NACDL
1660 L St., NW, 12th Fl.
Washington, DC 20036

February 17, 2015

To the Members of the Advisory Committee:

The National Association of Criminal Defense Lawyers is pleased to submit our comments on the proposed changes to Rule 41 of the Federal Rules of Criminal Procedure. Our comments on the proposed amendments to Rule 4 and 45 will be submitted separately.

Our organization has approximately 10,000 members; in addition, NACDL's 94 state and local affiliates, in all 50 states, comprise a combined membership of over 30,000 private and public criminal defense attorneys and interested academics. NACDL, which celebrated its 50th Anniversary in 2008, is the preeminent organization in the United States representing the views, rights and interests of the criminal defense bar and its clients. As you know, we are regular observers at Committee meetings and have a long record of submitting comments. On the basis of that history, we appreciate the close and respectful attention that our comments have always received.

## CRIMINAL RULE 41 – WARRANTS AUTHORIZING REMOTE ACCESS TO COMPUTERS

The proposed amendment to Rule 41(b) would add to the Rule a third circumstance in which a Magistrate Judge may issue a warrant to search for and seize property located outside the judicial district. One of the existing circumstances is uncontroversial and deals with a purely practical problem – a warrant to search in U.S. territory outside the boundaries of any District. *See* Rule 41(b)(5). The other such existing authority, found in subsection (b)(3), was inserted into the Rule by legislative action, the USA PATRIOT Act of 2001, and applies only to investigations of domestic or international terrorism. *See also* 18 U.S.C. § 2703(a); *In re Search Warrant*, 2005 WL 3844032 (M.D.Fla. 2006) (Stored Communications Act, as amended by PATRIOT Act, adopting procedures of Rule 41), *rev'g* 362 F.Supp. 2d 1298 (M.J.-M.D.Fla. 2003). The broad and remarkably vague wording of subsection (b)(3) has yet to be authoritatively construed and has been the subject of only a few lower-level opinions. Yet the proposed amendment, without legislative support, would go even further, and codify a broad new authority to issue warrants for out-of-district searches for (and of) computers in relation to the investigation of any federal crime and – in certain computer crime cases – simply for the convenience of law enforcement agents even if the location of the computers is known.

While presented as addressing a venue problem, the proposal would instead essentially eliminate any venue requirement for digital searches of this kind by making the Rule's limitations so expansive and unbounded as to be meaningless. NACDL opposes this amendment, both because it overreaches the authority of judicial branch, which is limited in its rulemaking authority to purely procedural matters – a limitation that calls for particularly sensitive attention in the area of search and seizure – and because it would upset the appropriate balance that must be struck between law enforcement methods and the protection of privacy in a civil society now become digital.

For nearly 50 years, ever since the landmark opinion of the Supreme Court in *Berger v. New York*, 388 U.S. 41 (1967), the Supreme Court has recognized that the Fourth Amendment is not impotent to control new forms of law enforcement intrusion upon the privacy and security of "the People in their persons, houses, papers, and effects" that are made possible by advances in technology. But ordinary search warrants, governed by ordinary standards, often will not suffice to meet the demands of particularity and reasonableness of execution in new technological contexts, as *Berger* explained. For this reason, in response to that decision, Congress in 1968 enacted a detailed statutory scheme for the authorization and regulation of wiretapping, 18 U.S.C. §§ 2510-2521 ("Title III"), which has since stood the test of time and judicial scrutiny. Congress acted upon the same lesson when it adopted – and on later occasions amended – the Stored Communications Act, 18 U.S.C. §§ 2701-2708, 2711, as well as less complex but nonetheless carefully crafted legislative provisions to govern other kinds of searches. *See* 18 U.S.C. § 3117 (mobile tracking devices); 18 U.S.C. §§ 3121-3127 (trap-and-trace devices).

No current law or rule attempts to address the Fourth Amendment issues implicit in any use of "remote access to search electronic storage media and to seize or copy electronically stored information," to quote the current proposal. The principal flaw in the proposed change in Rule 41 is that it suggests a view that such searches may properly be authorized by ordinary warrants. NACDL very much doubts this is so. By attempting to bring such searches within the conventional framework of Rule 41, the proposal disrupts fundamental balances of jurisdiction and traditional warrant requirements based upon an analysis of what is most expeditious for law enforcement, while turning a blind eye to the inescapable conclusion that these aggressive digital interventions, which both exploit vulnerabilities in the Internet and deliberately create new ones, have technological, political and constitutional implications far beyond the simple mechanics of their application to a specific law enforcement goal.

Changes with such far-reaching potential consequences, even when procedural in form, are not merely procedural. (The line between substance

and procedure is particularly fraught in the context of search warrant regulation, even in its least controversial provisions. See, *e.g.*, Rule 41(c) (listing items subject to search or seizure, which is arguably not "procedural" at all).) Expansion of search authority in response to new technological challenges is political in the purest sense, and requires a political process to justify enactment. No matter how sage and responsible in fulfilling its mission the Committee may be, it is not the forum for resolving the merits of such dramatic change against the demerits of its many unintended but inevitable consequences.

