

TRANSCRIPT OF PROCEEDINGS

JUDICIAL CONFERENCE ADVISORY)
COMMITTEE ON CRIMINAL RULES)

PUBLIC HEARING ON PROPOSED)
AMENDMENTS TO THE FEDERAL)
RULES OF CRIMINAL PROCEDURE)
)

REVISED AND CORRECTED TRANSCRIPT

Pages: 1 through 144

Place: Washington, D.C.

Date: November 5, 2014

HERITAGE REPORTING CORPORATION

Official Reporters
1220 L Street, N.W., Suite 600
Washington, D.C. 20005-4018
(202) 628-4888
contracts@hrcourtreporters.com

BEFORE THE ADMINISTRATIVE OFFICE OF THE UNITED STATES
COURTS

JUDICIAL CONFERENCE ADVISORY)
 COMMITTEE ON CRIMINAL RULES)
)
 PUBLIC HEARING ON PROPOSED)
 AMENDMENTS TO THE FEDERAL)
 RULES OF CRIMINAL PROCEDURE)
)

Mecham Conference Center
 Thurgood Marshall Federal
 Judiciary Building
 1 Columbus Circle, N.E.
 Washington, D.C.

Wednesday,
 November 5, 2014

The parties met, pursuant to notice, at 9:00 a.m.

BEFORE: HONORABLE REENA RAGGI
 Chair

APPEARANCES:

Participants:

HONORABLE REENA RAGGI
 HONORABLE JAMES C. DEVER, III
 HONORABLE MORRISON C. ENGLAND, JR.
 HONORABLE GARY SCOTT FEINERMAN
 HONORABLE DAVID E. GILBERTSON
 HONORABLE RAYMOND M. KETHLEDGE
 HONORABLE DAVID M. LAWSON
 HONORABLE TIMOTHY R. RICE
 HONORABLE AMY J. ST. EVE
 PROFESSOR SARA SUN BEALE
 PROFESSOR DANIEL R. COQUILLETTE
 PROFESSOR ORIN S. KERR
 PROFESSOR NANCY J. KING
 CAROL A. BROOK, Esquire
 MARK FILIP, Esquire
 LAURAL L. HOOPER
 JONATHAN C. ROSE, Esquire

Heritage Reporting Corporation
 (202) 628-4888

APPEARANCES: (Cont'd.)

JOHN S. SIFFERT, Esquire
JONATHAN WROBLEWSKI, Esquire
DAVID BITKOWER, Esquire

I N D E X

<u>Witnesses:</u>	<u>Page</u>
NATHAN FREED WESSLER American Civil Liberties Union	5
CHRISTOPHER SOGHOIAN American Civil Liberties Union	24
KEVIN S. BANKSTON Open Technology Institute New American Foundation	38
JOSEPH LORENZO HALL Center for Democracy and Technology	54
ALAN BUTLER Electronic Privacy Information Center	71
AMIE STEPANOVICH Access and the Electronic Frontier Foundation	85
AHMED GHAPPOUR University of California Hastings College of the Law	110
ROBERT J. ANELLO Federal Bar Council	137

P R O C E E D I N G S

(9:00 a.m.)

CHAIR RAGGI: Okay. I'm Reena Raggi. I'm the chairman of the Advisory Committee on the Criminal Rules. Around the table are the members of the Rules Committee. We want to thank all of you for coming to these public hearings today and for offering us your views on the rules that have been put out for public comment. I think all of you who have asked to speak today are speaking on Rule 41 or at least the vast majority of you are.

Again, I cannot emphasize how important it is to the work of the Rules Committee to have people put in the time to give these rule amendments careful consideration and constructive criticism. I say that because I know how much work had to go into this by each of your organizations, and I do want you to know how much we appreciate it.

How we're going to proceed this morning is to invite you all to make statements. In most of your cases we also have your written submissions, which we have already reviewed. But we're happy to hear you orally for about 10 minutes each. The committee may then have some questions for you. I hope you'll do your best to answer them for us. Again, it all serves

1 the purpose of making our review more informed.

2 So let's get started. I think the first
3 witness we'd like to hear from is Nathan Freed Wessler
4 from the American Civil Liberties Union.

5 MR. WESSLER: Good morning. Thank you, Your
6 Honors. Thank you, committee. Are these on?

7 (Pause.)

8 MR. WESSLER: Okay. Good morning. Thank
9 you for the opportunity to speak today on behalf of
10 the American Civil Liberties Union. Let me just begin
11 by saying that we really appreciate the careful
12 scrutiny the committee has given to the proposed
13 amendment to Rule 41 so far and your response to the
14 ACLU's and others' input last spring. I'm here to
15 offer additional testimony and the written comments we
16 submitted last week to help further inform your
17 deliberations.

18 I'm a staff attorney with the ACLU's Speech,
19 Privacy, and Technology Project, and I will address
20 legal and policy concerns we have with the proposed
21 amendment. Following my testimony you'll hear from
22 colleague, Chris Soghoian, who's our principal
23 technologist. He'll be able to address technological
24 concerns we have with this proposal.

25 The ACLU urges the committee to reject the

1 proposed amendment to Rule 41. This is not to deny
2 that the government now faces a conundrum when it
3 wants to remotely install surveillance software on a
4 computer in a criminal investigation but does not know
5 where that computer is located. However, the proposed
6 amendment raises far more questions than it answers
7 and would significantly expand use of a controversial,
8 invasive, and potentially damaging law enforcement
9 technique while failing to concomitantly regulate and
10 constrain that use.

11 If the searches the government seeks to
12 carry out are ever permissible pursuant to a Rule 41
13 warrant, and there's good reason to doubt that they
14 are, they need to be heavily regulated. Otherwise,
15 they will violate the Constitution and weaken
16 cybersecurity in entirely predictable ways.

17 But such regulation I think is beyond the
18 ambit of the Federal Rules of Procedure. The
19 government should present its case to Congress and to
20 the American people, and Congress should be given the
21 opportunity to craft comprehensive legislation
22 regulating government hacking, just as it regulated
23 wiretapping in Title III.

24 On its face, this proposal appears to simply
25 be a procedural tweak to the venue rules, but in

1 practice, the proposed amendment would have a broader
2 effect. It implicates myriad substantive issues that
3 will defy easy solution. The proposal should not be
4 viewed as a mere minor procedural change for several
5 reasons.

6 First, it is no answer to say that the
7 government is already hacking into computers to
8 install remote search software. Such searches have
9 not so far been contemplated by the Federal Rules, nor
10 sanctioned by legislation. They have been addressed
11 in only one public court opinion, which rejected the
12 government's application on particularity and other
13 grounds.

14 While I appreciate the committee's intent to
15 leave constitutional questions to ongoing caselaw
16 development, a body of caselaw about these searches is
17 unlikely to develop at least in the near future. Lack
18 of notice of these searches, excessive government
19 secrecy, the good-faith exception to the exclusionary
20 rule, the doctrine of qualified immunity, and the lack
21 of technical knowledge of computer security and
22 information systems architecture among magistrate
23 judges will hamper effective judicial review.

24 Indeed, we know that the FBI has used the
25 so-called CIPAV program to conduct remote access

1 searches for over a decade, and yet there is no
2 publicly available judicial opinion addressing it.

3 Second, in effect, the proposed amendment
4 assumes the conclusion that remote access searches are
5 constitutional. But as a category, these searches
6 threaten to violate the reasonableness, particularity,
7 and probable cause requirements of the Fourth
8 Amendment. These searches are unreasonable under the
9 Fourth Amendment because exploiting vulnerabilities in
10 computer systems and the internet to surreptitiously
11 install malware onto suspects' computers has the
12 potential to cause serious and widespread damage to
13 computers, including by opening the door to other
14 malicious actors to enter. On a larger scale, the
15 whole premise of stockpiling so-called zero-day
16 vulnerabilities in commonly used software weakens
17 cybersecurity for everyone.

18 These searches will generally fail the
19 particularity and probable cause requirements of the
20 Fourth Amendment as well. As has been amply
21 demonstrated by the Stuxnet episode and others, once
22 the government releases malware onto the internet, it
23 is difficult to control where it ends up. It is
24 entirely predictable that these searches will affect
25 not just particularly identified suspects but

1 unidentified targets and innocent nonsuspects as well.

2 One example is the 2007 investigation in
3 Washington State where the FBI impersonated the
4 Associated Press by creating a fake news story, sent a
5 link to that story to the suspect via social media,
6 and then waited for him to click on it and thereby
7 download remote search software. Once posted to
8 social media, though, the FBI would likely have lost
9 the ability to control who clicked on the link and
10 thus whose computer was searched. So-called watering
11 hole attacks raise this concern even more explicitly.

12 And further, even in searches with a lower
13 risk of malware spreading, the very thing that
14 triggers application of this new Rule 41 subsection,
15 the concealment of the location of the target
16 computer, will often mean that the government cannot
17 particularly describe the place to be searched. This
18 concern was highlighted, I think eloquently, by
19 Magistrate Judge Smith in his opinion out of the
20 Southern District of Texas last year.

21 A final constitutional concern is that this
22 proposal will not only sanction widespread use of
23 delayed notice searches but will necessarily result in
24 no notice searches in numerous cases. By requiring
25 only that the government make reasonable efforts to

1 provide notice of the search, the proposal
2 contemplates searches for which no notice actually
3 reaches the target or others affected. Yet searches
4 without notice are constitutionally infirm. A rule or
5 procedure that explicitly authorizes searches for
6 which no notice will be provided crosses the line into
7 substance.

8 Third, issues of procedure and substance are
9 so entangled in this proposal that the best course is
10 to allow Congress to act and to craft a statutory
11 solution. The proposed amendment effectively decides
12 that remote access searches are appropriate when the
13 location of a target's computer is unknown. But this
14 kind of intrusive electronic surveillance raises
15 particularly difficult legal and policy questions, and
16 Congress has expressed a preference for legislative
17 regulation of these sorts of invasive surveillance
18 practices.

19 If these searches are ever to be
20 constitutional, they must be heavily regulated in the
21 manner of Title III. By creating a mechanism to
22 conduct these searches using Rule 41 warrants without
23 exhaustion, minimization, and other limitations, the
24 proposed rule would effectively decide via rulemaking
25 a question better left to congressional regulation.

1 In closing, let me just say that I
2 understand the impetus to act to address an asserted
3 gap in the government's search powers, but doing so
4 via the proposed amendment to the Federal Rules will
5 open up a Pandora's box beyond this committee's power
6 to control. We respectfully recommend that the
7 committee reject the proposed amendment and let the
8 Department of Justice make its case to our elected
9 representatives.

10 That concludes what I have prepared. I
11 would be very happy to address questions or discussion
12 with the committee.

13 CHAIR RAGGI: Thank you. As I said, we've
14 also read the prepared remarks that you've given us,
15 but let me ask if there are any questions from the
16 committee. Professor Kerr?

17 PROF. KERR: Just a quick question. Can you
18 say a little bit more about why you think if the
19 amendment goes forward that would inhibit
20 constitutional challenges later? Because I guess one
21 counter-argument to consider would be that if the
22 technique is never used there could not be a
23 constitutional challenge because there would be no
24 case or controversy that could allow an Article III
25 court to step in. So, if you could sort of take us

1 through a little bit more why you think use of the
2 technique will actually stop the development of the
3 law on that grounds, that would be great.

4 MR. WESSLER: It's not that I think it will
5 stop development of law but rather that there will be
6 precious few opportunities in which judges will
7 actually weigh in, so that my point is really that the
8 committee should be careful before relying on an
9 expectation that the caselaw will robustly develop to
10 address all of these questions.

11 I think there are several reasons for that.

12 I mentioned some legal doctrines that for sure
13 operate in other Fourth Amendment areas too but in
14 this area will be particularly pronounced, so the
15 doctrine of qualified immunity, the good faith
16 exception to the exclusionary rule, because of the
17 problem with providing notice of these searches,
18 because of excessive government secrecy, in our view
19 excessive, around use of these techniques where we
20 have seen in these and similar electronic search areas
21 investigators and prosecutors going to great lengths
22 to conceal key and material details about what they
23 are doing from defense attorneys.

24 So you have a trouble on the back end for
25 having truly adversarial arguments, and then at the

1 front end, when a magistrate judge is reviewing these
2 applications, I think there are a couple problems.
3 One is that most magistrate judges simply aren't, and
4 there's no reason they should be, technical experts.
5 But it's an inherently ex parte proceeding.

6 You know, I'm a lawyer who spends most of my
7 time working on these issues, and were it not for our
8 technologist, who I work with closely in my office, I
9 would have a hard time understanding what all the real
10 implications of these issues are.

11 I think a related problem is that in the few
12 actual examples of applications for remote access
13 search warrants that we've seen from the government,
14 there's a consistent tendency to use euphemism or to
15 use vague description, terms like "network
16 investigative technique" or "remote investigative
17 technique" I think, "remote search technique," without
18 describing how the software will actually be
19 delivered, what kind of computer security problems it
20 may cause, the likelihood of affecting third parties'
21 computers, and just the -- I guess the last reason I
22 think we have concerns -- or maybe not the last, but
23 the last that comes to mind is that inherently this
24 technology very seriously risks affecting total
25 nonsuspects, nontargets, because of the ease with

1 which software travels over the internet, and in some
2 types of searches, these so-called watering-hole
3 attacks, intentionally it will affect whole ranges of
4 people.

5 But the troubles with providing notice for
6 these kind of searches will mean that in some cases
7 suspects who are actually charged and indicted may
8 know about it, but those third parties may never know.

9 And the person who does know may not have Fourth
10 Amendment standing or Article III standing to
11 challenge on behalf of those others affected who may
12 in fact have the stronger privacy argument under the
13 Fourth Amendment.

14 I can go on, but, you know, I'll stop there,
15 and just to say that our real point here is that the
16 committee should, as you are doing, should grapple
17 with the whole range of constitutional and statutory
18 issues now, and we think that the proper outcome of
19 that inquiry is to let Congress act in the first
20 instance because it can regulate in a much more
21 detailed and particular way.

22 CHAIR RAGGI: Judge Rice.

23 JUDGE RICE: If you could redraft the
24 amendment, how would you redraft the notice provision
25 to address the concerns you raised?

1 MR. WESSLER: So we do have suggestions
2 about redrafting the amendment. To be clear, we don't
3 think they could address all of our concerns. Some of
4 our concerns I think clearly could only be addressed
5 through real substantive regulation by Congress if
6 they can be addressed at all.

7 On the notice provision, I think there's one
8 tweak that could help, which would be to change the
9 word "or" to "and," right, so where the amendment says
10 "The officer must make reasonable efforts to serve a
11 copy of the warrant on the person whose property was
12 searched or whose information was seized or copied,"
13 to substitute "property was searched and whose
14 information was seized or copied." Maybe to say
15 "person" or "persons" would help to avoid a situation
16 where the government, you know, gets notice to
17 somebody tied to a physical computer, but that person
18 may actually not have the privacy interest here.

19 So that's one piece. I think on the broader
20 question, though, I understand why there's a perceived
21 need to change to the "use reasonable means" language
22 because of inherent difficulties when you don't know
23 where someone is and the information that is returned
24 by this malware may be limited. But inherently, you
25 know, conducting a search where notice is not going to

1 be given we think is unconstitutional. And so I'm not
2 sure there's actually a way to fix that problem
3 statutorily except by actually requiring notice, which
4 may preclude some of these searches. But I think that
5 may be the only, you know, outcome.

6 I'll just say that in terms of suggestions
7 for changing the sort of more substantive initial part
8 of the amendment, we have some suggestions. We'd be
9 happy to provide them to the committee, with the
10 understanding that, again, they only go part of the
11 way towards addressing our concerns and they really
12 can't get at many of the issues.

13 JUDGE RICE: Yes, that would be helpful.
14 Thanks.

15 CHAIR RAGGI: Anything else?

16 PROF. BEALE: Judge?

17 CHAIR RAGGI: Yes. Professor Beale.

18 PROF. BEALE: So I was wondering whether you
19 think the current rule is invalid because it allows
20 several options in terms of notice, so you must give a
21 copy of the warrant and a receipt for property taken
22 to the person from whom or from whose premises the
23 property was taken, or leave a copy of the warrant and
24 the receipt at that place, and it may not be picked up
25 by the person whose property was taken. And I think

1 there might be sort of a parallel here, that an effort
2 is made to provide the notice, but it doesn't get --
3 because there's only limited -- so do you think that
4 the Fourth Amendment standard is that the person
5 actually receives effective notice or that there's
6 proper effort to provide notice? Which do you think
7 is the constitutional standard?

8 MR. WESSLER: I think the constitutional
9 standard should be actual notice.

10 PROF. BEALE: Actual receipt of notice.

11 MR. WESSLER: Actual receipt of notice, but
12 I will say that I think that that issue is all the
13 more difficult and important in the electronic search
14 context, partly because so many people may be
15 affected. You know, it's a rare, very rare search in
16 the physical world where, you know, hundreds of
17 people's information may be taken pursuant to, you
18 know, a search of a server, for example, where lots of
19 people are keeping sensitive records. You know, it's
20 hard to imagine a physical analog to that, maybe a
21 doctor's office and their records.

22 PROF. BEALE: Right.

23 MR. WESSLER: But there you have, you know,
24 a person who actually has a relationship with those
25 whose privacy interests was affected and absent a gag

1 would be able to actually tell them.

2 PROF. BEALE: Right. I think that is the
3 standard typically, where you serve it on one of the
4 tenants who's there or the person whose office is
5 being managed, and then it's up to that person to make
6 sure that it gets to the other individuals, and they
7 may or may not do it in the physical world.

8 MR. WESSLER: Yes. No, I understand that
9 that's right. And, you know, for example, in the
10 Stored Communications Act context, you know, we have
11 serious concerns about the government practice of
12 giving notice only to the cloud storage provider or
13 the email provider and then the person whose email
14 account it is never receives notice. We think that --

15 PROF. BEALE: Unless the provider gives it.

16 MR. WESSLER: Unless the provider gives it.

17 And some providers have been very aggressive about
18 doing that, and that's terrific. But the burden
19 shouldn't be on them to undertake the time and expense
20 to do that in our opinion.

21 PROF. BEALE: So you think that practice
22 should change as well.

23 MR. WESSLER: Yes, yes.

24 PROF. BEALE: Thank you.

25 CHAIR RAGGI: Oh, I'm sorry. Judge

1 Feinerman.

2 JUDGE FEINERMAN: Good morning.

3 MR. WESSLER: Good morning.

4 JUDGE FEINERMAN: I'm going to ask you a
5 question that's similar to the question that Judge
6 Rice asked. You recognize that there's a problem, a
7 venue problem that the department faces when the
8 location of the computer is concealed in some way.
9 What's your solution to that problem?

