁹ The judgment is often entered on the same day as the sentencing hearing. Federal criminal defendants then have fourteen days to file a notice of appeal.²⁰⁰ In a system that provides for post-sentencing appellate waivers, the defendant and the government could use this fourteen-day appeal period to agree to an appellate waiver. The government's consideration would likely take the form of some reduction in punishment, such as less time in prison, a smaller fine, a reduction of supervised release, or less onerous conditions of supervision. If the parties reach an agreement, the government would move the district court for a

198. The defendant would remain free to waive her right to appeal her *conviction* in the plea agreement. Because the guilty plea is contemporaneous with the conviction, a plea agreement that waives appeal of errors attendant to the conviction does not present the same sorts of problems as a prospective waiver of the right to appeal errors in a future sentencing hearing.

199. FED. R. CRIM. P. 32(k)(1).

200. FED. R. APP. P. 4(b)(1)(A). This appeal period is not jurisdictional. *See, e.g.*, *Virgin Islands v. Martinez*, 620 F.3d 321, 327 & n.3 (3d Cir. 2010).

reduction of the sentence within the appeal period.²⁰¹ This motion could be styled as a “Motion to Reduce Sentence for Acceptance of Punishment.”

Filing the motion would toll the appeal period. The district court would conduct a hearing to ensure that the defendant knowingly and voluntarily entered into the appellate waiver agreement. The district court would be free to accept or reject the appellate waiver agreement. If it accepted the agreement, the district court would grant the motion to reduce the sentence and amend the judgment.²⁰² If, on the other hand, the district court rejected the appellate waiver agreement and denied the motion, the tolling of the original appeal period would be lifted. The parties could attempt to negotiate another appellate waiver agreement, or the defendant could file (or not file) a notice of appeal.

Adopting this post-judgment appellate waiver mechanism would require a new or amended rule of criminal procedure. The procedural rule would fit well as an amendment to Federal Rule of Criminal Procedure 35, alongside other methods for correcting or reducing a previously-imposed sentence.²⁰³ Such a rule would not be without precedent; the federal rules currently provide mechanisms for various post-judgment motions, including motions for a new trial,²⁰⁴ for a correction of a clear technical or arithmetic error,²⁰⁵ or for a reduction of sentence for substantial assistance to the government.²⁰⁶

201. The entry of judgment does not divest the district court of jurisdiction to hear such a motion. *Cf.* FED. R. CRIM. P. 35(b) (allowing a government motion to reduce sentence for substantial assistance within one year of sentencing or even later in certain instances).

202. The process to amend the judgment would work much in the same way that district courts currently reduce sentences in response to post-sentencing motions based on the defendant’s substantial assistance to the government. *Cf.* FED. R. CRIM. P. 35(b). In the proposed system, the amended judgment would begin the fourteen-day appeal period anew. Even with a valid appellate waiver in place, the defendant would be free to appeal issues that fall outside the scope of the waiver or are unwaivable.

203. Placement within Rule 35 would also alleviate the need for new statutory authorization. *See* 18 U.S.C. § 3582(c)(1)(B) (2012) (authorizing courts to modify an imposed term of imprisonment as permitted by Federal Rule of Criminal Procedure 35).

204. *See* FED. R. CRIM. P. 33.

205. *See* FED. R. CRIM. P. 35(a); *see also* 3 CHARLES ALAN WRIGHT & SARAH N. WELLING, FEDERAL PRACTICE & PROCEDURE § 613 (4th ed. 2011); *United States v. Morillo*, 8 F.3d 864, 868 n.5 (1st Cir. 1993).

206. *See* FED. R. CRIM. P. 35(b).

B. Consequences of a Post-Sentencing Appellate Waiver System

1. Advantages Relative to the Current System

Postponing appellate waiver bargaining until after the sentencing hearing offers significant advantages over the current system. These benefits address concerns regarding the knowledge and voluntariness of the waivers and the efficiency- and incentive-based concerns detailed in the previous Sections.

First, post-sentencing appellate waivers erase any doubt regarding the defendant's ability to enter into a knowing and voluntary waiver. Although individual defendants may still raise challenges to the knowing and voluntary nature of post-sentencing appellate waivers, such waivers could not be found per se unknowing or involuntary. After the hearing, the defendant is fully informed about the sentence's terms and the procedure the court employed in imposing that sentence. Thus, the defendant can estimate her likelihood for success on appeal and intelligently choose whether to bargain with her right to appeal. By moving the appellate waiver negotiation after the sentencing hearing, the defendant is no longer bargaining away the right to appeal the unknown errors of a future proceeding.

Second, and relatedly, both parties are able to more accurately value the defendant's appellate rights after the sentencing hearing. With a complete picture of the sentencing outcome and process, both parties can assess the likely appellate outcome, and the government can weigh the anticipated expenditure of resources in defending the sentence against an appeal. Because both of the parties' assessments would be better informed, their valuations of the defendant's appellate rights are more likely to converge. Additionally, because more accurate information would be available, the appellate waiver bargain is more likely to accurately reflect the true value of the defendant's appellate rights. Defendants with potentially meritorious appellate claims are less likely to undervalue those claims and defendants with only frivolous claims are less likely to overvalue those claims. The government is also more likely to offer a reciprocal benefit commensurate with the actual merit of the individual defendant's potential appellate claims.

