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@hrccourtreporters.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

APPEARANCES: (Cont'd.)

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

I N D E X

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

the purpose of making our review more informed.

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

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

(Pause.)

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

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

The ACLU urges the committee to reject the

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

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

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

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

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

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

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

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

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

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

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

unidentified targets and innocent nonsuspects as well.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

But the troubles with providing notice for these kind of searches will mean that in some cases suspects who are actually charged and indicted may know about it, but those third parties may never know. And the person who does know may not have Fourth Amendment standing or Article III standing to challenge on behalf of those others affected who may in fact have the stronger privacy argument under the Fourth Amendment.

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

CHAIR RAGGI: Judge Rice.

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

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

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

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

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

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

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

CHAIR RAGGI: Anything else?

PROF. BEALE: Judge?

CHAIR RAGGI: Yes. Professor Beale.

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

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

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

PROF. BEALE: Actual receipt of notice.

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

PROF. BEALE: Right.

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

would be able to actually tell them.

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

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

PROF. BEALE: Unless the provider gives it.

MR. WESSLER: Unless the provider gives it. And some providers have been very aggressive about doing that, and that's terrific. But the burden shouldn't be on them to undertake the time and expense to do that in our opinion.

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

MR. WESSLER: Yes, yes.

PROF. BEALE: Thank you.

CHAIR RAGGI: Oh, I'm sorry. Judge

Feinerman.

JUDGE FEINERMAN: Good morning.

MR. WESSLER: Good morning.

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

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

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

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

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

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

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

JUDGE FEINERMAN: All right. Thank you.

CHAIR RAGGI: Mr. Bitkower.

MR. BITKOWER: Thank you. I just want to

focus a little on what the scope of your objection is. You talk a lot about the difficulties inherent in remote searches, but most of your remarks relate to the use of network investigative techniques. Do your same objections apply to any remote search, or are your objections focused on the use of techniques like these?

MR. WESSLER: So we have concerns about any remote search. Now most of these remote searches require one of these techniques. I mean, inherently, unless you have the consent of the person whose computer you're trying to remotely search as a government investigative agent, then there needs to be some technical means to enter their computer, and computers, you know, computer security is now such a foreground of concern for all of us that firewalls and virus protection programs and other protections make it difficult without one of these technological means. And I'll leave it to my colleague, Mr. Soghoian, to help address that in a little more detail.

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

of information were.

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

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

internetworked information systems.

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

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

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

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

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

MR. WESSLER: Thank you.

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

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

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

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

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

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

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

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

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

As I noted before, in the course of my

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

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

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

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

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

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

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

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

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

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

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

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

If the FBI's malware malfunctions and causes, you know, some kind of further computer security issue to the affected targets, we have no way of knowing if the FBI will let people know and say, you know what, sorry, you know, that was our software. It accidentally spread to innocent people's computers. It accidently, you know, crashed 1,000 computers. From everything that we've seen to date, you know, they're not going to put out a press release and acknowledge that it was their fault.

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

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

Now thankfully, in that situation, they did not send the malware to the wrong email address, but I think the issues that we have already in the physical world of the police kicking down the wrong door are ever-present in the online world. And at least in the physical world, when the police kick down that door and they are expecting a man and they see a woman and they're expecting someone of a certain age and they see someone of a different age, they immediately have some idea that they've gotten the wrong email address. I suspect that in the case of malware, the malware may be able to get further before they realize that they have sent things to the wrong address.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CHAIR RAGGI: Thank you.

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

rights-abusing governments monitoring them.

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

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

CHAIR RAGGI: Thank you.

Any questions? Professor Kerr.

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

method is nonetheless too intrusive in your view?

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

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

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

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

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

CHAIR RAGGI: Any other questions?

(No response.)

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

MR. SOGHOIAN: Thank you.

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

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

Rule 41 regarding remote access searches.

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

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

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

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

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

particularly described in the warrant.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MR. BANKSTON: Huh?

CHAIR RAGGI: Is that a question?

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

MR. BANKSTON: Yes.

CHAIR RAGGI: Yes, Judge Feinerman.

JUDGE FEINERMAN: Let me ask you the same

question I asked Mr. Wessler. There are situations where the owner of a computer engaged in criminal activity, say trafficking in child pornography, hides the location of the computer. The government wants to investigate. What's your solution to the venue issue? What court should the government be allowed to go to in order to get a warrant to search that computer if it doesn't know where the computer is?

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

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

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

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

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

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

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

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

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

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

CHAIR RAGGI: Okay. Thank you.

PROF. BEALE: May I have one more?

CHAIR RAGGI: Yes, Professor Beale.

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

know, you might have thought about that as an analog. And we were just looking. We weren't seeing it.

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

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

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

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

MR. BANKSTON: Yeah.

PROF. BEALE: Thank you.

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

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

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

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

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

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

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

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

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

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

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

MR. BANKSTON: Thank you very much.