10 MR. WESSLER: I think our solution is for
11 the Department of Justice to approach Congress,
12 present the problem, and for Congress to holistically
13 regulate these searches in the manner of Title III, to
14 require minimization, to require exhaustion, to
15 require a heightened and more particularized factual
16 showing of particularity and probable cause as to the
17 place searched and the information seized, et cetera.

18 JUDGE FEINERMAN: I'm talking about the
19 venue provision. So say the dispute moves to Congress
20 and you're testifying in front of a congressional
21 committee and they say what court should the
22 department go to in order to get this warrant to
23 search a computer whose location is unknown. What's
24 your answer?

25 MR. WESSLER: So I don't know that I have a

1 full answer. I mean, I understand the inherent
2 problem here, and I think if Congress was to regulate,
3 it would have to go part of the way towards where this
4 committee's proposal is now. You know, I do think
5 that the language "any district where activities
6 related to the crime may have occurred" in the context
7 of digital searches opens up the possible venues too
8 far. You know, I think a limitation to any district
9 where substantial activities related to the crime have
10 occurred could help.

11 You know, and we're talking about internet
12 searches or searches related to interstate commerce
13 over the internet. You may have servers in 15 states
14 and emails transiting through 27 other states that,
15 you know, may have some tie to the crime. And I
16 think, you know, once it's opened up that much, the
17 concerns about venue shopping are just too great.

18 So I don't have a full answer to you except
19 to say that I would expect Congress, if they wanted to
20 address this problem, would have to come up with some
21 solution to the venue piece, but I think it should be
22 more narrowly drawn.

23 JUDGE FEINERMAN: All right. Thank you.

24 CHAIR RAGGI: Mr. Bitkower.

25 MR. BITKOWER: Thank you. I just want to

1 focus a little on what the scope of your objection is.

2 You talk a lot about the difficulties inherent in
3 remote searches, but most of your remarks relate to
4 the use of network investigative techniques. Do your
5 same objections apply to any remote search, or are
6 your objections focused on the use of techniques like
7 these?

8 MR. WESSLER: So we have concerns about any
9 remote search. Now most of these remote searches
10 require one of these techniques. I mean, inherently,
11 unless you have the consent of the person whose
12 computer you're trying to remotely search as a
13 government investigative agent, then there needs to be
14 some technical means to enter their computer, and
15 computers, you know, computer security is now such a
16 foreground of concern for all of us that firewalls and
17 virus protection programs and other protections make
18 it difficult without one of these technological means.

19 And I'll leave it to my colleague, Mr. Soghoian, to
20 help address that in a little more detail.

21 But I think there are concerns certainly in
22 the notice area, in the sort of Title III analogous
23 types of regulation of exhaustion and minimization
24 where it would not matter what the actual technical
25 means of entry, surreptitious entry, and exfiltration

1 of information were.

2 MR. BITKOWER: Well, if I can just follow up
3 on that. So, if your view is we should wait until
4 Congress acts to have a provision to allow remote
5 searches, if I can imagine a case where the government
6 is aware that child pornography is kept on a server
7 and a former employee of the criminal organization
8 provides the government with the password and log-in,
9 is it your view that it would be unconstitutional to
10 use that password and log-in until Congress acts to
11 create a statute?

12 MR. WESSLER: So having not thought entirely
13 through this question, so speaking for myself at the
14 spur of the moment, I'm not sure it would be
15 constitutionally problematic for the government then
16 to go to the physical server and access it. But
17 there's a question about what information they would
18 be -- pursuant to a valid warrant, right? But that
19 server presumably is being contacted by numerous
20 people, and the government's interest in part may be
21 to identify who those people are, where they are, what
22 they're doing, who their associates are. And if it
23 comes to then using that server to remotely search
24 those people's computers, then I think we're back to,
25 you know, all the problems attendant with these highly

1 internetworked information systems.

2 MR. BITKOWER: Right. But the basic
3 question of whether it's appropriate for the
4 government to search the server itself, if we assume a
5 server whose location is unknown, through the use of
6 the password and log-in credentials, is it your view
7 that the law currently makes that unavailable and that
8 it should be unavailable until Congress acts?

9 MR. WESSLER: If the government does not
10 know where that server is and is trying to remotely
11 log in, then I think the current formation of Rule 41
12 doesn't give the government a venue to get that
13 warrant. Now, as one of the other witnesses will
14 discuss, you know, that server could well be in
15 another country, and then we have questions about, you
16 know, the power of United States courts to issue
17 warrants for foreign searches and then all the
18 prudential concerns about comity and war powers, et
19 cetera.

20 But the basic question of -- you know,
21 beyond the fact that the rules I think do not give a
22 venue, there's no option to do that now, on the
23 constitutional side, I think some concerns remain,
24 although the basic reasonableness concerns about, you
25 know, breaking the computer security settings,

1 potentially destroying information, probably are not
2 present in that situation because you're not using new
3 software to put on that computer to try to get
4 information out.

5 CHAIR RAGGI: Thank you very much. We
6 appreciate your taking time with us today.

7 MR. WESSLER: Thank you.

8 CHAIR RAGGI: We'd next like to hear from
9 Christopher Soghoian. Mr. Soghoian, I hope I've
10 pronounced your name correctly.

11 MR. SOGHOIAN: Members of the committee,
12 thank you very much for giving me the opportunity to
13 testify before you today. So my name is Christopher
14 Soghoian. I'm the principal technologist for the
15 ACLU's Speech, Privacy, and Technology Project.
16 Before I begin my remarks, I want to make it very,
17 very clear I am not a lawyer. I am a computer
18 scientist who speaks English about technology to
19 lawyers. The goal of my coming here today is to try
20 and explain things to you and to answer any questions
21 you have. If you walk away more confused after my
22 remarks, I've not done my job.

23 So many of you may have seen in the
24 newspapers about a week ago a story about the FBI
25 impersonating the Associated Press. So that story

1 came out of my work. In the course of preparing for
2 this process and researching our comments, I went
3 through and did as much research as I could. I read
4 every warrant application that is public for a network
5 investigative technique or CIPAV. I read through
6 probably more than 800 pages of heavily redacted
7 documents that the DOJ had provided to civil liberties
8 groups and journalists in response to FOIA requests.
9 I have spoken to a number of people who have worked
10 for the government that have aided the teams that
11 deploy malware. I've tried to learn everything that I
12 possibly can.

13 In that incident that gained a lot of press
14 last week that happened in Seattle in 2007, we should
15 step back and note that in 2001 the FBI first
16 acknowledged that it had the capability to hack into
17 people's computers. In 2001, the capability was
18 called Magic Lantern, which was far too media-
19 friendly, so by the next year they had changed it to
20 the more boring CIPAV. But it wasn't until 2007 that
21 the media first learned of a single incident where the
22 FBI had used this technique.

23 Now, to be clear, they had put it into heavy
24 rotation by 2002, but it took more than six years for
25 the public to learn of a single case and for a single

1 application for a warrant and the warrant itself to
2 become public.

3 It took until 2014 for the United States
4 public to learn how the CIPAV tool in 2007 was
5 actually delivered, and it was because I was reading
6 through documents and stumbled across a single page
7 that referenced this fake Associated Press story. Had
8 it not been for this committee's invitation for the
9 public to submit comments and had it not been for the
10 10 hours I spent reading FOIA documents a week ago
11 Monday, we would not know that the FBI impersonated
12 the Associated Press.

13 The reason I bring this up is I think that
14 this neatly characterizes the persuasive secrecy that
15 surrounds the FBI's use of this technique and in fact
16 many other surveillance techniques. The government
17 considers their CIPAV or net tools to be sensitive
18 sources and methods that must be kept secret at all
19 costs because they fear that any public discussion of
20 these tools would mean that they would no longer be
21 effective. And I understand their concerns, but
22 they're keeping all information about these techniques
23 secret from the public, from defense counsel, and in
24 many cases from judges.

25 As I noted before, in the course of my

1 research, I have read every public warrant application
2 for the use of a net or CIPAV tool that has been made
3 public. There are probably half a dozen to date.
4 They include applications to hack into individuals'
5 computers and at least in one other case into the
6 computers of every individual who visits a particular
7 website.

8 I've read through all of these affidavits
9 and all the applications, and as someone with a Ph.D.
10 focused on surveillance, a background in computer
11 science, I still struggle to figure out what the
12 government is asking the courts to approve. The
13 government uses the most vague terms. So, for
14 example, they will ask a court to approve the
15 insertion of computer code into a webpage that causes
16 visiting computers to transmit their location
17 information.

18 There is nothing contained in that text that
19 would reveal to a judge, particularly a judge that is
20 not an expert on technology, there's nothing there
21 that would reveal to the judge that what the
22 government is in fact seeking is permission to hack
23 into someone's computer. There is nothing there that
24 would reveal that they plan to exploit security flaws
25 in that person's web browser or operating system or

1 word processing program. There is nothing there
2 indicating that they plan to impersonate a news
3 organization or other trusted third party.

4 So, for example, the 2007 Timberline High
5 School application that I referenced before, it does
6 in fact say we would like to use CIPAV and this is
7 what the CIPAV tool collects. But there is nothing in
8 there saying how the CIPAV tool will get onto the
9 computer to target or that the FBI plans to engage in
10 any form of impersonation to get this tool onto the
11 target's computer.

12 So this form of secrecy is not unique to the
13 government's use of hacking tools. In an article that
14 I published earlier this year in the *Yale Technology*
15 *Law Journal*, co-authored by Stephanie Powell, a former
16 national security prosecutor with DOJ, we argue that
17 the government has in fact practiced similar secrecy
18 with another tool known as the Stingray, which is a
19 sophisticated cell phone surveillance device. That
20 tool has been in use since the mid-1990s. It's
21 basically now in the hands of every local law
22 enforcement agency that wants it, yet we only have two
23 public court orders in 20 years in which judges have
24 even really considered the technology and only one of
25 those in which the judges considered the Fourth

1 Amendment issues at hand. These surveillance
2 technologies are really escaping thorough analysis by
3 the courts because the government is going out of its
4 way to keep everything about them secret.

5 Okay. So a couple technical issues that I
6 just want to bring to light and focus your attention
7 on. The first is that even after the government's use
8 of malware or hacking tools is discovered
9 inadvertently by the public, the FBI doesn't fess up
10 to its use of these tools. And so, for example, in
11 the summer of 2013, the computer security community
12 noticed that visitors to several popular websites that
13 could only be accessed via Tor were receiving malware.

14 This malware caused their computers to send
15 special information back to a data center in Virginia
16 run by Verizon, but there was nothing in the malware
17 itself that researchers analyzed, nor anything in the
18 information that was transmitting that gave a clear
19 signal that this was something being run by the FBI.
20 It wasn't until several months later when an FBI agent
21 testified in an Irish court that the public finally
22 got confirmation that this was an FBI operation.

23 The reason this is important is because the
24 computer security community itself, the computer
25 security experts who study malware, who have to be on

1 the lookout for suspicious software, who have to
2 decide whether to allow software in or out of their
3 networks, they themselves have no idea what the
4 government is doing not only in the moment but months
5 or years later.

6 And the reason that concerns me is that the
7 government doesn't have the finest track record when
8 it comes to computer security. As we note in our
9 comments, there were 25,000 breaches that federal
10 agencies reported last year. The White House just a
11 week and a half ago revealed that their own network
12 had been hacked by the Russian Government.

13 If the FBI's malware malfunctions and
14 causes, you know, some kind of further computer
15 security issue to the affected targets, we have no way
16 of knowing if the FBI will let people know and say,
17 you know what, sorry, you know, that was our software.

18 It accidentally spread to innocent people's
19 computers. It accidentally, you know, crashed 1,000
20 computers. From everything that we've seen to date,
21 you know, they're not going to put out a press release
22 and acknowledge that it was their fault.

23 As I said before, I have read through every
24 public warrant application for the use of malware.
25 Two things that struck me -- well, actually, three

1 things that struck me reading these. The first is in
2 one case in Colorado that we were looking at last
3 December, a judge authorized the delivery of malware
4 to an incorrect email address. The email address
5 initially provided by prosecutors was not the right
6 address, and so prosecutors had to come back a few
7 days later and provide the valid email address.

8 Now thankfully, in that situation, they did
9 not send the malware to the wrong email address, but I
10 think the issues that we have already in the physical
11 world of the police kicking down the wrong door are
12 ever-present in the online world. And at least in the
13 physical world, when the police kick down that door
14 and they are expecting a man and they see a woman and
15 they're expecting someone of a certain age and they
16 see someone of a different age, they immediately have
17 some idea that they've gotten the wrong email address.

18 I suspect that in the case of malware, the malware
19 may be able to get further before they realize that
20 they have sent things to the wrong address.

21 That's the first issue of sort of incorrect
22 delivery of malware. My colleague, Nate, referenced
23 the use of watering-hole attacks, and so for those of
24 you who don't know this, these are attacks that target
25 everyone who visits a particular website. In the

1 Freedom Hosting incident that I referenced before in
2 the summer of 2013, we don't know what the judge
3 authorized in that case because, although the malware
4 itself has been analyzed, the warrant application for
5 that incident isn't public.

6 But what is clear is that rather than just
7 delivering malware to the computers of people who are
8 visiting illicit websites, the FBI delivered malware
9 to the computers of anyone who visited any website
10 that was hosted by the same service. And let me just
11 unpack that for a second.

12 We are now firmly in an era of cloud
13 computing. Cloud computing means that many, many
14 websites share the same resources online. Today, if
15 you're visiting *The New York Times* or *The Washington*
16 *Post* or whitehouse.gov, because the U.S. Government
17 has now embraced cloud computing, you have no idea
18 which other sites are sharing those same resources.
19 And the servers may change. A server that is hosting
20 *The New York Times'* website today may be hosting a
21 competitor's website tomorrow or an illicit online
22 gambling operation. I mean, you can go to Amazon,
23 give them your credit card, and rent a server in five
24 minutes, but you won't get your own server. You will
25 get a slice of someone's server.

1 And so because we are now firmly in this era
2 of cloud computing, it raises particular concerns when
3 the government starts delivering malware to everyone
4 who visits a particular server, not everyone who
5 visits a site delivered by that server, because
6 consumers do not know which servers are actually
7 powering the websites they deliver.

8 Now I don't know what the affidavit said. I
9 don't know if the judge authorized more than he or she
10 should have or if the FBI interpreted the
11 authorization in an overbroad way, but there have been
12 no consequences for the FBI's delivery of malware to
13 people who are merely checking their email through the
14 Tor mail service or people who are merely looking at
15 what was called *The Encyclopedia of the Dark Web*.
16 There were legitimate, lawful sites that were being
17 run on the same service. People visiting them had no
18 idea that they were visiting a site that was sharing
19 server space with an illicit site, and those people
20 shouldn't have been targeted.

21 The last technical issue I'd like to bring
22 to your attention, reading between the lines of the
23 government's submission, it seems pretty clear that
24 the technology that they are worried the most about is
25 something called Tor, Tor, The Onion Router. This is

1 a widely available piece of software that allows
2 people first to hide their activities online but also
3 to set up websites where the location of the server is
4 not known to the visitors or to anyone else who would
5 seek to forensically analyze that service.

6 If you are not well-read on this topic, you
7 might get the idea that Tor is some kind of evil
8 technology made by bad people to allow other bad
9 people to hide. That is about as far as you can get
10 from the truth. Tor was created by the Naval Research
11 Lab here in Washington, D.C. It was created to allow
12 naval investigators to investigate crimes online
13 without the criminals they were investigating learning
14 that they were being investigated by the Navy.

15 Now the problem is the intention of Tor is
16 to allow people to blend into a crowd. The Navy
17 investigators needed a crowd to blend into. And if
18 the only people using the crowd were naval
19 investigators, then they wouldn't be blending in very
20 well at all. So they needed cover traffic. They
21 needed a crowd to blend into. And, of course, the way
22 you get that crowd is by providing a free service
23 online.

24 And so the folks at the Naval Research Lab,
25 when they created Tor, they fully acknowledged that

1 there would be bad people using the service, that
2 there would be people using it to access illicit
3 content, to post material that's objectionable, to
4 even hide illegal activities. But they needed that
5 traffic. They knew that to get the good you have to
6 get the bad. And when you provide a communication
7 service and you open it up to the whole world, you
8 have to accept the fact that bad people are going to
9 use it too, in the same way that, you know, auto
10 manufacturers have to deal with the fact that bank
11 robbers buy cars on occasion. They don't get to pick
12 who buys cars.

13 CHAIR RAGGI: Mr. Soghoian, you understand
14 you're well past your time. Do you want to wrap up?

15 MR. SOGHOIAN: Just 20 seconds more, ma'am.

16 CHAIR RAGGI: Thank you.

17 MR. SOGHOIAN: So the Naval Research Lab,
18 which created this, that was not the last involvement
19 of the U.S. Government. In fact, the State Department
20 has continued to fund Tor for the last few years.
21 They funded it as recently as this year. Tor gets
22 millions of dollars a year by the U.S. Government.
23 This is a technology -- the reason it's funded is to
24 enable dissidents in China and Iran to communicate
25 anonymously without their governments -- their human

1 rights-abusing governments monitoring them.

2 The reason I bring this up is that Tor is
3 not something that was created in the dark. This was
4 created by the U.S. Government. It is still funded by
5 the U.S. Government. It is a tool of U.S. Government
6 statecraft, and so it's a little bit odd to see on one
7 hand the U.S. Government creating Tor and then on the
8 other hand to see another piece of the U.S. Government
9 saying, well, this thing is creating so many problems
10 for us, now we need the authority to hack into any
11 computer in the world.

12 Thank you very much. I'd be happy to answer
13 any questions you have.

14 CHAIR RAGGI: Thank you.

15 Any questions? Professor Kerr.

16 PROF. KERR: Chris, a technological
17 question. I recognize your concerns with the use of
18 the CIPAV techniques. Are there technological
19 alternatives to the use of those techniques in the
20 kinds of cases where they've been used, like
21 Magistrate Judge Smith's opinion in Texas? Is the
22 concern that the government is improperly using
23 invasive techniques where they could solve the case
24 with less invasive techniques, or is it more that this
25 seems to be the only way to solve the case, but that

1 method is nonetheless too intrusive in your view?

2 MR. SOGHOIAN: I mean, we don't have a full
3 understanding of even the totality of the government's
4 capabilities. So, for example, we just learned in
5 December of last year through an ex FBI official
6 talking to *The Washington Post* that the FBI has the
7 ability to control webcams without the webcam light
8 turning on. That was a new capability that I didn't
9 know about. I suspect that there are other really
10 creative techniques that they have that raise also
11 similar concerns.