Third, separating the appellate waiver agreement from the larger plea bargain ensures that the defendant receives some additional consideration in exchange for her promise not to appeal. The defendant will not waive her appellate right for nothing. Thus, it is fair to conclude that whatever consideration she accepts in exchange for her right to appeal her sentence is adequate. Separating

the appellate waiver from the plea agreement ensures that the defendant receives some additional incremental consideration for her promise not to appeal, even though the sum total of the government's concessions may be identical to those if the sentencing appellate waiver had been included in the plea agreement because the government may offer less at the plea-bargaining stage.

Fourth, separating the sentencing appellate waiver from the larger plea agreement permits the defendant to reject the appellate waiver without rejecting the plea agreement.²⁰⁷ Vice versa, the defendant can enter into a sentencing appellate waiver agreement even if the parties had no plea agreement or the defendant was found guilty at trial. Appellate waivers do not naturally belong in plea agreements. Plea agreements focus on the defendant's admission of guilt. Sentencing appellate waivers concern the defendant's acceptance of the district court's sentence. The absence of one should not impede the existence of the other.

Fifth, delaying sentencing appellate waiver agreements until after the sentencing hearing will remove the incentive distortion created by plea-agreement sentencing appellate waivers. Because neither the parties nor the district court will know whether an appellate waiver will occur until after the sentencing hearing, all parties will have an incentive to conduct the hearing properly. Because every potential sentencing error may translate into additional concessions by the prosecutor to secure a post-sentencing appellate waiver, the prosecutor has an added incentive to ensure that the district court conducts the hearing according to proper procedure. Incentivizing stricter adherence to the procedural and substantive reasonableness requirements of federal sentencing will further reduce disparities in sentences among similarly situated defendants.

Sixth, defendants will be less likely to violate the waiver by appealing. By executing the waiver during the appeal period, defendants will be less likely to second-guess their waiver decisions.²⁰⁸ Rather than waiving the right to appeal some unknown future sentence months in advance, defendants would decide whether to execute post-sentencing appellate waivers during the

207. Federal prosecutors in some districts require defendants to waive their right to appeal their sentence as a provision of the plea agreement. In those districts, some defendants reject the plea agreement and opt to plea open or go to trial in order to protect their right to appeal their sentence. See King & O'Neill, *supra* note 3, at 251–52. Separating the sentencing appellate waiver from the greater plea bargain would allow the parties to enter into a plea bargain even if they did not later enter into a sentencing appellate waiver agreement.

208. See Haines, Jr., *supra* note 5, at 228 (suggesting that a lengthy “cooling off” period after striking a plea bargain gives “the defendant time to experience ‘buyer’s remorse’ and repudiate the plea agreement.”).

fourteen-day appeal period immediately following the district court's judgment. Defendants are less likely to suffer from buyer's remorse in the two weeks after entering into an appellate waiver with full knowledge of their sentence than under the current system, in which defendants must decide whether to waive their right to appeal months in advance of the sentencing hearing.

Additionally, defendants would be less likely to appeal in violation of the waiver because separating the appellate waiver from the plea agreement allows for actual enforcement of the appellate waiver beyond dismissal of the appeal. Defendants currently suffer no penalty, and therefore no disincentive, for breaching their appellate waiver agreements beyond dismissal of their appeal. Because post-sentencing appellate waiver agreements would be independent of plea agreements, the government could penalize a defendant for breaching the appellate waiver agreement while maintaining the plea agreement's integrity. If a defendant violated her post-sentencing appellate waiver agreement, the government could move for the district court to rescind the benefit conferred upon the defendant. Thus, a breaching defendant would lose the benefit of the appellate waiver bargain while keeping the guilty plea intact. By imposing real consequences for the violation of an appellate waiver, post-sentencing appellate waiver agreements will deter breaches.

2. Responses to Anticipated Criticisms

Two anticipated criticisms of a post-sentencing appellate waiver system are the expenditure of additional resources necessary to administer such a system and the concern that the imposition of a lesser punishment is not merited in exchange for a defendant's forbearance of her right to appeal her sentence. The first criticism is a true drawback of the post-sentencing waiver system, but the relative benefits of the proposal outweigh it. The second criticism is ill-founded.

First, critics might argue that post-sentencing appellate waivers will likely require the expenditure of more resources than the current system. Under the current system, the government and the defendant engage in one round of plea negotiations. The post-sentencing appellate waiver system creates the potential for a second round of negotiations. Assuming that an appellate waiver agreement is struck, the district court must hold essentially a second Rule 11 hearing to review the appellate waiver agreement and ensure

that the defendant entered into the agreement knowingly and voluntarily. The addition of these steps is not insignificant in terms of resource consumption.

