Testimony of Kevin S. Bankston,
Policy Director of New America's Open Technology Institute

On Proposed Amendments to Rule 41
of the Federal Rules of Criminal Procedure

Before The Judicial Conference Advisory Committee
on Criminal Rules

November 5, 2014

Members of the Committee,

Thank you for allowing New America's Open Technology Institute ("OTI")[1] to testify and share our concerns about the proposed amendment to Federal Rule of Criminal Procedure 41 regarding "remote access" searches of electronic devices.[2]

I am here today to question the basic and quite substantive premise implicit in the proposed amendment: that "remote access" searches by the government—or more accurately, the government's surreptitious hacking into computers or smartphones in order to plant malware that will send data from those devices back to the government—are allowed by the Fourth Amendment.

Based on precedent almost half a century old, we believe the proposed amendment authorizes searches that are unconstitutional for lack of adequate procedural protections tailored to counter those searches' extreme intrusiveness—much like the New York state electronic

[1] New America's Open Technology Institute ("OTI"), http://newamerica.org/oti/.
[2] Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure: Request for Comment (Proposed Amendments Draft), 338-342 (Aug. 2014), *available at* http://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0001 (authorizing issuance of warrants "to use remote access to search electronic storage media and to seize or copy electronically stored data" in cases where the target computer's location "has been concealed by technological means" or in a computer crime investigation where the computers to be searched "have been damaged without authorization and are located in five or more districts").

eavesdropping law that was struck down as unconstitutional by the Supreme Court in *Berger v. New York* nearly 50 years ago.[3] There, the court held that because electronic eavesdropping "by its very nature…involves an intrusion on privacy that is broad in scope," authority to conduct such surveillance should only be granted "under the most precise and discriminate circumstances" in order to ensure that the Fourth Amendment's particularity requirement is met.[4]

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

Foremost among those Title III safeguards are the four that are intended to enforce the Fourth Amendment's particularity requirement consistent with the *Berger* decision, which held that "[t]he need for particularity…is especially great in the case of eavesdropping."[8] The court in *US v. Torres*,[9] the first of many circuit courts to find that these four *Berger*-derived requirements are also constitutionally required for video surveillance,[10] summarized them well:

---

[3] 388 U.S. 41 (1967).
[4] *Id*. at 56.
[5] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III" or the "Wiretap Act"), 18 U.S.C. § 2510 *et seq*.
[6] *Id*. at §2518.
[7] *See, e.g.*, Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 Hastings L.J. 805, 815 (2003).
[8] *Berger*, 388 U.S. at 56.
[9] *United States v. Torres*, 751 F.2d 875 (7th Cir. 1984), *cert. denied*, 470 U.S. 1087 (1985).
[10] *See United States v. Biasucci*, 786 F.2d 504, 508-10 (2d. Cir. 1986), *cert. denied*, 479 U.S. 827 (1986), *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251-52 (5th Cir. 1987), *United States v. Mesa-Rincon*, 911 F.2d 1433, 1436-39 (10th Cir. 1990), *United States v. Koyomejian*, 970 F. 2d 536, 538-42 (9th cir. 1991) (*en banc*), *cert. denied*, 506 U.S. 1005 (1992), *United States v. Falls*, 34 F.3d 674, 678-80 (8th Cir. 1994), and *United States v. Williams*, 124 F.3d 411, 416 (3rd Cir. 1997).

> [T]he judge must certify that [1] "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," 18 U.S.C. § 2518(3)(c), and that [2] the warrant must contain "a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates," § 2518(4)(c), [3] must not allow the period of interception to be "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days" (though renewals are possible), § 2518(5), and [4] must require that the interception "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under [Title III].[11]

As the *Torres* court concluded, "Each of these four requirements is a safeguard against electronic surveillance that picks up more information than is strictly necessary and so violates the Fourth Amendment's requirement of particular description."[12]

Title III, consistent with *Berger* and the Fourth Amendment's demand of reasonableness, also includes a clear requirement of service of notice on the target of the surveillance soon after the surveillance is completed—with no exceptions for failure to notify.[13] And finally, Title III includes a number of additional "super-warrant" checks and balances intended by Congress to further ensure the reasonableness of the surveillance to balance its intrusiveness, including a requirement that such surveillance only be used in the investigation of specifically identified serious crimes.[14] Only with such super-warrant protections in place have warrants for electronic surveillance been found constitutional under the Fourth Amendment.

Today, nearly half a century later, we are faced with a digital surveillance technique that is substantially more invasive than the analog electronic surveillance techniques of the past. Yet this

---

[11] *Torres*, 751 F.2d at 883-84.
[12] *Id*. at 884.
[13] 18 U.S.C. §2518(8)(d).
[14] 18 U.S.C. §2516(1); *see also Torres*, 751 F.2d at 890-91 (summarizing additional Title III requirements).

Committee, without any support from Congress or the courts, is poised to explicitly authorize warrants for such remote access searches with no additional protections at all and with a constitutionally novel allowance for no notice in certain cases. This is particularly concerning because the procedural protections required in cases of eavesdropping, wiretapping and video surveillance are even more necessary here, when the devices to which the government seeks access can contain an unprecedented wealth of private data—our digital "papers and effects."