12 On the question of the Smith order, you
13 know, I'm not a law enforcement official. I've never
14 investigated a crime. I don't know how you would go
15 about doing that. My understanding is in this case
16 all they had was an email address. They didn't know
17 even which country the person was in. You know, I
18 don't know how you go about investigating that kind of
19 crime. But as a technologist, my primary objections
20 are the issues associated with the delivery of the
21 software and then the collateral damage associated
22 with how the software might function.

23 I'm personally less concerned about the
24 information that the software collects but far more
25 concerned about the kicking of the computer's front

1 door and the fact that this door is like left wide
2 open and anyone else can go and walk in and the
3 information that the government is required to
4 purchase or stockpile in order to have the capability
5 to open that door.

6 And, you know, I understand that this
7 committee feels like it needs to focus on the issues
8 that it understands the most, the legal questions, the
9 concerns of what information can be accessed with
10 which pieces of paper. But as a computer scientist,
11 as someone coming from the technical community, the
12 greatest concerns are actually those of how do they
13 get into the computer in the first place.

14 CHAIR RAGGI: Any other questions?

15 (No response.)

16 CHAIR RAGGI: Mr. Soghoian, we thank you
17 very much for appearing today.

18 MR. SOGHOIAN: Thank you.

19 CHAIR RAGGI: We'll hear next from Kevin
20 Bankston of the Open Technology Institute at the New
21 America Foundation.

22 MR. BANKSTON: Good morning, Your Honor and
23 members of the committee. Thank you for allowing New
24 America's Open Technology Institute to testify and
25 share our concerns about the proposed amendment to

1 Rule 41 regarding remote access searches.

2 I'm here today in my capacity as the policy
3 director of OTI to question the basic and quite
4 substantive premise that's implicit in the proposed
5 amendment, which is that remote access searches by the
6 government or, more accurately in many cases, the
7 government's surreptitious hacking into computers or
8 smartphones in order to plant malware that will send
9 data from those devices back to the government are
10 allowed by the Fourth Amendment.

11 Based on precedent almost a half century
12 old, we believe that the proposed amendment authorizes
13 searches that are unconstitutional for lack of
14 adequate procedural protections that are tailored to
15 counter these searches' intrusiveness, much like the
16 New York State electronic eavesdropping law that was
17 struck down as unconstitutional by the Supreme Court
18 in Berger v. New York nearly 50 years ago.

19 There the Court held that because electronic
20 eavesdropping by its very nature involves an intrusion
21 in privacy that is broad in scope, authority to
22 conduct such surveillance should only be granted under
23 the most precise and discriminate circumstances in
24 order to ensure that Fourth Amendment particularity is
25 met.

1 In response to that 1967 case, Congress in
2 1968 passed the federal wiretapping statute, often
3 referred to as Title III. There Congress addressed
4 the Supreme Court's Fourth Amendment concerns by
5 providing a precise and discriminate warrant procedure
6 for wiretapping and electronic eavesdropping, with
7 procedural safeguards so demanding that commentators,
8 including Mr. Kerr, routinely refer to Title III
9 orders as super-warrants.

10 Foremost among those Title III safeguards
11 are the four that are intended to enforce
12 particularity, consistent with the Berger decision,
13 which held that the need for particularity is
14 especially great in the case of eavesdropping. The
15 Court in U.S. v. Torres in the Seventh Circuit, the
16 first of many Circuit Courts, defined that these four
17 Berger-derived requirements are also constitutionally
18 required in the case of video surveillance, summarized
19 them well. I've quoted that in my testimony, but they
20 basically boil down to exhaustion of other
21 investigative techniques, a particular description of
22 the communications to be seized or intercepted, strict
23 limitation on the duration of the interception, and
24 finally and perhaps most importantly, minimization of
25 the interception of communications that were not

1 particularly described in the warrant.

2 As the Torres court concluded, each of these
3 four requirements is a safeguard against electronic
4 surveillance that picks up more information than is
5 strictly necessary and so violates the Fourth
6 Amendment's requirement of particular description.

7 Title III, consistent with Berger and the
8 Fourth Amendment's demand of reasonableness, also
9 includes a clear requirement of notice on the target
10 of the surveillance soon after the surveillance is
11 completed, with no exceptions for failure to notify.

12 And finally, Title III includes a number of
13 additional super-warrant requirements intended by
14 Congress to further ensure the reasonableness of this
15 surveillance, including a requirement that the
16 surveillance only be used in the investigation of
17 specifically enumerated serious crimes. Only with
18 such super-warrant requirements in place have warrants
19 for electronic surveillance been found constitutional
20 under the Fourth Amendment.

21 Today, nearly half a century later, we are
22 faced with a digital surveillance technique that is
23 substantially more invasive than the analog electronic
24 surveillance techniques of the past. Yet this
25 committee, without any support from Congress or the

1 courts, is poised to explicitly authorize warrants for
2 such remote access searches with no additional
3 protections at all and with a constitutionally novel
4 allowance for cases where notice may not be given or
5 received by the target.

6 This is particularly concerning because the
7 procedural protections required of eavesdropping,
8 video surveillance, wiretapping, are even more
9 necessary here when the devices to which the
10 government seeks access can contain an unprecedented
11 wealth of private data, our digital papers and
12 effects, if you will.

13 Indeed, the one published decision to
14 address a warrant application regarding a remote
15 access search, Magistrate Judge Smith's opinion in
16 Houston last year, the In re Warrant case, rejected
17 the application based not only on Rule 41
18 considerations but also based on a failure to satisfy
19 the particularity requirement, including the enhanced
20 Berger-Torres particularity requirements typically
21 applied to electronic surveillance.

22 The proposed amendment, in attempting to
23 address the Rule 41 issue raised by Judge Smith's
24 opinion, necessarily also makes a substantive judgment
25 regarding the Fourth Amendment's application to remote

1 access searches. It does so first by authorizing
2 remote access searches where the location of the
3 target computer is unknown, a type of search that
4 Judge Smith found was a per se violation of the
5 requirement that the place to be searched be
6 particularly described, and second, by choosing not to
7 insist that remote access searches meet the Berger-
8 Torres requirements that undoubtedly apply.

9 Those requirements undoubtedly apply, as
10 Judge Smith held, because remote access searches
11 implicate and amplify all of the same problems of
12 previous electronic surveillance techniques by virtue
13 of providing access to an even greater wealth of
14 private information. As he described and as the
15 Supreme Court described in the Riley case earlier this
16 year, computers and smartphones contain a wide wealth
17 of information, which is described at greater length
18 in my written testimony, the upshot simply being that
19 at this point the search of a computer or a smartphone
20 is, according to the Supreme Court, more invasive than
21 even the most exhaustive search of one's home.

22 In that technological context, the
23 constitutional necessity of applying the Berger-Torres
24 particularity requirements to remote access searches
25 is clear. That need, especially in regard to

1 minimizing the search of devices or the seizure of
2 data that are not particularly identified in the
3 warrant, is amplified even further by several other
4 risks that have been discussed at length by other
5 commentators as well as Judge Smith.

6 These risks include the privacy risks to
7 nonsuspects who share the target computer, which might
8 be a public terminal at a library or a café; the risk
9 that the government software may spread to nontarget
10 computers; the possibility in cases of botnet
11 investigations or so-called watering-hole attacks that
12 thousands or even millions of computers may be
13 infected with remote access software; and the risk
14 that the software used to remotely access any of those
15 computers may end up causing damage either by altering
16 or deleting data or creating security vulnerabilities
17 that may be exploited by others.

18 Indeed, it may be that remote access
19 searches carry so many risks that they are
20 unreasonable under the Fourth Amendment or, as a
21 policy matter, even if they satisfy the Berger-Torres
22 requirements. Notably, neither the courts nor
23 Congress have yet addressed those questions, which
24 brings me back to my starting proposition, that by
25 explicitly authorizing remote access searches, the

1 proposed amendment represents a substantive judgment
2 regarding the constitutionality of those searches and
3 a policy judgment regarding the appropriateness of
4 such searches, regardless of the committee note claim
5 that the amendment does not address constitutional
6 questions.

7 The proposed amendment's explicit
8 authorization of remote access searches where the
9 computer location is unknown, in the face of one
10 published decision on the matter, finding that such
11 searches are per se violations of the Fourth Amendment
12 represents a substantive legal judgment.

13 The proposed amendment's unprecedented
14 allowance for situations where notice may not be given
15 to the target in the context of caselaw that's never
16 provided any exception to that rule is a substantive
17 legal judgment.

18 The proposed amendment's authorization of
19 remote access searches without requiring satisfaction
20 of the Berger-Torres particularity requirements,
21 contrary to the one published decision finding that
22 those requirements do apply, is a substantive legal
23 judgment.

24 Ironically, so too would it be a substantive
25 legal judgment for the committee to include those

1 requirements, which just further demonstrates how the
2 substantive and procedural questions on this issue are
3 inextricably intertwined.

4 Ultimately, such substantive expansions of
5 the government's authority as those represented in
6 this proposed amendment are not the province of this
7 committee. We therefore urge the committee to reject
8 the proposed amendment and leave these substantive
9 constitutional and policy questions where they belong,
10 in the courts and in Congress.

11 Thank you for your consideration, and I
12 welcome your questions, although I'd love to use the
13 remainder of my time to address one of the questions
14 that was directed to the ACLU, which was the question
15 of whether and to what extent Rule 41 already
16 authorizes these searches. You gave the example of a
17 case of a remote log-in, would the court be able to
18 issue a warrant for that search.

19 I think that a court could plausibly find
20 that Rule 41 as written and the inherent authority of
21 the court allow them to issue such a warrant. In
22 fact, many courts have issued such warrants. This is
23 analogous to the situation in the Torres case where
24 the court prior to applying the Title III
25 particularity requirements held that Rule 41 and the

1 inherent power of the court allowed it to authorize
2 video surveillance, a decision that was then followed
3 by many Circuit Courts.

4 However, I think if this committee prior to
5 Torres and those many other Circuit Courts agreeing
6 with it had made that substantive decision on its own
7 that indeed Rule 41 authorizes such searches and that
8 the inherent power of the court authorizes such
9 searches and tried to codify that in the rule, I think
10 that would be a substantive decision that this
11 committee would not be authorized to make.

12 I think it would be different if after the
13 Torres court and the many other Circuit Courts that
14 have agreed with it ruled that Rule 41 did authorize
15 such searches and laid out the procedures necessary to
16 ensure that they are constitutional, if the committee
17 codified that, I think that would be more on the
18 procedural side of things. But hopefully that
19 addresses your question. Thank you.

20 CHAIR RAGGI: Thank you. Do we have any
21 further questions for Mr. Bankston? Yes, please, Mr.
22 Bitkower.

23 MR. BITKOWER: I just want to follow up on
24 your last comment, Mr. Bankston, because I'm not sure
25 exactly where it leaves us in terms of what your view

1 of the law is. It seems to me that you're saying that
2 there are cases in which you believe consistent with
3 the probable cause and particularity requirements of
4 the Fourth Amendment the government could remotely
5 search a computer.

6 MR. BANKSTON: I did not say that. I said
7 that it is plausible that a court may conclude that
8 Rule 41 in its inherent authority allows it to issue a
9 remote access search warrant. I did not state that I
10 believe that it's plausible that that would be
11 constitutional, and in fact I would have serious
12 constitutional concerns about that.

13 MR. BITKOWER: So your view is a court might
14 act unconstitutionally.

15 MR. BANKSTON: Huh?

16 CHAIR RAGGI: Is that a question?

17 MR. BITKOWER: I'm just trying to understand
18 it. I guess your view is not that there is any sort
19 of constitutional basis that you would agree is
20 currently constitutional. Your view is just that we
21 should let the courts decide those questions before
22 the committee acts.

23 MR. BANKSTON: Yes.

24 CHAIR RAGGI: Yes, Judge Feinerman.

25 JUDGE FEINERMAN: Let me ask you the same

1 question I asked Mr. Wessler. There are situations
2 where the owner of a computer engaged in criminal
3 activity, say trafficking in child pornography, hides
4 the location of the computer. The government wants to
5 investigate. What's your solution to the venue issue?

6 What court should the government be allowed to go to
7 in order to get a warrant to search that computer if
8 it doesn't know where the computer is?

9 MR. BANKSTON: Well, and I'm afraid my
10 answer is somewhat similar to Mr. Wessler's, which is
11 we have not developed a position on that. I think
12 that to the extent the Justice Department is raising
13 that problem, that is distinctly a policy problem that
14 is most appropriately addressed in Congress rather
15 than in this committee.

16 JUDGE FEINERMAN: So are you saying that in
17 the meantime the government can't go anywhere in order
18 to get a warrant to search a computer that is being
19 used for child pornography where it doesn't know where
20 the computer is until Congress acts?

21 MR. BANKSTON: I think that congressional
22 action would be the -- Congress would be the
23 appropriate venue to address that issue. As Judge
24 Smith noted and several of us have also noted, I think
25 there are potentially fatal particularity problems for

1 issuance of warrants where the place to be searched is
2 unknown and cannot be stated.

3 JUDGE FEINERMAN: Okay. So what is the
4 government to do in the meantime?

5 MR. BANKSTON: That's a wonderful question
6 to be debated in a policy arena. And --

7 JUDGE FEINERMAN: No, I'm saying before the
8 debate occurs and before a resolution is reached by
9 Congress, what is the government to do in the
10 meantime? Just not do anything?

11 MR. BANKSTON: I think that it should with
12 great haste go to Congress to seek a solution to this
13 problem.

14 CHAIR RAGGI: Mr. Filip, did I see that you
15 had a question as well?

16 MR. FILIP: No. Judge Feinerman touched on
17 my question.

18 CHAIR RAGGI: Okay. Thank you.

19 PROF. BEALE: May I have one more?

20 CHAIR RAGGI: Yes, Professor Beale.

21 PROF. BEALE: Was there statutory
22 authorization for the tracking warrants, or is that an
23 example where the rules imposed fairly specific
24 particular requirements on a new form of technology?
25 And that really is a question. I thought you might

1 know, you might have thought about that as an analog.

2 And we were just looking. We weren't seeing it.

3 MR. BANKSTON: You mean the tracking
4 provisions in Rule 41 as opposed to cell tracking?

5 PROF. BEALE: Correct, correct, correct.
6 And, again, it is a question that was before my time.

7 MR. BANKSTON: Yeah, well, and before my
8 time as well. I believe that that was essentially
9 attempting to codify the Supreme Court's rulings in
10 Karo and Knotts rather than creating a new authority
11 out of whole cloth. But I honestly --

12 PROF. BEALE: So we agree it may be an
13 analogy that we could think about, but neither of us
14 has enough information at this point to draw too much
15 wisdom from it.

16 MR. BANKSTON: Yeah.

17 PROF. BEALE: Thank you.

18 CHAIR RAGGI: Before you sit down, I'm going
19 to play off questions that have already been asked
20 you. I'm going to ask you to consider the possibility
21 that what the committee is striving to do here is
22 avoid getting itself into the discussion that you all
23 have articulated about what is required for this kind
24 of a remote warrant to be constitutional and limit its
25 own actions to assuming that a constitutional warrant

1 could be crafted where it is presented to a judicial
2 officer. And so what I'm asking you to assume is that
3 what we are trying to do with the rule is avoid
4 intruding into Congress or anyone else's sphere about
5 what would be constitutionally required and speaking
6 only to the question of where the warrant could be
7 sought. Why do you think that we have a problem with
8 the current rule in drawing that line?

9 MR. BANKSTON: I mean, I think you stated it
10 yourself. To create that rule, you first need to
11 assume that such a warrant can be constitutionally
12 issued, and that to us seems a substantive decision
13 that would be more appropriately debated and decided
14 in a policy arena or in the courts.

15 CHAIR RAGGI: Well, just to use the Berger
16 analogy that you urged us to draw on, the rules have
17 never spoken to what would satisfy particularity, what
18 would satisfy the additional requirements of the
19 Constitution, which after all speaks in terms of
20 reasonableness, not in terms of specific criteria
21 along the lines you've identified. That litigation
22 will continue to go through the courts, and that
23 debate would be certainly carried on in Congress. The
24 rule is striving not to limit that in any way. Why do
25 you think we don't succeed?

1 MR. BANKSTON: I mean, I think if we're
2 analogizing to Berger, that's a situation where there
3 was extensive -- there was Supreme Court, indeed
4 Supreme Court precedent laying out procedures --

5 CHAIR RAGGI: Right. So the courts -- what
6 I'm trying to suggest to you is the courts would still
7 be able to decide either at the issuance stage or at
8 the review stage that these kind of warrants -- and
9 they are not all of a kind -- need certain extra
10 features, so to speak, to satisfy constitutional
11 reasonableness, but none of that would be limited or
12 cabined in any way by a venue procedural rule. At
13 least that's what we are striving towards. So I want
14 to know why we don't succeed.

15 MR. BANKSTON: I certainly recognize that's
16 what you're striving for. I do feel that explicit
17 authorization for this type of warrant in the Federal
18 Rules, when the constitutionality of such warrants is
19 in doubt and has not been established, that seems
20 unavoidably substantive.

21 CHAIR RAGGI: Not the courts' problem. You
22 don't want us to act on venue until it's clarified as
23 to constitutionality.

24 MR. BANKSTON: I think acting on venue in
25 regard to a type of search the constitutionality of

1 which has not been established and which has not been
2 authorized by Congress is premature.

3 CHAIR RAGGI: All right. We thank you very
4 much for your time.

5 MR. BANKSTON: Thank you very much.

6 CHAIR RAGGI: Could we hear next from Joseph
7 Lorenzo Hall from the Center for Democracy and
8 Technology?

9 MR. HALL: Hi, everyone. I have to
10 apologize to the committee and the witnesses that come
11 after me. I have to leave immediately after you're
12 done with me, so I've left a bunch of business cards.
13 You're welcome to get in touch with me subsequently.

14 And so thank you for the opportunity to
15 address you today. My name is Joseph Lorenzo Hall.
16 I'm the chief technologist with the Center for
17 Democracy and Technology. CDT is a nonprofit public
18 interest organization dedicated to promoting policies
19 and technical standards to protect civil liberties,
20 such as privacy and free expression, globally. I'm
21 also not a lawyer. I have a Ph.D. Two members of my
22 Ph.D. committee were law professors, though, so maybe
23 I have a little bit more facility with that stuff.
24 Pam Samuelson and Deirdre Mulligan, if you know them,
25 they're awesome.