As discussed above, however, post-sentencing appellate waivers will lead to efficiency gains in other parts of the criminal justice system. Fewer defendants will be likely to violate post-sentencing appellate waiver agreements because breaching the agreement will carry real consequences. This reduction in appeals that are destined for dismissal will save appellate-level judicial, prosecutorial, and governmental defense resources.²⁰⁹ Federal defenders will be spared the need to file opening briefs only to later respond to motions to dismiss on the basis of appellate waivers. Prosecutors will be spared the burden of moving to dismiss on the basis of appellate waivers. Federal appellate courts will be spared the burden of ruling on motions to dismiss based on appellate waivers and scouring the record as the result of frivolous *Anders* appeals.²¹⁰ These resource savings are likely to be substantial, albeit centered in the appellate sphere.²¹¹ Post-sentencing appellate waivers will undeniably add work at the district court level.

Conservation of resources, however, cannot be the overriding goal of the criminal justice system. Otherwise, we could forgo trials and appeals in the name of resource conservation. Conserving resources is only a worthy pursuit when the system that conserves resources leads to the same results as the more costly one.²¹² Just results trump resource conservation. The expenditure of additional resources required by post-sentencing appellate waivers is justified because it achieves more just results.

A second possible criticism of the proposed system is that it explicitly trades defendants' appellate rights for punishment reductions. A newly-sentenced defendant may find that even a modest-but-certain sentence reduction is an irresistible carrot and trade away her appellate rights, especially if she has only borderline appellate issues. Other defendants who never harbored an intention

209. The government funds many defendants' attorneys in the form of federal public defenders or attorneys appointed pursuant to the Criminal Justice Act. *See* 18 U.S.C. § 3006A (2012).

210. *See supra* notes 81–85 and accompanying text.

211. It is difficult to predict whether the proposed system would lead to the execution of more or fewer appellate waiver agreements. Defendants may feel more comfortable waiving their appellate rights after the sentencing hearing because they are content with the outcome. On the other hand, defendants who are unhappy with the sentencing outcome may decline to waive appellate rights. The government may decline to enter into appellate waiver agreements where the defendant lacks any meritorious appellate argument.

212. For example, motions for summary judgment should only be granted when the moving party would have prevailed at trial.

to appeal may threaten appeal just to extract even the most modest benefit from the prosecution.

The above scenarios do not give rise to legitimate concerns. Defendants purportedly receive benefits in exchange for their appellate waivers under the current system,²¹³ so severing the appellate waiver agreement and making the consideration explicit should not raise any new eyebrows. Moreover, defendants have every right to rationally weigh the relative attractiveness of bargaining their appellate rights even for modest punishment reductions. To many, a modest-but-certain sentence reduction may be more enticing than a speculative appeal. Defendants are capable of making these determinations, and the system should permit them to do so. After all, they must live with the consequences.

All else being equal, defendants who agree not to appeal (and then abide by that promise) should receive less punishment than defendants who press frivolous claims through every available level of the court system. Similar to defendants who receive lower sentence calculations for pleading guilty and “accepting responsibility,”²¹⁴ defendants who “accept punishment” by waiving their appellate rights *deserve* less punishment than defendants who fight their punishment tooth and nail. Defendants who accept their punishment are likely easier to rehabilitate. To the extent that acceptance of punishment and responsibility correlates with a lesser likelihood of future dangerousness, society has less of an interest in incapacitating or specifically deterring non-appealing defendants.²¹⁵ Strict retributivists may be unsatisfied with a determination that non-appealing defendants receive a smaller desert, but the concept should be no less palatable than reducing the punishment of a defendant who pleads guilty and receives a sentence reduction for acceptance of responsibility.

CONCLUSION

Sentencing appellate waivers are not inherently problematic. Rather, it is the timing of the waivers that creates problems. The parties cannot efficiently bargain over a plea-agreement provision that they cannot accurately value, and they cannot accurately value

213. See King & O’Neill, *supra* note 3, at 232–35.

214. See, e.g., U.S. SENTENCING GUIDELINES MANUAL § 3E1.1 (2013).

215. But see King & O’Neill, *supra* note 3, at 260 (opining that defendants who agree to appellate waivers are “no less culpable or easier to rehabilitate” and “may simply be opportunists” seeking less punishment). The same claim could be made of defendants who elect to plead guilty in exchange for a punishment reduction.

a defendant's promise not to appeal her sentence until after the sentence has been imposed. Although this valuation problem does not rise to the level of an unknowing or involuntary waiver, it does leave some plea agreements unconsummated and others lopsided.

Postponing the sentencing appellate waiver agreement until after the sentencing hearing will restore the threat of potential reversal to the sentencing process, thereby better incentivizing district court judges to adhere to proper sentencing procedures. Defendants will also be less likely to breach separate sentencing appellate waiver agreements for fear of losing the incremental benefit received in exchange for their promise not to appeal. In short, postponing the appellate waiver agreement until after the sentencing hearing will lead to better bargaining, better sentencing, and better adherence to the terms of appellate waiver agreements.