Indeed, the one published decision to address a warrant application regarding a remote access search—Magistrate Judge Smith's opinion in Houston last year, the *In Re Warrant* case—rejected the application based not only on Rule 41 considerations but also based on a failure to satisfy the Fourth Amendment's particularly requirement, including the enhanced *Berger*/*Torres* particularity requirements typically applied to electronic surveillance.[15]

The proposed amendment, in attempting to address the Rule 41 issue raised by Judge Smith's opinion, necessarily also makes a substantive judgment regarding the Fourth Amendment's application to remote access searches. It does so first by authorizing remote access searches where the location of the target computer is unknown—a type of search that Judge Smith found was a *per se* violation of the requirement that the "place to be searched" be particularly described[16]—and second by choosing not to insist that remote access searches meet the *Berger*/*Torres* requirements that undoubtedly apply.

Those requirements undoubtedly apply, as Judge Smith held,[17] because remote access searches implicate and amplify all of the same problems as electronic surveillance, by virtue of providing access to an even greater wealth of private information. As he described, computers contain—and the government's remotely installed software has the capacity to access—"Internet browser history, search terms, e-mail contents and contacts, 'chat', instant messaging logs, photographs, correspondence, and records of applications run, among other

---

[15] *In Re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 758-61 (S.D. Tex. 2013).
[16] *Id*. at 758-760.
[17] *Id* at 760-61

things…."[18] Not only can government software secretly "search the computer's hard drive, random access memory, and other storage media," but it can also "activate the computer's built-in camera[,] generate latitude and longitude coordinates for the computer's location[,] and[] transmit [all of that] extracted data to the FBI…."[19]

Like Judge Smith, the Supreme Court recently recognized the unprecedented amount of private data that may be stored on an electronic device such as a computer or a smartphone. As the Court explained in this year's *Riley v. California* decision regarding searches of cell phones incident to arrest, many cell phones "are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[20] These devices, with "immense storage capacity," can hold "every picture [their users] have taken, or every book or article they have read," and "even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on."[21] Stand-alone computers that could be reached by a remote access search can store even more—and even more types—of private data than the smartphones that the Supreme Court sought to protect against unreasonable searches. Ultimately, as the Supreme Court explicitly held, the search of a modern electronic device such as a smartphone or a computer is more privacy invasive than even "the most exhaustive search of a house".[22]

In this technological context, the constitutional necessity of applying the *Berger*/*Torres* particularity requirements to remote access searches is clear. That need—especially in regard to minimizing the search of devices or the seizure of data that are not particularly identified in the warrant—is amplified even further by several other risks that have been discussed at length by other commentators as well as Judge

---

[18] *Id.* at 760.
[19] *Id*. at 755.
[20] *Riley v. California*, 134 S. Ct. 2473, 2489 (U.S. 2014).
[21] *Id.*
[22] *Id*. at 2491.

Smith.[23] These risks include the privacy risk to non-suspects who share the target computer, which might be a public terminal at a library or a café;[24] the risk that the government's software may spread to non-target computers;[25] the possibility, in cases of botnet investigations or so-called "watering hole" attacks, that thousands or even millions of computers may be infected with remote access software;[26] and the risk that software used to remotely access any of those computers may end up causing damage, either by altering or deleting data or creating security vulnerabilities that may be exploited by others.[27]

Indeed, it may be that remote access searches carry so many risks that they are unreasonable under the Fourth Amendment or as a policy matter even if they satisfy the *Berger/Torres* requirements; notably, neither the courts nor Congress have yet addressed those questions. This brings us back to my starting proposition: that by explicitly authorizing remote access searches, the proposed amendment represents a substantive judgment regarding the constitutionality of those searches and a policy judgment regarding the appropriateness of such searches, regardless of the Committee Note's claim that "[t]he amendment does not address constitutional questions.[28]

The proposed amendment's explicit authorization of remote access searches where the computer location is not known, in the face of the one published decision on the matter finding that such searches are *per*

---

[23] *In Re Warrant*, 958 F. Supp. 2d at 759.
[24] *Id*.
[25] *Id*.
[26] *See, e.g.,* Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media at 6-8, 14-15(Oct. 31, 2014), *available at* https://www.aclu.org/sites/default/files/assets/aclu_comment_on_remote_access_proposal.pdf ("ACLU Comments") (discussing "watering hole" attacks on visitors to popular websites); Written Statement of the Center for Democracy & Technology Before the Judicial Conference Advisory Comm. on Criminal Rules at 8, 10 (Oct. 24, 2014), *available at* https://cdt.org/insight/testimony-for-the-judicial-conferences-advisory-committee-on-criminal-rules-rule-41/ ("CDT Comments") (discussing how botnet investigations may implicate millions of computers).
[27] *See, e.g.*, ACLU Comments at 9-10, 17-18; CDT Comments at 8-9.
[28] Proposed Amendments Draft at 341.

se violations of the Fourth Amendment's particularity requirement, represents a substantive legal judgment.

The proposed amendment's unprecedented allowance for situations where notice may not reach the target, in the context of case law that has never provided any exception to the rule that notice must be served, is a substantive legal judgment.

The proposed amendment's authorization of remote access searches without requiring satisfaction of the *Berger*/*Torres* particularity requirements, contrary to the one published decision finding that those requirements do apply, is a substantive legal judgment. So too would it be a substantive legal judgment for the Committee to include those requirements, which just further demonstrates how the substantive and procedural questions on this issue are inextricably intertwined.

Ultimately, such substantive expansions of the government's authority as those represented in this proposed amendment are not the province of this Committee. We therefore urge that this Committee reject the proposed amendment to Rule 41 and leave these substantive constitutional and policy questions where they belong, in the courts and in Congress.

Thank you for you consideration, and I welcome your questions.