1 I co-authored the written testimony today
2 with CDT's senior counsel, Harley Geiger, and I'm
3 happy to take questions of the law specific to our
4 testimony and fold them back into our written comments
5 due in February.

6 So I'll start by emphasizing we recognize
7 that law enforcement faces real challenges in securing
8 search warrants in criminal investigations on the
9 internet where things like location are just not the
10 same and have really no analog to what we have in the
11 physical world. But we do believe that changes that
12 have some of these legal policy and technological
13 implications like that in the proposed amendment in
14 question should happen in a public legislative debate.

15 I'm going to make my oral remarks about five
16 minutes. I've got five points to make, so it should
17 happen pretty quickly.

18 First, the proposed amendment would
19 authorize extraterritorial searches that will
20 circumvent the MLAT, Mutual Legal Assistance Treaty,
21 process and may violate international law. Simply, if
22 the location of a computer is concealed, it can be
23 anywhere in the world. It may even be in the
24 international space station, which has really fun
25 jurisdictional issues to think about. The issue as to

1 whether or not magistrates may circumvent the MLAT
2 process and issue warrants to search data abroad is
3 under active litigation at the moment.

4 Second, the proposed amendment joins other
5 elements of Rule 41 --

6 CHAIR RAGGI: May I interrupt you to just
7 ask where that is under litigation?

8 MR. HALL: That's the Microsoft Ireland
9 case. It's cited in our written testimony.

10 CHAIR RAGGI: Thank you. Go ahead.

11 MR. HALL: New York? Yeah, I should be able
12 to recite that.

13 PROF. KING: Southern District of New York.

14 MR. HALL: Yeah, there you go.

15 Second, the proposed amendment joins other
16 elements of Rule 41 that authorize searches outside of
17 a magistrate's judicial district. However, those
18 other cases were specifically grounded in authorizing
19 legislation. So subsections (b)(3) and (b)(5) [of
20 Fed. R. Crim. P. 41] allow warrants to issue for
21 searches outside the magistrate's judicial district
22 respectively in cases involving terrorism-related
23 activity and within U.S. jurisdiction but outside any
24 specific federal judicial district.

25 Both of these changes were either directly

1 added by legislation, the USA Patriot Act of 2001 for
2 section (b)(3), or as a result of specific legislative
3 augmentation of judicial authority in the case of
4 (b)(5), also a result of the Patriot Act.

5 Third, the triggers for new authority to
6 issue a warrant here are not at all that specific.
7 The committee note attached to the proposed rule
8 change says "The amendment provides in two specific
9 circumstances." These are not specific circumstances.
10 Techniques that have the effect of concealing
11 location are used regularly every day by hundreds of
12 millions of people worldwide. In no way is using
13 these kinds of tools, standards, and mechanisms
14 indicative of illegal or suspicious activity.

15 To the extent that you or anyone in this
16 room have ever used a computer to securely access
17 sealed or confidential documents over what's called a
18 VPN, a virtual private network, you've done exactly
19 this. The proposed amendment is poorly tailored as to
20 seem even absurd circumstances, such as someone
21 misreporting their location on things like Facebook
22 and Twitter. It should not reach something that
23 absurdly trivial.

24 Secondly, approximately 30 percent of all
25 computers in the world are infected with malware,

1 malicious software of some sort. The second provision
2 of the proposed amendment hinges on damage without
3 authorization under the Computer Fraud and Abuse Act,
4 but damage under that statute is so broadly defined as
5 to encompass any computer that is infected with
6 malware, viruses, Trojans, any kind of malicious
7 software. Nothing about technical mechanisms that
8 conceal location or damage devices under the CFAA is
9 specific. These circumstances will reach a truly vast
10 quantity of computers worldwide.

11 Fourth, four out of five, the proposed
12 amendment expands the authority for remote access,
13 which is in no uncertain terms law enforcement
14 hacking. Unlike in the physical world, these kinds of
15 searches and seizures involve exploitation and
16 penetration of computing systems which can very easily
17 damage these systems or impact services in the real
18 world that they mediate. And I'm happy to take
19 technical questions about having a log-in or maybe
20 less intrusive ways of getting this information that
21 we know of.

22 The record before you has a number of cases
23 where this kind of law enforcement hacking has gone
24 wrong, leaving scores of innocent people and their
25 devices in the lurch. In the physical world, the law

1 enforcement agent can be reasonably certain that
2 entering a premises will not result in the building
3 falling down or even all the buildings around it
4 falling down, but we cannot be so sure online.

5 Further, law enforcement agents cannot be
6 certain online that what appears to be a single-family
7 home is not in fact a nuclear power plant or a
8 hospital or anything that may be even less crucial
9 than that.

10 Finally and lastly, we are concerned that
11 the five or more district consolidation mechanisms,
12 this venue piece, aimed at botnets specifically in the
13 proposed amendment would result in forum shopping. So
14 that is, if the applicable precedent varies across
15 districts or if a particular district's magistrates
16 are more likely to issue remote search and seizure
17 warrants, these warrants will be issued at a higher
18 volume and separately will be much less likely that
19 the targets can physically travel or secure counsel to
20 challenge these warrants and that the caselaw
21 development the amendment seeks not to address will
22 not evolve to address the kinds of concerns you're
23 seeing today. Thank you.

24 CHAIR RAGGI: Thank you very much. We have
25 a number of questions.

1 MR. HALL: Oh, please.

2 CHAIR RAGGI: Judge Kethledge.

3 MR. HALL: If they're legal, I'm going to
4 write them down, so --

5 JUDGE KETHLEDGE: That's all right. Thanks
6 for coming to see us today, Mr. Hall. I understand
7 you're not a lawyer. I think you're doing pretty well
8 in speaking our language. But specifically, your
9 point about the language in the proposed rule
10 regarding techniques to conceal location and your
11 point that you think that is overbroad and it captures
12 a lot of pedestrian, benign uses like VPNs, do you
13 have any suggestions about how that potentially could
14 be narrowed to apply more specifically to the sort of
15 nefarious activity that the government is concerned
16 about?

17 MR. HALL: So I'll have to take that back
18 and think about it. But certainly when it comes to
19 narrowing that language, it seems like on some extent
20 you need some of the evidence you're seeking to get to
21 do the narrowing. So, for example, maybe you could
22 say something like -- and I'm just totally speaking
23 freely here. Maybe you could say something like the
24 action of concealing the location was instrumental for
25 the criminal activity. And so something that sort of

1 segregates garden-variety things that we all do, some
2 of which our employers require us to do that have this
3 kind of technical concealment element to it.

4 And the most basic thing here is location
5 means nothing in the digital world. You know, you
6 have an IP address, which is a series of numbers, that
7 is your network location that has a somewhat tenuous
8 connection to your geographical location. There are
9 techniques to link the two, but they are error-prone
10 and not nearly as systematic as like, you know, GPS
11 coordinates or a telephone book with an address in it
12 or something like that.

13 But we can certainly think about that. We
14 didn't in our written testimony propose any
15 recommendations because we wanted to hear the whole
16 thing, but we'll certainly think about that and put it
17 in our comments.

18 JUDGE KETHLEDGE: Sure. Thank you.

19 CHAIR RAGGI: Professor Beale.

20 PROF. BEALE: Mr. Hall, does it change your
21 views any to focus on the fact that the anonymizing
22 software, the technique that conceals, is not part of
23 the probable cause, right? So the officer seeking the
24 warrant has to separately demonstrate probable
25 cause --

1 MR. HALL: Yes.

2 PROF. BEALE: -- to show that evidence of a
3 crime could be found at the place to be searched, and
4 the anonymizing software or the concealment only goes
5 to the question of which courthouse you go to, right?

6 Because when I saw a reference to a VPN, I use a VPN,
7 right? Most people do --

8 MR. HALL: I hope so.

9 PROF. BEALE: -- if they're traveling
10 remotely or at their work. But I believe that doesn't
11 increase my chances of being searched under this
12 amendment. This is really only about forum shopping.

13 And do your remarks at all depend -- when you were
14 saying it has to be connected to illegality and it's
15 really innocent, if we focus on that, does that change
16 your view at all?

17 MR. HALL: Well, certainly to the extent
18 that there's some connection with the criminality to
19 the concealment, that makes a big difference. The
20 trick is that right now, as it's written, you know, it
21 triggers the authority for the magistrate to issue
22 these kind of warrants on that simple technical fact.

23 PROF. BEALE: No, no, no. You have to show
24 probable cause.

25 MR. HALL: Well, certainly, you know, in the

1 process, but, you know, for magistrates to even have
2 the ability to do these remote things, you need this
3 rule change or you wouldn't be doing it, right?

4 CHAIR RAGGI: I think what you don't
5 understand --

6 MR. HALL: Maybe I'm not understanding.

7 CHAIR RAGGI: -- is that whether you seek
8 the warrant in Washington, D.C. right now depends on
9 your being able to say the computer is here in
10 Washington, D.C.

11 MR. HALL: Yeah.

12 CHAIR RAGGI: You don't know where it is
13 because of the anonymizing, but the harm is being done
14 in New York.

15 MR. HALL: Uh-huh.

16 CHAIR RAGGI: Now go to the court in New
17 York. That's what this changes is it --

18 MR. HALL: Yeah.

19 CHAIR RAGGI: -- gives you the ability to go
20 in New York if that's where the harm is occurring.
21 How does that --

22 MR. HALL: May be occurring, right.

23 CHAIR RAGGI: Okay.

24 PROF. BEALE: Is alleged, yeah.

25 CHAIR RAGGI: Well, that's a question for

1 the magistrate to evaluate.

2 MR. HALL: Sure.

3 CHAIR RAGGI: But does that affect any of
4 your remarks at all?

5 MR. HALL: I guess I'm having a hard time
6 understanding the gulf here. But certainly, you know,
7 anonymizing tools necessarily route information
8 throughout the global internet. And so that's the
9 reason they do what they're supposed -- that's the
10 reason they accomplish what they accomplish is that
11 they make sure that nodes that are distributed over
12 all of humanity, you know, route traffic. And so they
13 will necessarily implicate things like the MLAT -- you
14 know, issues of jurisdiction that are very bigger than
15 just the United States.

16 So I don't know. Maybe feel free to send me
17 the question again and I'll try and do a better job.

18 CHAIR RAGGI: Mr. Filip, you have a
19 question.

20 MR. FILIP: I think maybe this will help
21 clarify it some. The probable cause determination --

22 CHAIR RAGGI: Could you turn on the mike?

23 MR. FILIP: Sure. The probable cause
24 determination can be done in various ways:
25 circumstantially, direct evidence. It's never

1 required that you need evidence that you can only get
2 through a search warrant in order to get the search
3 warrant, right, because that can't be --

4 MR. HALL: Yeah.

5 MR. FILIP: -- that's just not reasonable.
6 So you independently have established probable cause
7 to believe that a crime is occurring, and it could be
8 any of a variety of crimes. I think typically in this
9 area it's fraud or child pornography, maybe mostly
10 child pornography. But you have reason to believe
11 that child pornography is occurring. Maybe consistent
12 with what you said that location is not sort of the
13 principal driver, what the venue rule would seek to do
14 I think is consistent in some ways with what you're
15 talking about because the location is unknowable for
16 whatever reason, because people have taken steps so
17 that it is effectively unknowable, so you have a
18 probable cause determination.

19 You have the reality that the location is
20 unknowable. And so this rule would seek, without
21 trying to adjudicate upfront whether or not ever a
22 warrant could be constitutional, what would be
23 required, what 25 years of caselaw might conclude a
24 generation from now, it seeks I think to address the
25 issue that Judge Feinerman is asking about, which is

1 what courthouse do you go to to start the debate.

2 MR. HALL: Yeah.

3 MR. FILIP: And so, in terms of thinking
4 about sort of potential reforms or tweaks or
5 improvements, I think it would be really helpful to
6 try to work within that framework.

7 MR. HALL: And my initial thought is that it
8 would definitely need to be some very well-informed
9 courthouse, maybe a subset -- and this is where I get
10 out of my element here, but someone that has the
11 technical capabilities to address the issues that will
12 be discussed in the other parts of the warrant that
13 aren't specific to the venue. But I think that's a
14 really important part to this because, you know, very
15 few magistrate judges have the capabilities that we've
16 seen people like Judge Smith actually bring to bear
17 when you actually address these questions and dig
18 really deep into them in the full context of one of
19 these warrant applications.

20 CHAIR RAGGI: Anything else?

21 PROF. BEALE: So may I ask you about your
22 concern about going around the MLATs and so forth?
23 How can the government use the MLAT process if it
24 doesn't know whether the computer might be or the
25 device might be in another country and, if so, which

1 country it is?

2 MR. HALL: So they'll certainly know where
3 the exit, so where the last hop through the network
4 was. The trick here is that piercing the veil of
5 where all the other hops are is a serious technical
6 challenge that people that developed this software
7 work very hard to make sure that cannot happen because
8 there are extremely hostile adversarial governments
9 trying to exploit this stuff as well that don't have
10 the respect for human rights that we do.

11 So I don't know how to answer your question
12 in the sense that -- you know, I'll think about it,
13 but that's a fundamental problem with trying to do
14 these investigations, you know, that if you don't know
15 where it is and if they're using one of these tools,
16 you necessarily raise questions that involve
17 international law and the MLAT process.

18 But the whole point is -- the simple point
19 that we were trying to make there was that even the
20 fact of a magistrate going around the MLAT process
21 when you do know where the crime has occurred, in the
22 Microsoft Ireland case, even one where you don't have
23 this location concealment problem, it's still under
24 consideration even without the -- and it's still, you
25 know, developing in ongoing litigation right now

1 without even the concealment element.

2 CHAIR RAGGI: Judge Feinerman.

3 JUDGE FEINERMAN: Thank you, Mr. Hall. You
4 said during your testimony location means nothing in
5 the digital world. Could you -- right. Could you
6 elaborate on that from the perspective of a scientist?

7 MR. HALL: Sure. So the notion of network
8 location means something. There are certain aspects
9 of the devices that most of you have in front of you
10 or in your pockets used to be addressed on the
11 network. Those don't have very strong connections to
12 actual physical geography. IP addresses, which are a
13 string of numbers that identify where you are, we use
14 the domain name system to translate something like
15 josephhall.org into 136.84.92.1. I totally made that
16 up. It's not like I memorize that stuff.

17 That's why we have the DNS, so I don't have
18 to remember that. But certainly there are entities
19 that you don't need to know anything about that issue
20 IP addresses, and you can take them wherever you want.

21 So, as someone who has been issued a chunk of these
22 numbers, you can move to, you know, some different
23 part of the country, some different part of the world
24 and fundamentally sever any historical connection you
25 may have had between the mapping of geographic

1 location and the network location.

2 And that's why I think even using the word
3 location in terms of remote search strikes people with
4 technical knowledge as just fundamentally just strange
5 because are you talking about geographic location?
6 Are you talking about network location? In certain
7 cases with the use of the CIPAV, these computer
8 internet protocol address verifier techniques, they're
9 seeking to get elements of network location, and then
10 law enforcement uses other techniques to try and drill
11 down where that network location maps into sort of
12 geographic reality to do the actual jurisdictional
13 stuff that you struggle with every day.

14 And so the reality is they're very fluid.
15 They're meant to be so that, you know, we don't have
16 the sort of, you know, cyberspace anchored to what we
17 call meet space. You know, it's sort of a very fluid
18 way of doing things where data would necessarily have
19 more of the characteristics of nonpublic goods, of
20 things that you can't copy, of things that have some
21 of these elements of -- you know, you can't occupy
22 space. I'm a physicist, so I will shut up, or I may
23 bore you to death, or go into sci fi, which may not,
24 but --

25 (Laughter.)

1 CHAIR RAGGI: Any other questions?

2 (No response.)

3 CHAIR RAGGI: All right.

4 MR. HALL: Thank you.

5 CHAIR RAGGI: We want to thank you very much
6 for coming. Since you mentioned that you were going
7 to have to leave, let me say this for your benefit and
8 that of others.

9 MR. HALL: Sure.

10 CHAIR RAGGI: We have two public hearings
11 scheduled on this rule, today here in Washington and
12 then another one in January at Vanderbilt Law School.

13 We urged as many interested parties as possible to
14 give us your comments and to appear today rather than
15 to wait until January because we knew you would be
16 raising issues that we would want time to study.

17 I also asked the government not to respond
18 to each of you individually as your comments came in
19 but to respond once we had any of the thoughtful
20 criticisms about their proposal. What does this mean
21 going forward? The government if it files a response,
22 which I expect is likely, that will become public, and
23 some of you may wish to respond to that. I'm not
24 encouraging an endless debate, but you can certainly
25 do that. We would prefer actually if it were in

1 writing rather than to drag you back for the
2 Vanderbilt meeting.

3 So I just want you to know, if you're
4 wondering how we would like to proceed, that would be
5 our preferred course. Of course, if there's anyone we
6 didn't hear from who really wants to be heard, we'll
7 hear them, you know, in January. But the ideal would
8 be anything further you want to send us, send us in
9 writing, okay?

10 MR. HALL: Okay. Thank you very much.
11 Thank you, Your Honor. Thank you to the committee.

12 CHAIR RAGGI: Thank you very much. Thank
13 you.

14 Alan Butler from the Electronic Privacy
15 Information Center. Could we hear from you, Mr.
16 Butler?

17 MR. BUTLER: Good morning, Judge Raggi,
18 members of the Advisory Committee. Thank you for the
19 opportunity to participate at today's hearing. My
20 name is Alan Butler. I'm here on behalf of the
21 Electronic Privacy Information Center. EPIC is a
22 nonpartisan research center based in Washington, D.C.
23 which focuses public attention on important privacy
24 and civil liberties issues. One of our most important
25 goals is to ensure that Fourth Amendment rights are

1 not diluted as a result of the emergence and use of
2 new surveillance technologies. We support the maxim
3 articulated by Justice Sandra Day O'Connor in Arizona
4 v. Evans that with the benefits of more efficient law
5 enforcement mechanisms comes the burden of
6 corresponding constitutional responsibilities.

7 We appreciate the committee's important work
8 in maintaining the Federal Rules of Criminal Procedure
9 but are here today asking the committee to reject the
10 proposed amendments to Rule 41 because they would
11 expand the powers of law enforcement to
12 surreptitiously monitor private files without imposing
13 necessary procedural safeguards.