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

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

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

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

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

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

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

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

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

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

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

CHAIR RAGGI: Thank you. Go ahead.

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

PROF. KING: Southern District of New York.

MR. HALL: Yeah, there you go.

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

Both of these changes were either directly

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

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

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

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

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

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

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

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

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

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

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

MR. HALL: Oh, please.

CHAIR RAGGI: Judge Kethledge.

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

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

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

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

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

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

JUDGE KETHLEDGE: Sure. Thank you.

CHAIR RAGGI: Professor Beale.

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

MR. HALL: Yes.

PROF. BEALE: -- to show that evidence of a crime could be found at the place to be searched, and the anonymizing software or the concealment only goes to the question of which courthouse you go to, right? Because when I saw a reference to a VPN, I use a VPN, right? Most people do --

MR. HALL: I hope so.

PROF. BEALE: -- if they're traveling remotely or at their work. But I believe that doesn't increase my chances of being searched under this amendment. This is really only about forum shopping. And do your remarks at all depend -- when you were saying it has to be connected to illegality and it's really innocent, if we focus on that, does that change your view at all?

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

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

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

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

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

MR. HALL: Maybe I'm not understanding.

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

MR. HALL: Yeah.

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

MR. HALL: Uh-huh.

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

MR. HALL: Yeah.

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

MR. HALL: May be occurring, right.

CHAIR RAGGI: Okay.

PROF. BEALE: Is alleged, yeah.

CHAIR RAGGI: Well, that's a question for

the magistrate to evaluate.

MR. HALL: Sure.

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

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

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

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

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

CHAIR RAGGI: Could you turn on the mike?

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

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

MR. HALL: Yeah.

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

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

what courthouse do you go to to start the debate.

MR. HALL: Yeah.

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

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

CHAIR RAGGI: Anything else?

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

country it is?

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

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

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

without even the concealment element.

CHAIR RAGGI: Judge Feinerman.

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

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

That's why we have the DNS, so I don't have to remember that. But certainly there are entities that you don't need to know anything about that issue IP addresses, and you can take them wherever you want. So, as someone who has been issued a chunk of these numbers, you can move to, you know, some different part of the country, some different part of the world and fundamentally sever any historical connection you may have had between the mapping of geographic

location and the network location.

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

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

(Laughter.)

CHAIR RAGGI: Any other questions?

(No response.)

CHAIR RAGGI: All right.

MR. HALL: Thank you.

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

MR. HALL: Sure.

CHAIR RAGGI: We have two public hearings scheduled on this rule, today here in Washington and then another one in January at Vanderbilt Law School. We urged as many interested parties as possible to give us your comments and to appear today rather than to wait until January because we knew you would be raising issues that we would want time to study.

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

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

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

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

CHAIR RAGGI: Thank you very much. Thank you.

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

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

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

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

I'm going to talk just briefly on a few points. My colleagues have covered many points today. But most importantly, I'm going to talk about the issues of necessity and prompt notice.

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

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

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

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

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

The problem with the proposed rule is that it provides specific rules about how and if notice will be delivered without providing for requiring notice within a given amount of time or prompt notice and also without requiring the level of necessity that I believe courts and Congress have previously imposed. And I think this has come out in many of the sort of questions and discussions here with regard, for example, to the venue issue.

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

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

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

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

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

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

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

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

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

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

Thank you.

CHAIR RAGGI: Yes. Professor King.

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

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

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

PROF. KING: Thank you.

CHAIR RAGGI: Any other questions? Professor Kerr.

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

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

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

MR. BUTLER: Right.

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

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

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

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

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

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

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

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

MR. BUTLER: Sure.

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

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

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

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

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

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

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

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

MR. BUTLER: Right.

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

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

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

MR. BUTLER: Right. Exactly.

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

CHAIR RAGGI: Thank you.

MR. BUTLER: Thank you.

MR. BITKOWER: One more question.

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

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

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

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

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

MR. BUTLER: Right.

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

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

CHAIR RAGGI: Anything else?

(No response.)

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

MR. BUTLER: Thank you.

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

MR. ANELLO: Yes.

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

(Whereupon, a brief recess was taken.)

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

MS. STEPANOVICH: Thank you.

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

MS. STEPANOVICH: Yes.

CHAIR RAGGI: Thank you.

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

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

My name is Amie Stepanovich.

CHAIR RAGGI: We feel the same way.

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

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

My first emphasis is that this rule change

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

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

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

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

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

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

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

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

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

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

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

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

A little bit about the CFAA so I can give you background on a law that many of you may not be familiar with. It was initially passed in 1986. It's traditionally used to prosecute the theft of private data or damage to systems by way of malicious hacking. The CFAA was designed to provide justice for victims of these activities by offering a remedy against perpetrators. The plain text of the relevant section of the CFAA clearly focuses on knowing or intentional malicious activity.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CHAIR RAGGI: Professor Beale.