14 I'm going to talk just briefly on a few
15 points. My colleagues have covered many points today.

16 But most importantly, I'm going to talk about the
17 issues of necessity and prompt notice.

18 The proposed amendment would allow
19 officer -- I'm sorry. Courts have previously held
20 that covert entry or sneak-and-peek warrants, for
21 example, which share many similarities with the remote
22 access proposals here today, require several
23 conditions in order to be constitutionally firm.
24 Specifically, courts and Congress have required in
25 cases of surreptitious searches that there be a

1 reasonable necessity of not giving prior advance
2 notice and that notice be given within a reasonable
3 amount of time after the entry.

4 Specifically, the Ninth Circuit in Freitas
5 and the Second Circuit in Villegas adopted these
6 standards in regards to covert searches and applied
7 them, and there are not sort of countervailing Circuit
8 or Supreme Court opinions that have overturned these
9 notice requirements.

10 Congress subsequently authorized certain
11 delayed notice and surreptitious searches in the USA
12 Patriot Act and imposed similar requirements, again
13 finding that reasonable cause to believe that
14 providing immediate notification of the execution may
15 have an adverse result and also requiring that the
16 warrant not allow for the seizure of electronic files
17 or tangible property without a reasonable necessity
18 for such seizure.

19 Finally, Congress in that provision required
20 prompt notice, specifically within 30 days. So these
21 requirements that have been imposed by courts and by
22 Congress I think are founded on the principle adopted
23 by the Supreme Court in the Wilson v. Arkansas case
24 that notice is in fact a Fourth Amendment, a core or
25 procedural requirement of the Fourth Amendment.

1 The problem with the proposed rule is that
2 it provides specific rules about how and if notice
3 will be delivered without providing for requiring
4 notice within a given amount of time or prompt notice
5 and also without requiring the level of necessity that
6 I believe courts and Congress have previously imposed.

7 And I think this has come out in many of the sort of
8 questions and discussions here with regard, for
9 example, to the venue issue.

10 I think one question raised by the proposal
11 is sort of how necessary is it to proceed through
12 remote access when under let's say the first case
13 there has been some mechanism to conceal location.
14 And I think that just by way of an example, one thing
15 that the rule does not appear to require is that it
16 actually be necessary or reasonably necessary to
17 proceed through remote access. The rule simply
18 requires that some mechanism to conceal location have
19 been used.

20 So you could certainly imagine cases
21 where -- and my previous colleague mentioned a few --
22 where there is arguably some method used to conceal
23 location, but that would not preclude through
24 investigatory means the sort of uncovering of location
25 or reasonable venue, and it would not in that sense be

1 necessary to proceed through remote access if there is
2 some alternative mechanism.

3 So under the rule, the rule would
4 essentially allow -- would authorize the judge to
5 issue a warrant for remote access in that sense in a
6 case where remote access itself may not be necessary,
7 and there may be an alternative, a reasonable
8 alternative.

9 Similarly, the rule provides for requiring
10 law enforcement to make reasonable efforts to notify,
11 but it doesn't specify the timing of that potential
12 notification, and as my prior colleagues have
13 mentioned, it really under the rule could envision a
14 situation where there's ultimately no notice, no
15 actual notice given to the subject of the search.

16 So, in that case, I think the rule would
17 essentially allow for a warrant to be issued in a
18 circumstance that no court or Congress has ever
19 authorized, which is a potential no notice
20 circumstance, or a circumstance where the court would
21 not require that prompt notice be given.

22 And I think just to touch on a few points
23 that have been mentioned earlier, one question was
24 raised about, for example, the tracking warrant
25 provision in Rule 41, which I believe was actually

1 adopted or at least envisioned by Congress when it
2 enacted ECPA in 1986, which has a specific provision
3 that touches on that type of warrant.

4 So again, it's not uncommon for Congress, as
5 many of my colleagues have mentioned, for Congress to
6 act first in an area involving new techniques that are
7 sort of presented by new problems of either venue or
8 sort of technological means and then for courts again
9 to develop those congressionally authorized provisions
10 and for this committee to adopt rules consistent with
11 those decisions.

12 But what I believe is problematic about this
13 proposal is that the rules, the proposed rules to be
14 adopted would not incorporate existing constitutional
15 precedents and even sort of similar congressionally
16 authorized procedural protections that are necessary
17 when using the type of tool that we're talking about
18 here, remote access, essentially the digital
19 equivalent of a covert search or a sneak-and-peek.

20 Thank you.

21 CHAIR RAGGI: Yes. Professor King.

22 PROF. KING: Thank you. I have a question
23 about your points on the notice. If the rule were to
24 specify, as the tracking warrant provision does, that
25 such applications must comply with the Patriot Act

1 provision on notice, would that resolve your concerns
2 about the absence of the promptness, the 30-day, and
3 the reasonable necessity requirements that are in that
4 statute but you say are not in the existing language
5 of the proposed amendment?

6 MR. BUTLER: I think the adding of provision
7 that would require compliance with the prompt notice
8 requirement would certainly go a long way to improving
9 the proposal. I think that would certainly address
10 that portion of the issues at least that I've raised.

11 PROF. KING: Thank you.

12 CHAIR RAGGI: Any other questions?
13 Professor Kerr.

14 PROF. KERR: I was hoping you could say a
15 little bit more about the potential application of the
16 language concealed through technological means outside
17 of cases where the government truly does not know the
18 district in which the computer is located. And you
19 raised the possibility as I understood it that it may
20 be that, for example, a virtual private network is
21 used. The government actually could find out where
22 the computer is located but maybe doesn't want to or
23 something like that.

24 So I guess part of it is maybe just how you
25 read the phrase "concealed through technological

1 means." Do you interpret as being that there is at
2 some point a tool that's used to conceal, or do you
3 interpret that as being the government -- it has been
4 successfully concealed? I guess there's that
5 interpretive question.

6 MR. BUTLER: Right.

7 PROF. KERR: And to the extent you think the
8 language is broader than it needs to be -- this is a
9 question that was asked earlier of another speaker --
10 what's the narrower language that could then focus the
11 amendment just on the cases which are the ones that
12 clearly there is the broader concern of where the
13 government truly does not know in what district to
14 apply for the warrant.

15 MR. BUTLER: Sure. I think that part of the
16 issue with the language as it currently stands is that
17 the idea of concealing through technological means I
18 think is a definition that, as sort of my colleagues
19 who are technologists have mentioned, really can
20 describe many different situations. One you mentioned
21 is a VPN. You know, others might be certain types of,
22 you know, IP address spoofing or other sorts of
23 methods that might be used again to conceal but may
24 not, I guess to your point, fully conceal in the sense
25 that they may not actually preclude someone through

1 other investigative means from being able to discern
2 location or at least location within a venue, for
3 example. Like they may conceal your location, you
4 know, within a certain area or in a certain way but
5 not preclude the proper assertion of venue, for
6 example.

7 So I think it would be better to include the
8 language of necessity, I think, to address some of the
9 concerns here that as a result of the concealing it is
10 necessary to proceed through this other method. I
11 think that that really addresses some of what's been
12 raised today. Likely not all, but I think so.

13 PROF. BEALE: May I ask one more question?
14 So, as I understand it from your statement, various
15 Ninth Circuit precedents limiting warrants were then
16 later codified by Congress in the Patriot Act. Is
17 that right?

18 MR. BUTLER: So Congress -- it was certainly
19 discussed at the time that section 213 was adopted
20 that the rule would be consistent with established
21 precedents. I don't know that it directly -- I don't
22 believe it directly necessarily codified those rules,
23 but I believe that the rules -- and essentially as my
24 statement lays out, the rules are both consistent with
25 the view that necessity and prompt notice are required

1 when engaging in the type of delayed notice and
2 surreptitious search that --

3 PROF. BEALE: Well, and you understand what
4 we're trying to figure out is whether in all cases
5 Congress -- it's a chicken-and-egg problem, as I think
6 Judge Raggi said. So, on some of the cases that you
7 cited, it seems that the caselaw sets some precedents
8 and Congress came in. And in other cases it seems
9 like Congress came in first. And just trying to
10 understand your view of the relationship --

11 MR. BUTLER: Sure.

12 PROF. BEALE: -- and what precedents we
13 should be respecting and trying to understand in this
14 area. Thank you.

15 MR. BUTLER: Sure, yeah. And I think on
16 that same point, one thing that's sort of been a trend
17 in the questions and discussions today is the issue of
18 sort of partially who acts first and, you know, what
19 authority is necessary. And the role I think of the
20 committee that you're properly concerned about in sort
21 of how to set the rules and where the rules come from,
22 I think that just to use a surreptitious search
23 example, I mean, that was a situation where judges
24 authorized -- issued warrants for a particular type of
25 search, and that issue, you know, was litigated

1 through the normal process. And as a result of that,
2 I think later Congress was able to come back and
3 really describe in a more full way what the
4 constitutional requirements are.

5 And I think one concern about adopting a
6 rule that's as specific as the one -- as focused as
7 this rule is without including those procedural
8 protections that I outlined is that it may later be
9 the basis for a court to rule that any challenge to a
10 search conducted under this type of warrant is not
11 going to result in any Fourth Amendment relief. For
12 example, looking, as my colleagues have mentioned
13 earlier, at the good faith exception.

14 So I think in that way it could actually
15 inhibit any further development of Fourth Amendment
16 law with regards to remote access searches.

17 PROF. BEALE: And that brings me to the
18 delayed notice provision, the existing delayed notice
19 provision in Rule 41(f)(3) where it says, "Upon the
20 government's request, a magistrate judge may delay any
21 notice required by this rule if the delay is
22 authorized by statute." That would already be
23 applicable to this rule if it were adopted.

24 So unless statutory law authorizes a delayed
25 notice, then the notice would have to be given

1 promptly, as otherwise required by the rule. Does
2 that kind of intermesh between the existing statutory
3 provisions that only under limited circumstances
4 authorize a delay in providing the notice and the
5 existing rule, which then, you know, sort of clasps
6 hands with that and says you've got to do it promptly?

7 MR. BUTLER: Right.

8 PROF. BEALE: I don't actually understand
9 why that doesn't respond to your concerns if you, you
10 know, look at that part of the rule.

11 MR. BUTLER: Sure. I think that part of the
12 problem is again that the rule provides specific
13 language addressing notice without sort of directly
14 referring to or mentioning the prompt notice
15 requirement. So I think the additional delay of
16 notice being authorized in the way that you describe
17 is allowed under the statutory provisions as the rule
18 references but that the proposed amendment would sort
19 of create an alternative regime for notice.

20 PROF. BEALE: A little dissonance between
21 those two in a sense.

22 MR. BUTLER: Right. Exactly.

23 PROF. BEALE: You sense that, okay. That's
24 helpful.

25 CHAIR RAGGI: Thank you.

1 MR. BUTLER: Thank you.

2 MR. BITKOWER: One more question.

3 CHAIR RAGGI: Oh, I'm sorry. Mr. Bitkower.

4 MR. BITKOWER: I'd just like to follow up a
5 little bit on the discussion of necessity that you
6 outline. If we imagine a situation where law
7 enforcement has established the probable cause
8 requirements and the particularity requirements to
9 apply for a warrant for information contained on a
10 computer in a particular location in a particular
11 residence, for example, is there a reason why we
12 should prefer that that search be conducted physically
13 through an intrusion into the house versus remotely
14 through remote search of one kind or another, and what
15 are the considerations we should use in preferring one
16 or the other type of entry?

17 MR. BUTLER: Sure. So I think that the main
18 issue is that absent a reasonable necessity, I think
19 that the individual who's being searched should have
20 an opportunity, sort of a presentment and challenge
21 opportunity that you might have or at least an
22 opportunity to be present that you might have in a
23 physical search, for example, absent reasonable
24 necessity or with a, you know, more formal process
25 served on them in advance. I mean, I think that the

1 default should always be notice and process in advance
2 absent some reasonable necessity for the alternative.

3 MR. BITKOWER: Well, but my question relates
4 to the execution of a search warrant, which doesn't
5 usually involve an opportunity to litigate beforehand
6 whether the search is reasonable or should be done.
7 It involves usually officers presenting a warrant and
8 proceeding into the residence without a further
9 opportunity to challenge.

10 MR. BUTLER: Right.

11 MR. BITKOWER: So my question is between
12 that option of officers or agents effectively invading
13 a house to locate the computer in the upstairs bedroom
14 versus being able to access it remotely, is there a
15 reason we should prefer one or the other, and why does
16 your question I guess presuppose that we should prefer
17 the physical invasion to the electronic invasion?

18 MR. BUTLER: I guess my answer is that it
19 presupposes that we prefer advanced notice to delayed
20 notice, and that's the main reason, is that under the
21 first scenario you described you would actually have
22 notice at the time or before the search is executed,
23 whereas in the remote access situation you would have
24 either delayed notice or potentially no notice.

25 CHAIR RAGGI: Anything else?

1 (No response.)

2 CHAIR RAGGI: Thank you very much. We
3 appreciate your time.

4 MR. BUTLER: Thank you.

5 CHAIR RAGGI: May I just -- I'd like to take
6 a brief break, but I'd like to know how many more
7 witnesses are actually here. Amie Stepanovich, yes,
8 you're going to be next. Ahmed Ghappour was -- ah,
9 you are here, good. I knew you were encountering some
10 problems in transit. And Robert Anello?

11 MR. ANELLO: Yes.

12 CHAIR RAGGI: Ah, good. All right. So why
13 don't we take 10 minutes. And I'd like to keep us on
14 time, and we'll get started again.

15 (Whereupon, a brief recess was taken.)

16 CHAIR RAGGI: Amie Stepanovich, thank you
17 for coming, and we will be happy to hear from you.

18 MS. STEPANOVICH: Thank you.

19 CHAIR RAGGI: From the Access and the
20 Electronic Frontier Foundation, correct?

21 MS. STEPANOVICH: Yes.

22 CHAIR RAGGI: Thank you.

23 MS. STEPANOVICH: Thank you to all the
24 members of the committee both for being here today and
25 for listening to all of us testify but also for your

1 incredible level of engagement throughout every single
2 testimony. I really appreciate how involved you are
3 in what we consider to be a very important issue.

4 My name is Amie Stepanovich.

5 CHAIR RAGGI: We feel the same way.

6 MS. STEPANOVICH: Thank you. My name is
7 Amie Stepanovich. I am senior policy counsel with
8 Access, which is a global digital rights organization.
9 We were founded in 2009 in the wake of the Iranian
10 election and the problems that resulted from that.
11 And we work from a technological angle as well as a
12 policy and an advocacy angle. And members of our tech
13 team have informed my testimony, which was also
14 informed by hiring individuals at the Electronic
15 Frontier Foundation, on whom I am also testifying on
16 behalf of. EFF was founded in 1990 and champions
17 privacy, free expression, and innovation.

18 My testimony today is going to be incredibly
19 narrow and very brief. I want to more or less stick
20 to my written remarks but emphasizing just a few
21 points that I think bear to be emphasized.
22 Specifically, I will be talking today about the rule
23 change that involves the issuance of warrants for
24 computers infected by botnets.

25 My first emphasis is that this rule change

1 is substantive. It is going to have a profound impact
2 on privacy rights of individuals around the world, and
3 it's going to have this impact during a time when
4 there is a global conversation happening about the
5 appropriate extent of government surveillance. This
6 will actually be extending unilaterally the
7 surveillance that the government can engage in.

8 As discussed in the relevant committee note,
9 this change involves the creation and control of
10 botnets. Today I will provide to the committee some
11 technical background on botnets, the unique nature of
12 botnets that would cause the rule to have an overbroad
13 and substantive impact on computing, and how DOJ's
14 interpretation of the Computer Fraud and Abuse Act, or
15 the CFAA, is going to compound these impacts. I will
16 end discussing how the proposed change is going to
17 cause more harm than good in practice.

18 Botnets are robot networks. This is what
19 botnet is short for. A botnet is a network of
20 computers that have been linked together through the
21 insertion of malware, which is a bad computer program,
22 and it links these network of computers to a command
23 and control center where they can be remotely accessed
24 and used, typically for malicious purposes. A lot of
25 times botnets are used, for example, to engage in

1 denial of service attacks, which is basically the
2 equivalent of shutting down websites. And many
3 government and private websites we have heard over the
4 past many years have been impacted by denial of
5 service attacks.

6 So I'd like to say that we recognize that
7 the investigation of botnets is a real problem, and we
8 definitely empathize with the government as they try
9 to investigate and control and shut down incredibly
10 problematic botnets.

11 Botnets can be anywhere from a few hundred
12 computers to many millions. One of the largest
13 botnets known to have existed, the Conficker botnet,
14 was somewhere between 9 million and 15 million
15 computers located all around the world. It was
16 incredibly large. But it means that this rule is
17 going to have an incredibly large impact because it
18 would allow searches of anywhere from 9 million to
19 15 million computers that are involved in this botnet.

20 Botnet malware, once it's on a computer, can
21 sit stagnant for years without causing any harm,
22 without causing the computer to take any action. The
23 Conficker botnet I just referenced actually was not
24 used or was largely not used. Only one brand of it
25 was ever thought to have taken any action. So this is

1 15 million potentially computers infected with
2 malware, part of a botnet that didn't ever do
3 anything, which is interesting from the perspective
4 that this malware may never be found by the user of
5 the computer. They may not know it's there. They may
6 never have the chance to know that it's there.

7 Finally, not all networked computers are
8 malicious or unlawful. So there are botnet-like
9 networks that would be encompassed by this rule that
10 have legitimate purposes. For example, there is one
11 that I will call to mind that I will bring to you that
12 allows users to devote their spare computing power to
13 searching for life in outer space. They can donate
14 the time that they are not using their computer to let
15 that computing power be sent out into space to see if
16 there's any activity that can be picked up.

17 This is much like a botnet. It's command
18 and control. It's remote access. But it is not
19 necessarily unlawful by any means. And this is just
20 the beginning. There are many lawful systems like
21 this.

22 On account of the distributed nature,
23 investigations of unlawful botnets undoubtedly pose a
24 significant barrier to law enforcement. However, we
25 urge the rejection of the proposed amendment to Rule

1 41 in favor of pursuit of a statutory solution
2 promulgated democratically in open, public, and
3 accountable legislative process.

4 A little bit about the CFAA so I can give
5 you background on a law that many of you may not be
6 familiar with. It was initially passed in 1986. It's
7 traditionally used to prosecute the theft of private
8 data or damage to systems by way of malicious hacking.

9 The CFAA was designed to provide justice for victims
10 of these activities by offering a remedy against
11 perpetrators. The plain text of the relevant section
12 of the CFAA clearly focuses on knowing or intentional
13 malicious activity.

14 Using this authority, magistrate judges
15 issue warrants against those who create and use
16 unlawful botnets, controlling the infected computers
17 of otherwise innocent users. However, the proposed
18 procedural amendment unilaterally expands these
19 investigations to further encompass the devices of the
20 victims themselves, those who have already suffered
21 injury and are most at risk by the further utilization
22 of the botnet and, as noted, since a single botnet can
23 include millions or tens of millions of victims'
24 computers which may not only be located around the
25 United States but around the world.

1 Victims of botnets include journalists,
2 dissidents, whistleblowers, members of the military,
3 lawmakers, world leaders, members of other protected
4 classes, and potentially members of this committee.
5 Each of these users and any other user subject to
6 search or seizure under the proposed amendment has
7 inherent rights and protections under the United
8 States Constitution, the International Covenant on
9 Civil and Political Rights, and/or other well-
10 established international law.

11 Without reference to or regard for these
12 rights and protections, the proposed change would
13 subject any number of these users to state access of
14 their personal data on the ruling of any district
15 magistrate. This is a substantive expansion of the
16 CFAA.

17 Further complicating matters, the proposed
18 change considered here today will have ramifications
19 for the large number of users who are not part of a
20 botnet. These users may be tangentially connected to
21 a botnet through any number of means, such as the use
22 of a common shared server or provider. I will draw
23 your attention to one case, the case of Microsoft and
24 No-IP. This was a civil case, but it is telling for
25 how this will be used in a criminal context.

1 Microsoft had applied to a federal judge for
2 a court order to assist in dismantling a pair of
3 botnets, two botnets that encompassed a total of
4 18,000 computers. In implementing the court order,
5 they actually led to the disruption of service for
6 nearly 5 million legitimate websites or devices of
7 1,800,000 nontargeted users. So this is taking
8 something that was supposed to be used for 18,000
9 users and expanding it by a factor of 100 and actually
10 impacting 1,800,000 users.

11 The above problems are exacerbated by the
12 overbroad interpretations of the CFAA itself. The
13 Department of Justice has continually expanded the
14 CFAA to the point where it's now used for many
15 instances in which it was not anticipated to be used
16 when it was passed, and we believe this procedural
17 rule further cements a further expansion of the CFAA
18 that we don't believe is in the law itself.

19 And then the proposed amendment in practice,
20 this actually could bring an enormous number of
21 computers belonging to innocent users under the
22 purview of the CFAA and subject them to law
23 enforcement surveillance. It is likely that law
24 enforcement can cause more harm to these users than
25 good when it seeks to investigate botnets. The range

1 of cybersecurity measures available to law enforcement
2 vary immensely, and it's arguable at what extent law
3 enforcement should be able to engage in government-
4 sponsored hacking. But I think the one thing that
5 everybody agrees to is that if they're able to engage
6 in this activity, it should be under the purview of
7 Congress and not necessarily unilaterally allowed
8 either by procedure or by other activity.

9 So, to wrap up in my last 55 seconds, this
10 is a substantive amendment. It is not procedural at
11 least in the case of the CFAA and this particular
12 provision. So I urge you to reject it and to turn to
13 Congress for an expansion of the CFAA if this is
14 activity that the Department of Justice and law
15 enforcement would like to engage in investigating.

16 CHAIR RAGGI: Thank you. I think we have a
17 number of questions. Professor King?

18 PROF. KING: I just have one question. The
19 CFAA says it's not speaking to -- it doesn't prohibit
20 any authorized investigative or law enforcement
21 activity. It defines a crime. It doesn't regulate
22 investigations. So why is it that you're saying --

23 MS. STEPANOVICH: We believe that the
24 provisions of the CFAA in [18 U.S.C. § 1030](a)(5) are
25 anticipated to allow primarily computer-to-computer

1 crimes, and in some cases, they could allow botnet
2 investigations. But the fact that this rule is
3 allowing investigations under the CFAA to encompass
4 millions of computers of victims and not people who
5 are perpetrating crimes, we don't think that that was
6 anticipated when the CFAA was passed, similar to many
7 other crimes that are currently being investigated and
8 prosecuted under the CFAA. And if they want to engage
9 in this activity, they have to go back and get
10 additional authority under statute.

11 CHAIR RAGGI: What part of the rule do you
12 think creates the concern you've just identified? I
13 ask this because, as others have said earlier today,
14 we are trying to tell people what courthouse they have
15 to go to. We are not in any way limiting the
16 government or relieving it from its obligations to
17 satisfy the probable cause particularity requirements
18 of the Fourth Amendment. So what is it in the text of
19 the rule that was put out for comment that you think
20 raises the concern you've identified?

21 MS. STEPANOVICH: So the fact that the rule
22 allows for the search and seizure of victims' devices,
23 specifically of the computers that have been harmed by
24 botnets, we would raise attention to. We also believe
25 that there is a problem with the fact that there is a

1 odd drafting construction that seems to prevent
2 magistrates from issuing these multijurisdictional
3 warrants if any member of the botnet is located within
4 their jurisdiction. That might not be intended, but
5 the language is ambiguous on that point.

6 However, by allowing the investigations into
7 the victims' computers, it is something that we don't
8 believe was anticipated by the CFAA. So we think that
9 turning to venue is premature before the substantive
10 allowance for these investigations has been granted.

11 PROF. BEALE: This may be the same question,
12 but --

13 CHAIR RAGGI: Professor Beale.

14 PROF. BEALE: -- does it affect your view
15 that a warrant cannot be issued now and couldn't be
16 issued in the future without probable cause? So there
17 would have to be probable cause for the search of any
18 computer, the victim's computer, the anticipated
19 perpetrator's computer, so probable cause to believe
20 that evidence of a crime could be obtained there.

21 And right now the government if it can show
22 probable cause for a botnet investigation could go to
23 1, 2, 10, 94 districts and either get or not get these
24 warrants for the victim computers depending on whether
25 they can show probable cause.

1 MS. STEPANOVICH: Uh-huh.

2 PROF. BEALE: Right? So they can do that.
3 We understand that they can do that right now. And
4 the question is, is there probable cause or not. All
5 this does is say you don't have to do it 94 times.

6 MS. STEPANOVICH: Uh-huh.

7 PROF. BEALE: If we focus on that question,
8 then what would make it preferable from your point of
9 view that the same action be taken, the same
10 information be provided, 94 judges having to look at
11 it, 94 prosecutors having to do this, if there is a
12 serious botnet investigation? So you understand that
13 that's -- the efficiency argument was made by the
14 government that this would be a good idea. If it
15 could get a warrant, in this particular type of
16 investigation, it should just be able to go to one
17 place. Why is that not a good idea?

18 MS. STEPANOVICH: So I believe many of my
19 colleagues have spoken to this. I will emphasize the
20 Microsoft case that I brought up in addition because
21 there is actually a problem with following through in
22 these investigations. A probable cause showing
23 relevant to one or any number, 94 computers, could
24 actually have ramifications for many computers more
25 than that that are not part of the botnet, just in how

1 the warrant and how the search is carried out.

2 So, if you see the Microsoft case, they had
3 probable cause. They had reason to believe that there
4 were 18,000 computers that were part of a botnet. But
5 in carrying out that investigation, because of the
6 unique nature of investigations into botnets and how
7 botnets function, they actually ended up shutting down
8 service for, as I said, many numbers of magnitude
9 beyond who were infected by the botnet itself, so --

10 PROF. BEALE: So that's a policy argument
11 that Microsoft shouldn't have done that. The
12 government shouldn't do this. You said this is
13 substantive, right? It's substantive, and so it's
14 improper for the committee to do this. But I'm still
15 not understanding why having to go one courthouse as
16 opposed to 94 different courthouses is substantive,
17 and I think I might be missing part of your argument.

18 MS. STEPANOVICH: I believe that when you go
19 to one courthouse you actually exacerbate the harm
20 allowed under the statute and you end up having a
21 substantive impact on users who would not otherwise be
22 impacted by the search or by the seizure. So, when
23 you go to 94 different courthouses and you're
24 conducting 94 separate searches, it is a different
25 animal than when you're going to one courthouse.

1 You're getting a search warrant for 94 computers and
2 executing it in a way that could have far-flung
3 impact, well beyond what is anticipated by the search
4 warrant.

5 CHAIR RAGGI: Professor Kerr, you had a
6 question?

7 PROF. KERR: So my question is a little bit
8 of technology and a little bit of law, and it goes to
9 imagine the government is investigating a botnet case,
10 and for a variety of reasons they need to get a sense
11 of the scale of the network. Maybe they need to
12 prove, you know, 10 or more computers to get to a
13 felony enhancement. Maybe it's a sentencing issue and
14 they need to show overall loss. And they want to
15 somehow query the network in order just to get a sense
16 of the number of computers that are part of the
17 botnet.

18 So it's a little bit of technology, a little
19 bit of law. The question is do you have a sense of
20 how the government can find that out without somehow
21 sending a query to the network or to the computers
22 connected to the network, and then do you think they
23 can do that without a warrant? Is a warrant required
24 for that? That's where the legal part comes together.

25 MS. STEPANOVICH: Uh-huh.

1 PROF. KERR: And I guess the question is
2 really of putting yourselves in the shoes of the
3 investigators that have to try to figure out the scale
4 of the network. Is there under current law in your
5 view a problem where they really could not find out
6 the scale of the network under the current
7 authorities, or is that something that they can figure
8 out now without any need to amend Rule 41?

9 MS. STEPANOVICH: I don't believe that they
10 could do that without infringing on the computers
11 themselves, without doing what we are calling
12 government-sponsored hacking, basically sending out
13 some sort of device, beacon, tool, and inserting it
14 onto the computer. Now again, I am not a tech -- as
15 my colleagues are not lawyers, I am not a
16 technologist, and I would have to consult with our
17 tech team in order to 100 percent verify that, but I
18 believe that that would be necessary in order to
19 determine the size or scope of the botnet.

20 I do not believe that that is allowed under
21 current law, which is why we think that this is
22 substantive. I think that in order to be able to do
23 that that a legislative change is necessary. And I
24 empathize that it is very hard to get a legislative
25 change. We've been trying to update the law, as you

1 well know, by which law enforcement accesses email for
2 any number of years, have more than the majority of
3 the House of Representatives ready to support it and
4 can't get a vote. So I know it's hard to get
5 legislative change. However, when you have us
6 resorting to Congress to get increasing privacy
7 protections, we would also like to see the government
8 turning to Congress to get increasing surveillance
9 authority as well.

10 CHAIR RAGGI: I think Judge Lawson.

11 JUDGE LAWSON: Good morning.

12 MS. STEPANOVICH: Good morning.

13 JUDGE LAWSON: Could you -- do you have the
14 language of the proposed amendment handy?

15 MS. STEPANOVICH: I do not.

16 JUDGE LAWSON: Well, my question is you made
17 a statement that you believe that the amendment would
18 authorize the search of a victim's device. And I'm
19 wondering if you could point to that language --

20 MS. STEPANOVICH: Uh-huh.

21 JUDGE LAWSON: -- because I suggest to you
22 that the idea was not intended to authorize the search
23 of anything. It was merely to provide a procedure to
24 engage.

25 MS. STEPANOVICH: Uh-huh.

1 JUDGE LAWSON: So maybe that's a drafting
2 issue we need to address. So this is a lawyer
3 question, not a technology question. Could you tell
4 me what you had in mind?

5 MS. STEPANOVICH: So specifically, it's the
6 line -- it says -- part B, "Is an investigation of a
7 violation of 18 USC 1030(a)(5)," which is the CFAA.

8 JUDGE LAWSON: Right.

9 MS. STEPANOVICH: "The media, the media to
10 be searched, are" --

11 JUDGE LAWSON: No, it doesn't say "media to
12 be searched." It says the media. The media are
13 protected computers.

14 MS. STEPANOVICH: Yes.

15 JUDGE LAWSON: So that --

16 MS. STEPANOVICH: The part 6, which leads
17 into part B, is talking about when you can search or
18 seize a computer, when you can search or seize
19 electronic media, and you can conduct a search or
20 seizure of electronic media --

21 JUDGE LAWSON: Now are you referring to the
22 Computer Fraud and Abuse Act, or are you referring to
23 the language of the --

24 MS. STEPANOVICH: The language of the rule
25 itself. If you read it in its entirety, when you read

1 part 6 flowing into subpart B, it is authorizing a
2 search or seizure of media that are protected
3 computers that have been damaged without authorization
4 or are located in five or more districts.

5 JUDGE LAWSON: All right. I think I part
6 company with you there. I don't necessarily read
7 that -- I look at part B as triggering language as to
8 when a magistrate judge would be authorized to issue a
9 warrant, but that doesn't language doesn't
10 authorize -- doesn't suggest what can be searched and
11 must be seized. That's left to current Fourth
12 Amendment law. But you don't read it that way. You
13 read it as authorizing the search of media that might
14 be affected under -- a victim's media that might be
15 affected under the Computer Fraud and Abuse Act?

16 MS. STEPANOVICH: So I read it, a magistrate
17 judge with authority in any district where activities
18 related to a crime may have occurred has authority to
19 issue a warrant to use remote access to search
20 electronic storage media and to seize or copy
21 electronically stored information located within or
22 outside the district if -- barring the first part, the
23 media, which I believe references back to the use of
24 the word media in the prior section --

25 JUDGE LAWSON: Yeah.

1 MS. STEPANOVICH: -- are protected computers
2 that have been damaged without authorization.

3 CHAIR RAGGI: All right. We can take that
4 drafting into consideration.

5 JUDGE LAWSON: Good, good. All right.

6 CHAIR RAGGI: Mr. Bitkower?

7 JUDGE LAWSON: That's helpful. Thank you.

8 MR. BITKOWER: And if I can just follow up
9 on that question, though, so if we were to assume that
10 this provision only applies to venue, that is, this
11 provision would only apply in cases where there was
12 already probable cause to search particular victim
13 media, that is, this did not by itself give authority
14 absent a further showing of probable cause and
15 particularity to search a particular computer but only
16 invoked the venue provision, would that satisfy some
17 of your concerns about overbreadth?

18 MS. STEPANOVICH: As I had said before, I
19 don't believe that we are at a point where we can get
20 to the venue question yet. I think that first we have
21 to address by statute whether or not these searches
22 and seizures can occur, whether or not you can use the
23 CFAA in this way. And I think that requires
24 legislative change, and then the venue question has to
25 come after that.

1 MR. BITKOWER: So can I just -- I'm sorry.
2 If we assume that this provision only applied in cases
3 where under current law you could already search a
4 victim computer and took that current law and then
5 instead of requiring you to go to 94 judges only
6 required you to go to one judge, would that put to
7 rest the concerns about searching victim computers?

8 I understand you have concerns about forum
9 shopping, et cetera, but in terms of the concerns
10 about searching victim computers as opposed to, for
11 want of a better word, perpetrator computers, target
12 computers, if we assume that all the current law and
13 rules remained the same, would that concern go away?

14 MS. STEPANOVICH: I would say that current
15 caselaw specifically already overexpands the
16 provisions of the language of the CFAA to allow it to
17 be used in circumstances that it wasn't intended to be
18 used when it was drafted. If it was interpreted in a
19 way that only allowed it to be used in instances which
20 by the plain text of the CFAA were able to be
21 investigated, then that is one matter.

22 But I don't think under -- when you say
23 current law, I interpret that to mean both current law
24 under the statute and current caselaw. And I think
25 caselaw already overexpands what the CFAA should be

1 used for and that some of the instances are
2 inappropriate.

3 MR. BITKOWER: So understanding that there
4 may be disagreements about what the CFAA provides, I
5 guess the question I think we're trying to focus on
6 is, is there a drafting issue with the way the venue
7 provision here is drafted that could be corrected or
8 narrowed or qualified in some way, or is your quarrel
9 simply with what current law allows within a district?

10 MS. STEPANOVICH: I mean, personally I have
11 a quarrel with both. In this specific circumstance, I
12 would like to -- I mean, if it is a drafting error, as
13 it may be highlighted by other questions, I would like
14 to see a redraft and to see what you actually
15 intended. I believe that the language as it is allows
16 for an overexpansion of the CFAA, a continued
17 expansion of the CFAA. So here I am bringing issue
18 with the procedure.

19 As to your former question where you asked
20 if I would be comfortable if it was only allowed under
21 current law, I did just want to flag that under
22 current statutory law, yes. Under current caselaw, I
23 and Access would have issue.

24 CHAIR RAGGI: Mr. Filip, you had a question?

25 MR. FILIP: Yeah, I just want to clarify

1 this. Your organization and you believe that the CFAA
2 has been misinterpreted by the federal courts. Fair
3 enough, right? Maybe district judges sometimes think
4 that Circuit Courts got it wrong or circuit judges
5 think the Supreme Court got it wrong, but everybody
6 has to apply the law that the system has given us.

7 So independent of whether or not the CFAA
8 has been in the past interpreted consistent with the
9 organization's viewpoint or in the future will be
10 interpreted consistent with your aspirations, this is
11 a venue provision about where to go to file a warrant.

12 So is there anything about the venue provision that
13 will allow in the future you to litigate maybe as
14 amicus and defendants, all sorts of folks, to have
15 substantive debates about the precedent? And you can
16 go to Congress and try to get the law changed, all
17 sorts of things. Is there something about the venue
18 provision that you would offer that you think would
19 improve it?

20 MS. STEPANOVICH: Noting that I do believe
21 the CFAA has been overused and overexpanded, I don't
22 believe that any caselaw allows it to be used in this
23 way. So I believe that even if you incorporate all of
24 the cases that are out there and look at how it can be
25 used under current law and how judges have interpreted

1 it, that it is not able to even in its current state
2 be used in a way that would allow the investigations
3 that this rule anticipates.

4 MR. FILIP: Okay.

5 CHAIR RAGGI: Let me put the venue question
6 to you a little differently. At present, the general
7 venue statute, Rule 41, is that warrants are to be
8 sought in the location of the place where the search
9 is to be conducted. If we were to amend Rule 41 to
10 say searches can be conducted either at the location
11 of the premises to be -- they can be sought, the
12 warrant can be sought, either where the premises to be
13 searched is located or where the harmful effect of the
14 crime is being committed, for any warrant. Do you
15 have a problem with that, a constitutional problem
16 with that?

17 MS. STEPANOVICH: I would have the same
18 constitutional problems that many of my colleagues
19 have raised.

20 CHAIR RAGGI: I don't think anybody has
21 addressed that. I mean, that goes to whether or not
22 under the Fourth Amendment it would be reasonable to
23 allow warrants to be issued by judges who were located
24 in those two particular or more than two particular
25 districts, either where the premises to be searched is

1 located or where the crime is having its effect,
2 because effectively what this rule does is it does
3 that but only for a narrow category of cases. And so
4 I think you urge us to start with the CFAA. I'm
5 urging you to think instead the other way, that what
6 problem is there with expanding the venue for
7 warrants.