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

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

MS. STEPANOVICH: Uh-huh.

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

MS. STEPANOVICH: Uh-huh.

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

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

the warrant and how the search is carried out.

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

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

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

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

CHAIR RAGGI: Professor Kerr, you had a question?

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

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

MS. STEPANOVICH: Uh-huh.

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

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

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

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

CHAIR RAGGI: I think Judge Lawson.

JUDGE LAWSON: Good morning.

MS. STEPANOVICH: Good morning.

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

MS. STEPANOVICH: I do not.

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

MS. STEPANOVICH: Uh-huh.

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

MS. STEPANOVICH: Uh-huh.

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

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

JUDGE LAWSON: Right.

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

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

MS. STEPANOVICH: Yes.

JUDGE LAWSON: So that --

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

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

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

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

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

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

JUDGE LAWSON: Yeah.

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

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

JUDGE LAWSON: Good, good. All right.

CHAIR RAGGI: Mr. Bitkower?

JUDGE LAWSON: That's helpful. Thank you.

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

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

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

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

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

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

used for and that some of the instances are inappropriate.

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

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

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

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

MR. FILIP: Yeah, I just want to clarify

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

So independent of whether or not the CFAA has been in the past interpreted consistent with the organization's viewpoint or in the future will be interpreted consistent with your aspirations, this is a venue provision about where to go to file a warrant. So is there anything about the venue provision that will allow in the future you to litigate maybe as amicus and defendants, all sorts of folks, to have substantive debates about the precedent? And you can go to Congress and try to get the law changed, all sorts of things. Is there something about the venue provision that you would offer that you think would improve it?

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

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

MR. FILIP: Okay.

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

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

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

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

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

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

MS. STEPANOVICH: Uh-huh.

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

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

CHAIR RAGGI: Please, take your time.

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

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

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

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

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

CHAIR RAGGI: Thank you. Thank you.

Any other questions?

(No response.)

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

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

CHAIR RAGGI: Good. Thank you.

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

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

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

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

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

Now, in terms of the substantive expansion

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

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

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

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

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

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

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

is not encroaching upon their investigative activities.

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

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

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

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

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

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

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

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

Reportedly, this was the first ever FBI case to utilize the technique of extraterritorial seizure of digital evidence. Notably, in this case, the access was through the web using log-in information that was obtained consensually from the perpetrators. So that is to say that the level of powers that we're seeking here are much broader than that that was implemented in the Seattle example, in the Russia example.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

submitted.

CHAIR RAGGI: Oh, okay.

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

CHAIR RAGGI: Thank you. Thank you very much.

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

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

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

JUDGE KETHLEDGE: Okay.

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

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

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

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

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

MR. GHAPPOUR: Absolutely.

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

MR. GHAPPOUR: Yes. That is correct.

JUDGE KETHLEDGE: Thank you.

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

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

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

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

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

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

However, as far as concerns about violating

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

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

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

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

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

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

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

MR. GHAPPOUR: Yes.

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

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

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

Again, I'm not saying that this is sort of like a loophole that's crafted by the DOJ or anything. It's just a very difficult technical problem. And I do understand that we need this operational capacity. But unfortunately, as things stand, I don't think we're there yet in terms of where we are in terms of our international policy around cyberspace, in terms of our military policy around cyberspace.

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

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

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

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

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

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

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

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

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

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

MR. FILIP: Yeah.

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

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

enforcement agency by design.

MR. GHAPPOUR: Exactly.

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

MR. GHAPPOUR: Yeah.

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

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

MR. FILIP: Fair enough.

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

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

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

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

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

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

solution to regulate our foreign policy?

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

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

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

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

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

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

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

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

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

CHAIR RAGGI: We understand. That's okay.

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

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

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

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

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

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

obligations.

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

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

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

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

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

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

CHAIR RAGGI: Is there any problem,

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

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

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

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

CHAIR RAGGI: Okay.

MR. GHAPPOUR: Yes.

CHAIR RAGGI: All right. Mr. Siffert?

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

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

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

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

MR. GHAPPOUR: Thanks so much.

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

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

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

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

The council has provided its views to the proposed amendment for this rule and for Rule 4 in a letter dated October 27 to the advisory committee. And on behalf of the council, I commend the advisory committee for its work in developing these amendments. I don't envy this committee in trying to merge a 200-year plus old Constitution with modern technology, and I believe it has done an excellent job in attempting to do that.

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

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

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

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

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

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

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

crimes involving computers and electronic information. Rule 41's current limits present unique problems for investigations requiring access to electronic information or storage devices.

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

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

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

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

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

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

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

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

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

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

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

CHAIR RAGGI: Thank you very much.

Do we have any questions for Mr. Anello?

(No response.)

CHAIR RAGGI: No? Thank you very much.

MR. ANELLO: Thank you.

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

start with lunch.

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

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

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