8 MS. STEPANOVICH: I believe by using it for
9 a specific circumstance -- and I would have to go back
10 and think a little bit harder about the broader
11 provision, but by incorporating the CFAA specifically
12 into the rule by reference, that it inherently
13 authorizes certain activities under the CFAA that are
14 not otherwise allowed and that happen specifically by
15 referencing that provision. If it was a broader
16 provision, then there would likely be many issues with
17 it being used in certain circumstances that could be
18 addressed by the courts. And again, I would have to
19 try to go back and spend some time musing upon how
20 that language could be used.

21 CHAIR RAGGI: Well, now let's go to your
22 point, that by referencing the CFAA -- it could
23 reference any statute. It could reference Title 21,
24 the drug crimes. It could reference any of a number.
25 It chose the CFAA.

1 MS. STEPANOVICH: Uh-huh.

2 CHAIR RAGGI: It doesn't say anything about
3 how the CFAA should be construed. So presumably it's
4 to be construed lawfully, and there can be debates
5 about that. Given that all it does is reference a
6 statute, not how that statute should be interpreted,
7 what's the problem? Help me out.

8 MS. STEPANOVICH: So I -- gathering my
9 thoughts.

10 CHAIR RAGGI: Please, take your time.

11 MS. STEPANOVICH: I believe it allows -- in
12 the universe of what the CFAA allows and the universe
13 of what could be searched under the statute, I believe
14 they are nonoverlapping bubbles based on the expansive
15 language of the statute, based on its invocation of a
16 large number of victims' computers. And so perhaps a
17 rule -- a drafting change --

18 CHAIR RAGGI: But only if there's probable
19 cause. You understand that. No computer can be
20 searched without probable cause. So again, I'm having
21 difficulty understanding what the problem is if
22 there's a authority to expand venue -- these are all
23 hypotheticals -- if there's authority to expand venue,
24 if the statute only references the CFAA, not how it
25 should be interpreted, and it demands probable cause.

1 MS. STEPANOVICH: I would have to go back
2 and bring an answer to you.

3 CHAIR RAGGI: All right. Thank you very
4 much. I didn't mean by any means to fluster you. We
5 are genuinely trying to understand where the problems
6 may lurk in this rule amendment and to make sure that
7 we're sensitive to them. So I do thank you very much.

8 MS. STEPANOVICH: And I do believe there are
9 unique circumstances raised by this specific factual
10 scenario that you are trying to address that by
11 incorporating this provision raise unique issues that
12 may not be raised in other cases.

13 CHAIR RAGGI: Thank you. Thank you.
14 Any other questions?

15 (No response.)

16 CHAIR RAGGI: All right. Thank you. We
17 will hear next from Ahmed Ghappour. And I hope I
18 pronounced your name correctly, Professor.

19 MR. GHAPPOUR: You pronounced it perfectly.
20 Thank you.

21 CHAIR RAGGI: Good. Thank you.

22 MR. GHAPPOUR: Hi. Good morning. Thanks
23 again for the opportunity to address the committee
24 today. I'll be very brief. My name is Ahmed
25 Ghappour. I'm a visiting professor at the University

1 of California, Hastings College of the Law. I teach a
2 clinic on security and technology, and we litigate
3 constitutional issues that arise in the context of
4 cybersecurity and national security cases.

5 Very briefly, I wish to touch upon some of
6 the issues that relate to the extraterritorial aspect
7 that the venue provision will raise. Now the DOJ has
8 explicitly stated that the amendment is not meant to
9 give courts the power to issue warrants that authorize
10 searches in foreign countries. But the practical
11 reality of the underlying technology means that doing
12 so will be unavoidable.

13 So the problem is that we don't have a
14 technical ability to tether our operational capacity
15 to the requirements of the law. And specifically,
16 that means that it doesn't seem possible to keep the
17 venue rule while limiting the investigation to the 94
18 judicial districts of the United States.

19 To my knowledge, therefore, this would be
20 the first time U.S. law enforcement would on a regular
21 basis encroach on the sovereignty of foreign nations
22 as a matter of course in the pursuit of general crimes
23 as opposed to national security crimes with what
24 appears to be judicial approval.

25 Now, in terms of the substantive expansion

1 that this will cause, first the FBI currently lacks
2 clear authority to unilaterally violate the
3 sovereignty of other nations. While the FBI's
4 extraterritorial activities are nothing new -- and
5 indeed their responsibilities date back to the mid-
6 1980s when Congress first passed laws authorizing the
7 FBI to exercise federal jurisdiction overseas when a
8 U.S. national was murdered or assaulted or taken
9 hostage by terrorists.

10 However, the extraterritorial activities
11 have generally fallen in line with customary
12 international law. Under international law, it is
13 considered an invasion of sovereignty for one country
14 to carry out law enforcement activities within another
15 country without that country's consent. And to that
16 end, the FBI avoids acting unilaterally, relying
17 instead on U.S. diplomatic relations with other
18 countries and the applicability of any treaties,
19 seeking permission from the host country where
20 necessary and requesting assistance from the local
21 authorities whenever possible. I believe these issues
22 were addressed in detail in the prior testimony.

23 One exception, of course, might be the
24 abduction of fugitives that are residing in a foreign
25 state when those actions would be contrary to

1 customary international law. That is, we would go in
2 and seize someone in violation of a particular host
3 state's sovereignty. But in those cases, typically
4 diplomatic efforts are first made and denied by that
5 foreign host country.

6 Here, unilateral state action will be the
7 rule and not the exception in the event that any
8 anonymous target proves to be outside of the United
9 States. And the reason is simple. Without knowing
10 the location of a target before the fact, there is no
11 way to provide notice or obtain consent from a host
12 country until after its sovereignty has been
13 encroached.

14 So not only is this a substantive expansion,
15 but as a matter of policy, it puts the United States
16 in a position where law enforcement encroaches on
17 territorial sovereignty without any coordination with
18 the agency in charge of our foreign relations, that
19 is, the State Department.

20 So, without advance knowledge of the host
21 country, there is no way to adequately avail yourself
22 of the protocols currently in place to facilitate
23 foreign relations, to coordinate with the Department
24 of State, to coordinate with the CIA for that matter,
25 to make sure that your network investigative technique

1 is not encroaching upon their investigative
2 activities.

3 So, second, the judiciary lacks power to
4 authorize overseas searches that constitute unilateral
5 encroachments of foreign sovereignty. I think we're
6 all in agreement about that, but while the warrants
7 issued under the rule may not have any specific legal
8 significance in as far as extraterritorial activities
9 are concerned, it may nonetheless pose a security risk
10 to our judiciary. And I'll get to that in a second.

11 Well, let me just get to that right now. It
12 would pose a security risk to our judiciary, our
13 federal agents, and our prosecutors. And I think this
14 is the biggest policy concern in my eyes, and that is
15 when a state sovereignty is encroached upon, its
16 response depends on the nature and the intensity of
17 the encroachment.

18 In the context of cyberspace, states,
19 including the United States, have asserted sovereignty
20 over cyberinfrastructure, and despite the fact that
21 cyberspace as a whole is a global common, states do
22 find that once you come into their territory you are
23 in violation of sovereignty. And to be sure, this is
24 not to say that the FBI's current arsenal of network
25 investigative techniques are equivocal to acts of war,

1 to cyber armed attacks, as would be defined by Article
2 51 of the U.N. Charter, for which the use of cyber
3 kinetic force and response might be permissible, but I
4 do note that technology is expanding ever so swiftly.

5 But what these activities do constitute is
6 cyberespionage, clandestine information-gathering by
7 one state from the territory of the other at least
8 from the perspective of the invaded state. That's how
9 they might choose to see this, and that is how they
10 would likely see this. And as a general matter, while
11 there are no prohibitions on cyberespionage in
12 international law, law enforcement hacking will
13 probably be regulated by the violated states' domestic
14 criminal law, counter-espionage, other counter-
15 measures.

16 Given the public nature of the U.S. criminal
17 justice system, it's hard to see how our agents,
18 prosecutors, and judiciary would avoid the prosecution
19 in foreign countries. The reason is that the
20 encroachments that result will be public, whether
21 arising in a criminal trial, an indictment, a publicly
22 issued opinion such as that of Magistrate Smith.

23 And on this point, I think an incident back
24 in 2002 is very instructive. In 2002, Russia's
25 federal security service filed criminal charges

1 against an FBI agent for illegally accessing servers
2 in Russia. The purpose of accessing those servers was
3 to seize evidence against hackers and that evidence
4 was later used in a criminal trial. The FSB, which is
5 the security service, was tipped off to the fact when
6 the defendants were indicted in Seattle, Washington.

7 Reportedly, this was the first ever FBI case
8 to utilize the technique of extraterritorial seizure
9 of digital evidence. Notably, in this case, the
10 access was through the web using log-in information
11 that was obtained consensually from the perpetrators.

12 So that is to say that the level of powers that we're
13 seeking here are much broader than that that was
14 implemented in the Seattle example, in the Russia
15 example.

16 Fourth, the judicial process is not going to
17 be a remedy for this extraterritorial aspect. And the
18 caselaw is clear that violations of international law
19 have very limited application to Fourth Amendment law,
20 if any.

21 And so I have a number of very quick
22 recommendations. Please feel free to intervene. In
23 light of the above, I would be very hesitant to amend
24 Rule 41 at this time without having a thorough
25 discussion of the potentially far-reaching

1 consequences of the change. The technologies involved
2 are rapidly developing and poorly understood, as are
3 the existing international legal norms, including the
4 United States' position within them.

5 It's critical then that these issues be
6 approached with comprehensive deliberation. This is
7 particularly the case when we've got similar issues
8 making their way not only through the judicial
9 process, as we've heard by reference to the Microsoft
10 case, but also in the foreign affairs context and in
11 the legislative context.

12 A new bill, called the Law Enforcement
13 Access to Data Stored Abroad Act, LEADS, aims to amend
14 the ECPA to authorize the use of search warrants
15 extraterritorially only when the communications belong
16 to a U.S. citizen, LPA, or a company incorporated in
17 the U.S., or when there is no requirement that the
18 communications provider or remote computing service
19 violate the laws of a foreign country. So that's a
20 bill that's taking into account the sovereignty of
21 another nation.

22 I would also mention that Judge Preska,
23 who's the District Court judge in the Microsoft case,
24 did in her oral opinion in that case reference and
25 give mention to the fact that she did not believe that

1 Ireland's sovereignty was violated by the subpoena,
2 which is a very different case than here.

3 Now I would also note that these authorities
4 are much broader than Microsoft, as we've said.
5 However, if we do amend the rule, we should certainly
6 takes steps to minimize the encroachments on other
7 states' sovereignty, leaving open the possibility for
8 diplomatic overtures. And to that end, the rule
9 should require network investigative techniques to
10 return only country information at first, prompting
11 the executing FBI agent to utilize the appropriate
12 protocols and institutional devices. This basically
13 puts us back at the position we would have been if we
14 knew where the computer was. We can utilize MLAT
15 procedures and so on.

16 The rule should also ensure that network
17 investigative techniques are used sparingly and only
18 when necessary by requiring a showing similar to that
19 required by ECPA, specifically that less intrusive
20 investigative methods have failed or are reasonably
21 unlikely to succeed. And that is by reference section
22 2518(1)(c).

23 Another way to do this might be to narrow
24 the class of potential targets from targets whose
25 location is concealed through technological means to

1 those whose location is not reasonably ascertainable
2 by less invasive means. The rule should also limit
3 the range of hacking capabilities it authorizes.
4 Remote access should be limited to the use of
5 constitutionally permissible methods of law
6 enforcement trickery, deception that result in target
7 initiated-access.

8 In other words, in the Seattle-Russia
9 example, we actually lured the hackers over into
10 Seattle, created a shell company, and had them type in
11 their password. So that component of the remote
12 search was governed by deception. The next thing they
13 did in that case was they actually went through the
14 MLAT process or went through the bilateral process.
15 And Russia said no. They said, you can't have access
16 to these computers. And so we went ahead and did
17 anyway.

18 CHAIR RAGGI: So you are well past your
19 time. Are you close to wrapping up?

20 MR. GHAPPOUR: I am actually -- there are
21 other suggestions, of course, but I'll just refrain.

22 CHAIR RAGGI: Okay. You didn't submit
23 anything in writing, correct?

24 MR. GHAPPOUR: I think there was a confusion
25 about -- I had done an op ed that I thought I

1 submitted.

2 CHAIR RAGGI: Oh, okay.

3 MR. GHAPPOUR: But I will submit more
4 comprehensive paperwork.

5 CHAIR RAGGI: Thank you. Thank you very
6 much.

7 Are there some questions for the professor?
8 Yes, Judge Kethledge.

9 JUDGE KETHLEDGE: Professor Ghappour, I just
10 want to make sure I understand two aspects of your
11 comments. So the concern you raise is not a Fourth
12 Amendment concern. It's a foreign policy concern. Is
13 that fair?

14 MR. GHAPPOUR: Well, it's not a Fourth
15 Amendment concern.

16 JUDGE KETHLEDGE: Okay.

17 MR. GHAPPOUR: But it is a concern that the
18 proposed rule is increasing the substantive powers of
19 the FBI and that that will affect our foreign policy,
20 yes.

21 JUDGE KETHLEDGE: Okay. That's helpful.
22 And so the other point is you're saying if the
23 government doesn't know where the computer is that it
24 wants to search, it therefore doesn't know whether the
25 computer is overseas, and therefore the government

1 should take no action. Is that a fair distillation of
2 what you're saying?

3 MR. GHAPPOUR: I do not think that our
4 domestic law enforcement agencies should conduct
5 overseas cyber operations without at least
6 coordinating within our government, yes.

7 JUDGE KETHLEDGE: Okay. But, I mean, so the
8 government is presented with a situation where a
9 computer somewhere is distributing child pornography.
10 They don't know where it is. You would advocate that
11 the government not take any action at that point, and
12 more to the point, that you would advocate that we do
13 not amend Rule 41 to potentially, subject to, you
14 know, constitutional limitations, et cetera, try to
15 act in that situation.

16 MR. GHAPPOUR: Absolutely.

17 JUDGE KETHLEDGE: Okay. No, I appreciate
18 your clarity.

19 MR. GHAPPOUR: Yes. That is correct.

20 JUDGE KETHLEDGE: Thank you.

21 CHAIR RAGGI: I think there was another
22 question. Professor Kerr.

23 PROF. KERR: Do you have a sense of what the
24 law enforcement in other countries do when confronted
25 with these same questions? Because it seems to me

1 that we're talking about a technological problem that
2 law enforcement in every country that's investigating
3 these sorts of cases would encounter, sort of each
4 side raising -- to the extent there are sovereignty
5 issues, any country is going to have to grapple with
6 them.

7 Do you have a sense of are there other
8 specific countries that refrain from investigating
9 these cases out of concerns of violating the
10 sovereignty of the United States or other countries,
11 and is there a norm of cooperation among law
12 enforcement groups, United States and other countries,
13 for example, say on a botnet case?

14 I know I've read press releases that suggest
15 that there is some cooperation at least where multiple
16 jurisdictions are involved. But I'm curious to the
17 extent you know, if you can shed light on how other
18 countries are dealing with these same question, that
19 would be great.

20 MR. GHAPPOUR: I think that there are
21 coordinated efforts for certain botnet investigations
22 and certainly some child pornography cases, and I
23 think that is a solution. That is not the solution
24 proposed.

25 However, as far as concerns about violating

1 sovereignty when using cyber operations or other forms
2 of surveillance abroad, I think that typically most
3 countries, including the United States, kind of
4 reserve that for their espionage activities. And
5 espionage activities are essentially encroaching on
6 sovereignty to conduct some form of surveillance,
7 getting information in a clandestine manner.

8 The difference here is that this is all in
9 public, and that is a very big concern because all of
10 a sudden you're violating the number one rule of
11 spying, which is getting caught. You're actually
12 volunteering the information. And when we start
13 volunteering the information, it will result in some
14 very catastrophic, in my opinion at least, some very
15 catastrophic foreign policy and international
16 relations issues.

17 The reason I would curtail the network
18 investigative technique, particularly when abroad, to
19 just returning back location information is that at
20 least it opens the door or it leaves the door open to
21 some sort of diplomatic resolution where you can think
22 that there might be an easier multilateral agreement
23 reached where the only sort of capability that's
24 allowed is figuring out what country that a certain
25 perpetrator is in, as opposed to a multilateral

1 agreement that allows law enforcement, whatever that
2 means in the international context, to just go ahead
3 and conduct cyber operations on targets that they
4 believe are in violation of a crime.

5 So, in a way, it is a policy issue, but the
6 threshold here is that we are expanding state power of
7 our domestic law enforcement.

8 CHAIR RAGGI: Judge Feinerman, did I see
9 your hand up?

10 JUDGE FEINERMAN: Would a way around the
11 international relations problem that you've raised be
12 that the magistrate judge satisfy herself or himself
13 that the government has a good faith basis to believe
14 that the target computer is in a judicial district of
15 the United States? And the reason I ask that is the
16 language of the rule, of the proposal, subsection A
17 and subsection B, refer to districts.

18 MR. GHAPPOUR: Yes.

19 JUDGE FEINERMAN: So the intent of the rule
20 I take from the use of the words districts is that
21 only domestic searches be permitted. So would my
22 proposal, my proposal on top of that proposal, address
23 your concern?

24 MR. GHAPPOUR: I don't think the current
25 language satisfies that. I mean, I agree that it at

1 least on its face appears to talk about districts.
2 But technologically, the reality is that 85, 90
3 percent of folks that are using this type of anonymity
4 software are abroad. And the purpose that we are
5 requesting or that this proposal is before us is
6 because we don't know where they are. And so it's a
7 very difficult sort of -- I don't know sort of what
8 the level of good faith -- is ignorance good faith?
9 Because if it is, then that would be automatically
10 satisfied.

11 Again, I'm not saying that this is sort of
12 like a loophole that's crafted by the DOJ or anything.

13 It's just a very difficult technical problem. And I
14 do understand that we need this operational capacity.

15 But unfortunately, as things stand, I don't think
16 we're there yet in terms of where we are in terms of
17 our international policy around cyberspace, in terms
18 of our military policy around cyberspace.

19 So there was just a joint -- there was
20 just -- I believe just a month ago there was a release
21 of a document by the Joint Chiefs on cyberwarfare and
22 cybersecurity that underscored the fact that for
23 certain operations that -- I mean, not in these
24 words -- that violate sovereignty of other nations or
25 sort of implicate these international issues that we

1 have to all be in agreement, all different sectors of
2 government.

3 The ignorance of where the location is is
4 precisely the problem there. Can you imagine being in
5 the State Department and all of a sudden realizing
6 that in order to go after someone that's suspected of
7 internet fraud I in the DOJ have just stepped on your
8 turf and kind of possibly ruined a lot of the hard
9 work that you've been doing with that foreign country.

10 I mean, that's just the reality, this sort of issue.

11 CHAIR RAGGI: Mr. Filip, you had a question?

12 MR. FILIP: Yeah. At one point you said
13 that it's quite clear that the U.S. never acts without
14 permission of the host country. Let's assume that's
15 false, okay? Let's assume that there's lots of
16 countries in the world who actively, perniciously,
17 violently try to harm U.S. citizens and U.S.
18 interests. So we'll assume that's false.

19 So, if that's true, and here we have an
20 unknown about whether the server is located in
21 Cleveland or in Syria or in Tehran or wherever it
22 might be. The FBI is prepared to take the risk that
23 its agents are going to be prosecuted and we won't
24 extradite them. That's not an issue. Then how else
25 but providing for some courthouse in the U.S. to go to

1 to present the warrant, would you address what you I
2 think just said to Judge Feinerman is a capacity that
3 must exist in order to prosecute these sort of crimes?

4 MR. GHAPPOUR: Yeah. So first of all, I
5 didn't say the United States Government never does
6 this. I said domestic law enforcement does not do it.
7 That was my statement. But it's a nuance.

8 MR. FILIP: Let's assume that's not true
9 too.

10 MR. GHAPPOUR: Yeah, I will, definitely. So
11 just assuming that that's not true, and the question
12 appears to be what would you do as an alternative.

13 MR. FILIP: Yeah.

14 MR. GHAPPOUR: I certainly wouldn't use the
15 FBI. I certainly wouldn't include this in the
16 traditional line of law enforcement. I wouldn't go
17 after -- I'd select very few crimes that I can go
18 after, in the same way that we do with national
19 security, and I would -- it depends on what my
20 interests are. If my interests are state security and
21 our national security, I would not do this in a public
22 venue. So there are cases where you have other bodies
23 of our government that can do a lot of -- you know,
24 whose very nature is covert, but it's not the FBI.

25 MR. FILIP: Sure. But the CIA is not a law

1 enforcement agency by design.

2 MR. GHAPPOUR: Exactly.

3 MR. FILIP: It can't operate that way in the
4 United States.

5 MR. GHAPPOUR: Yeah.

6 MR. FILIP: So they're not going to
7 prosecute child pornography cases.

8 MR. GHAPPOUR: Exactly. That's the problem.
9 I totally agree. And it is a very difficult problem,
10 but, you know, I think we're going a little too fast,
11 too soon with this. That's just my testimony, my
12 opinion, as just representing me here.

13 MR. FILIP: Fair enough.

14 MR. GHAPPOUR: And it's a very complex and
15 nuanced sort of issue. And that's why I think that
16 maybe -- maybe it's a congressional issue, you know.
17 Maybe it's not for a rulemaking body to decide these
18 very complicated issues. Once we get into
19 classification -- for instance, wouldn't we want to
20 classify all of this information? Wouldn't we want to
21 keep it away from the public view?

22 For instance, right -- and this is not
23 something we can determine here today, nor should it
24 be, right? And so maybe Congress is really the right
25 body to be talking about this issue because it

1 involves more than going after child pornographers.
2 It involves international relations.

3 CHAIR RAGGI: Mr. Bitkower, do you have a
4 question?

5 MR. BITKOWER: Yes. I guess I'm curious
6 because a lot of your comments have focused on the
7 need for State Department coordination or perhaps
8 intelligence community coordination in the Executive
9 Branch. And assuming that that were true in a
10 particular case, I guess I'm not understanding what
11 about the Rule 41 proposal would preclude or in any
12 way change the government's interest in doing that
13 intra-Executive Branch coordination prior to taking a
14 step that the government believed might have foreign
15 policy implications.

16 That is, what is it about the venue proposal
17 here would change that? And then taking that a step
18 further, let's imagine that coordination all took
19 place and everybody that you believe should be at the
20 table had their voice heard, and after being heard,
21 everybody agreed that the foreign policy and law
22 enforcement benefits outweighed any risks. Should
23 that step be precluded by the possibility of Bivens
24 liability if the computer turned out to be in the
25 United States? That is, why is that the proper

1 solution to regulate our foreign policy?

2 MR. GHAPPOUR: Well, you know, the problem
3 with the rule is not that it allows access within the
4 94 districts of the United States. Again, the problem
5 is that it sort of -- it's like turning on a switch,
6 but the switch all of a sudden -- instead of turning
7 on a faucet, it's a fire hose. So all of a sudden
8 we've got this enormous capability, right? And the
9 problem with the capability is you can't fine-tune it.
10 You can't tell the capability limit yourself to the
11 94 districts.

12 And that's the fundamental problem. So I'm
13 not saying that the problem with the proposal is that
14 it would allow 94 -- it would allow sort of increased
15 access within the 94. The concern is broad.

16 In terms of coordinating in advance, again,
17 because it's a fire hose, right, you don't really know
18 what you're coordinating about until after the fact.
19 There is no way -- it's actually impossible to -- if
20 you were -- let's say we want to coordinate and you're
21 sort of in the part of the government that deals with
22 foreign relations. I'm in the part that deals with
23 law enforcement. I can't call you up before the fact
24 and say anything but I'm about to execute a cyber
25 operation. It might be a foreign country. It might

1 be in the United States. That's not coordination.
2 And let's say it is coordination, right? That
3 decision hasn't been made or it's being kept away from
4 the public because the President's perspective -- the
5 President's policy views, as illustrated time and
6 again, in addition to that of our military, in
7 addition to that of the FBI, all contradict what's
8 about to happen here.

9 That is to say the President in his policy
10 view respects some notion of cyber sovereignty. The
11 military wants to act as a cohesive whole. That's not
12 happening here. And in terms of the FBI, if you go on
13 any public document of the FBI, that the FBI has of
14 the DOJ, it actually explicitly states that we don't
15 do investigations abroad without consent.

16 CHAIR RAGGI: All right. We're getting very
17 far afield from the rule that's before us. I have
18 this question for you. Assuming, as you've stated,
19 that the jurisdiction of a federal court does not
20 extend extraterritorially. Nevertheless, district
21 judges do issue and magistrate judges do issue arrest
22 warrants for people whose locations are not known and
23 who may very well be abroad. It then becomes the
24 responsibility of the Executive Branch if it's going
25 to seek to have an arrest made abroad to operate in

1 whatever way our treaties and mutual assistance
2 understandings obligate it to.

3 Why isn't the same thing so here? This rule
4 says to the Executive, if you don't know where a
5 computer is and you want to search it, go to the court
6 where the harm is being affected. Once the warrant is
7 issued, then again, isn't it the Executive Branch's
8 obligation to ensure that it doesn't execute it in a
9 way that creates any kind of international problems?
10 I don't see where it's a problem for the court any
11 more than the arrest warrant. But what am I missing
12 perhaps?

13 MR. GHAPPOUR: Well, what's interesting
14 is -- and I guess that's what I was trying to just
15 articulate. And I'm sorry. I was on an overnight
16 flight, and so --

17 CHAIR RAGGI: We understand. That's okay.

18 MR. GHAPPOUR: -- there are bags under my
19 eyes, very difficult to be standing here. But I think
20 the problem is that the current view that is at least
21 in the public about what the Executive's position is
22 on this exact issue does not comport with what the
23 rule is trying to do.

24 So, in other words, it sounds like what
25 you're saying -- and I might be wrong, but it sounds

1 like what you're saying is that the Executive has
2 given a directive to the FBI or whatever law
3 enforcement agency that says if a computer's location
4 is unknown you're allowed to go get it. So long as
5 you have probable cause you're allowed to go get it.

6 But what the government's position is as a
7 state is not that. And that's sort of the problem.
8 And maybe this is a process of the rulemaking that
9 sort of -- maybe we're jumping ahead, and maybe that's
10 why this needs to be before Congress. I'm not sure.

11 CHAIR RAGGI: No, we're asking you to
12 consider only that all we've done is tell them what
13 courthouse to go to, to think of this practically.
14 They then take the warrant and they do whatever they
15 do technologically, and they find out that the
16 computer causing havoc is in Germany.

17 Now I don't know whether they find that out
18 first and then go to their German counterparts or
19 whatever, but at that point, the court is out of it.
20 The court has made its determination that they've
21 shown us they don't know where the computer is
22 located. They've got probable cause. They fit
23 whatever else they have to fit. I'm not sure I
24 understand why it's a judicial concern how they
25 execute that warrant vis-à-vis our international

1 obligations.

2 MR. GHAPPOUR: So the problem is that there
3 is -- you do know -- or what you do know is that there
4 is no way that we're going to coordinate before
5 hacking Germany in that case or before launching a
6 cyber operation against Germany in that case.

7 CHAIR RAGGI: I don't know. We may have
8 tacit understandings with any number of our foreign
9 counterpart nations.

10 MR. GHAPPOUR: Well, yeah. But you don't
11 know that the --

12 CHAIR RAGGI: Or we may have understandings
13 that as long as you tell us as soon as you find out
14 it's in our country that's okay.

15 MR. GHAPPOUR: Yeah, and I agree. And
16 that's why I would recommend that only location
17 information is returned because that actually allows
18 there to be diplomatic discussion around something
19 that's more minimally invasive than turning on a
20 camera, for instance.

21 But to answer your question, you've issued
22 the warrant, and the question I believe is, is there a
23 constitutional issue with issuing that warrant where
24 it might end up going to another country.

25 CHAIR RAGGI: Is there any problem,

1 constitutional, statutory, any problem with the
2 court's actions? As I said, I'm putting aside the
3 Executive's obligations, but is there any problem with
4 what the court has done?

5 MR. GHAPPOUR: So, yes, maybe, perhaps.
6 I'll do my best to sort of wing up a response just
7 because in my gut I feel like it's wrong. And the
8 first reason is the court really shouldn't be involved
9 in our foreign policy. And if I am a prosecutor
10 giving you an application or submitting an application
11 to you and my statement is I don't know where this is
12 located, there's an 85 percent chance it will be
13 abroad, I'm going to conduct a unilateral cyber
14 operation in order to accomplish the search, and your
15 response as a judge is to say okay? Something in
16 there just doesn't sit well with me.

17 The second reason is that the authorizing
18 statute for the FBI to conduct arrests and searches
19 and such, while it doesn't have a geographic
20 limitation per se, it's never really been interpreted
21 one way or the other to my knowledge by a court to say
22 that, yes, you can by default, so just based on this
23 statutory authority you are allowed to go and conduct
24 investigative operations overseas, in violation of
25 international law.

1 Now, if we were to look back maybe 100 years
2 or so, we would see a lot of caselaw that would ask us
3 to interpret that authorizing statute within -- so as
4 not to contravene international law. That's just one
5 way to construct that statute.

6 CHAIR RAGGI: Okay.

7 MR. GHAPPOUR: Yes.

8 CHAIR RAGGI: All right. Mr. Siffert?

9 MR. SIFFERT: Isn't your concern better
10 addressed by politicking or petitioning Mr. Bitkower
11 and telling him that when you get warrants from a
12 court in a jurisdiction that you're authorized to get
13 it from now, that you only obtain first the country of
14 origin location data that you're talking about and
15 then decide what you want to do? But that's all
16 delegated to the Executive Branch. Why should that be
17 something that is in the court's province in the
18 beginning?

19 MR. GHAPPOUR: I think you said it right
20 there, and I think that I'd probably be better off
21 petitioning my congressman about that and not the
22 investigative authorities because that kind of inserts
23 the whole democratic process into it. Of course, I'm
24 basically -- it's a very difficult problem. I'm not
25 really sure how to solve it. I'm just sort of giving

1 recommendations that would still leave us open to some
2 sort of diplomatic overture.

3 CHAIR RAGGI: All right. I know you have
4 traveled far and, as you said, are exhausted, but
5 we've kept you a very long time. But we do thank you
6 for all your comments and insights. Thank you.

7 MR. GHAPPOUR: Thanks so much.

8 CHAIR RAGGI: All right. Now our last
9 speaker is Robert J. Anello of the Federal Bar
10 Council. Mr. Anello.

11 MR. ANELLO: Good morning. I think it's
12 still morning. So my thanks to Judge Raggi and the
13 advisory committee for the invitation to testify here
14 today. I am the president of the Federal Bar Council.
15 I am also a principal of a law firm that practices
16 criminal law, in particular white collar criminal
17 defense.

18 I am notably, as my family and partners have
19 told me, not a technology expert. The organization I
20 speak on here today is the Federal Bar Council, which
21 is a organization of lawyers that practice in the
22 federal courts and the Second Circuit. The council
23 was founded in 1932 and is dedicated to promoting
24 excellence in the federal practice. And the council
25 together with its several committees regularly

1 comments on proposed changes to the various rules that
2 affect the practice of our members.

3 The council has provided its views to the
4 proposed amendment for this rule and for Rule 4 in a
5 letter dated October 27 to the advisory committee.
6 And on behalf of the council, I commend the advisory
7 committee for its work in developing these amendments.

8 I don't envy this committee in trying to merge a 200-
9 year plus old Constitution with modern technology, and
10 I believe it has done an excellent job in attempting
11 to do that.

12 Because I have submitted my statement, I
13 will in fact be very brief today because I understand
14 I am the last person between you and the lunch break.

15 So Rule 41 addresses the circumstances under
16 which a court has authority to issue a warrant to
17 search and seize a person or property. With few
18 exceptions, the court's authority is limited to
19 issuing warrants for the search and seizure of
20 property located within the district.

21 Based on its recent experiences and the
22 evolving nature of crime, the Department of Justice
23 has raised concerns about the rule's territorial venue
24 restrictions in the context of efforts to search and
25 seize electronic information. In particular, the

1 Department of Justice is concerned that the rule may
2 impede investigations when location of electronic
3 information sought is unknown or the electronic
4 information sought spans multiple districts, requiring
5 law enforcement to coordinate efforts with local
6 enforcement and prosecutors and courts in multiple
7 districts.

8 At least one court in the Southern District
9 of Texas has ruled that a warrant under such
10 circumstances, because of the rule's express
11 territorial limits, was improper.

12 The advisory committee has proposed two
13 changes to Rule 41 to address these concerns. A
14 proposed section, Rule 41(b)(6), sets out two
15 circumstances under which a court may issue a warrant
16 to use remote access to search electronic storage
17 media and to seize or copy information even if the
18 information is or may be located outside of the
19 district. And the second rule, 41(f)(1)(c), would be
20 amended to include language indicating the process for
21 providing remote access, notice of remote access
22 search.

23 The Federal Bar Council believes that on
24 balance these amendments are necessary and will be
25 effective in permitting law enforcement to investigate

1 crimes involving computers and electronic information.

2 Rule 41's current limits present unique problems for
3 investigations requiring access to electronic
4 information or storage devices.

5 For instance, sophisticated software that we
6 heard about today may be used to mask the location of
7 a computer or electronic storage devices. In this
8 situation, law enforcement may be prevented from
9 identifying the district in which the electronic
10 information or electronic device is located in an
11 otherwise sufficiently detailed warrant.

12 Important law enforcement efforts likewise
13 may be thwarted or delayed by complex criminal schemes
14 that involve the use of multiple computers in multiple
15 districts simultaneously.

16 Under the current Rule 41, investigations of
17 such schemes may require the government to expend
18 extraordinary resources and efforts to obtain
19 individual warrants from various districts. Both of
20 these problems have become more common as crimes
21 involving the use of computers have increased in
22 frequency and complexity.

23 The advisory committee took prudent action
24 to propose the narrowly tailored amendments at issue,
25 reasoning that the use of anonymizing software to mask

1 a computer's location or the use of malicious software
2 to infect a large number of computers scattered in
3 multiple districts should not prevent law enforcement
4 from efficiently investigating serious federal crimes
5 in the face of increasingly more sophisticated
6 criminal activities.

7 Under the proposed amendments, investigators
8 could obtain a warrant to install remotely software on
9 a target device to determine the true address or
10 identifying information for that device, but only if
11 the location of the device or the information has been
12 concealed through technological means.

13 The council understands that the ACLU has
14 submitted thoughtful comments to the advisory
15 committee objecting to this type of remote access.
16 The council's federal criminal practice committee has
17 reviewed the ACLU's objections, which initially were
18 submitted in response to the broader version of the
19 proposed rule. The council has concluded that the use
20 of remote access is appropriate under the narrow
21 circumstances outlined in your proposed rule.

22 While providing important rules and vehicles
23 for law enforcement to proceed, the proposed
24 amendments leave unanswered a number of important
25 constitutional questions, and we think it does so

1 wisely, such questions as the level of specificity
2 required in a warrant seeking authorization to conduct
3 remote access or seizure.

4 The council believes, however, that these
5 questions and technological and treaty issues that
6 we've heard about today can and will be addressed by
7 the courts, and with respect to things like the
8 treaty, the Executive Branch, as matters develop.
9 They are not something that can or in our opinion
10 should be addressed by the rules.

11 For these reasons and those set forth in the
12 October 27 letter, the Federal Bar Council supports
13 the proposed amendments to the Federal Rules and
14 believes that they effectively and fairly address the
15 current issues faced by this committee. Thank you.

16 CHAIR RAGGI: Thank you very much.

17 Do we have any questions for Mr. Anello?

18 (No response.)

19 CHAIR RAGGI: No? Thank you very much.

20 MR. ANELLO: Thank you.

21 CHAIR RAGGI: I want to thank everyone who
22 participated today for both your written and oral
23 comments. The committee is now going to break for
24 lunch, so we thank you all very much. You're all
25 excused. All right. So 10 minutes, and then we'll

1 start with lunch.

2 (Whereupon, at 12:05 p.m., the public
3 hearing in the above-entitled matter was adjourned.)

4 //

5 //

6 //

7 //

8 //

9 //

10 //

11 //

12 //

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

REPORTER'S CERTIFICATE

DOCKET NO.: N/A
CASE TITLE: Public Hearing - Criminal Rules
Committee Meeting
HEARING DATE: November 5, 2014
LOCATION: Washington, D.C.

I hereby certify that the proceedings and evidence are contained fully on the tapes and notes reported by me at the hearing and include the revisions provided by the agency in the above case before the Administrative Office of the United States Courts.

Date: November 5, 2014

David W. Jones
Official Reporter
Heritage Reporting Corporation
Suite 600
1220 L Street, N.W.
Washington, D.C. 20005-4018

Heritage Reporting Corporation
(202) 628-4888