The Advisory Committee Note assures us that "the amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require." Given the disruptive constitutional and commercial potential inherent in the aggressive tactics to be authorized under the jurisdictional liberality of the amended Rule, and in light of the dearth of precedent guiding the procedural innovation of countering hackers with hacks and the obscure horizons of the permissible scope of authorized seizures, the deferring of such questions is unsatisfactory. This is particularly so where the first case to discuss an application for a "network investigative techniques" warrant concluded that the request had to be denied on constitutional grounds. See *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 758-61 (S.D.Tex. 2013). The fact that there is almost no case law under subsection (b)(3), the terrorism clause, after more than a decade further suggests that reliance on later litigation is not a solution in this context. Motions to suppress are no answer, when the "good faith" exception to the exclusionary rule validates nearly any search conducted under a facially valid warrant. (Moreover, as described below, many of the resulting invasions of privacy will involve searches of computers belonging to bystanders; no person who is later accused will necessarily even have standing to challenge the search.) The proposed amendment thus constitutes a *de facto* grant of power unaccompanied by any framework of restraint. Only a Title III-like statutory regime, not a Rule amendment, can provide what is needed to render such searches reasonable in the context of the often unfamiliar and always transforming digital domain.

The NACDL respects the need for evolution in our criminal procedural rules designed to preserve their traditional purpose and function in changing times. In the face of evolving demands, it is certainly within the reach of this committee to make incremental, graduated and moderate changes in Rule 41 that pull up short of a constitutional, technological and diplomatic cliff. In this instance, however, the fact that the Rule presently does not always authorize a Magistrate Judge to issue a warrant to search the whole of the Internet to locate a computer that is being surreptitiously used to commit some federal offense is not a flaw or weakness in the Rule; rather, it is a

reflection of the fact that such searches by their nature pose threats to the protected privacy interests of an unknown number of innocent persons, require special regulation as to scope, and pose special problems with respect to the constitutional requirement of particularity that cannot be addressed with a simple Rules amendment.

Other submissions and letters to the Committee have identified many of these inherent dangers. Some have set out proposals for additional language that would establish additional limits upon the scope and impact of the proposed Rule change. Technologists have identified and explained why so radical a change in the scope of network search and seizure urgently demands extensive legal controls – defined legislatively and enforced judicially – over the use of "network intervention techniques." This is especially so where all the effects of deploying these search methods cannot be anticipated and in some respects are not even fully understood.[1] Internet privacy advocates have sounded alarms that place the present problem in the larger context of how the Fourth Amendment applies in the digital realm.[2]

The proposed restrictive clauses – which would be codified as Rules 41(b)-(6)(A) and (B) – do not serve to limit the scope or cabin the danger nearly enough.

To begin with, the introductory language would permit a warrant authorizing remote access to search and seize electronic storage media and information outside a district to be issued by a Magistrate Judge "in any district where activities related to a crime may have occurred." This, of course, is essentially no restriction at all. First, the speculative phrase "activities related to a crime may have occurred," which is derived from the PATRIOT Act provision, has yet to be judicially limited in any way. What is "activity" that is "related to" a crime? It is not even clearly limited to "criminal activity." Does it require that the warrant application include a showing upon which the Magistrate Judge could find reason to believe that venue for prosecution of the suspected offense might later properly be found in that District? Does it include victim impact that would not support venue? See *United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (extravagant government theory of

[1] *See* "Comments on Proposed Search Rules" submitted by Steven M. Bellovin, Matt Blaze, and Susan Landau and "Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning 'Remote Access' Searches of Electronic Media" for elaborate detailing of government experience and practices deploying surveillance software.

[2] *See* Electronic Privacy Information Center, "Testimony and Statement for the Record," presented for the hearing held November 5, 2014; "Written Statement of The Center for Democracy & Technology," submitted October 24, 2014.

venue over computer crimes rejected). Does it mean a District through which an electronic communication may have traveled? If so, then not one of the 94 federal districts is ineligible for warrant-issuing jurisdiction over a crime alleged to have been committed through use the use of an anonymized device, or if the offense being investigated is a CAFAA violation and several target computers in various localities have been "damaged" in the trivial sense defined at 18 U.S.C. § 1030(e)(8). Since no single Internet-connected location in any District can be excluded as one that "may" have experienced activities related to the crime, a diligent Magistrate Judge assessing her jurisdictional authority could hardly come to any conclusion other than that jurisdiction resides with her. The fruits of the Internet, bitter or sweet, are accessible in every part of our Nation and across the world wherever an IP address is to be found, and any device can be linked, even unknowingly with any other (so long as even one user among many shares access to that device). The incentive that is created for zealous law enforcement officials to forum-shop for the most pliant Magistrate Judge is also apparent.

Unlike more measured and carefully considered legislative solutions to the inaccessibility of telephonic aural communications, which are equally opaque to investigators without intrusion into the technology of the device network, the proposed Rule change would not discriminate as to the gravity of the offense. Instead, a paragraph inserted into a procedural rule invokes the most invasive technological dragnet of digital information and communication ever granted by a non-FISA warrant and applies it across the entire range of federal crimes. Rule 41 as amended would offer federal agents the power to hack their way into any number of computers, servers, storage accounts, laptops, and flash drives once an anonymous address had been exposed, whether the offense under investigation is commercial production and distribution of child pornography or a hit-and-run collision in the Veterans Administration hospital parking lot.

We respectfully disagree with the premise of the proposed amendment that all crimes under federal investigation associated with any concealed location or content on the Internet, or which may involve minor even if inadvertent damage to five disparately located computers, can justify the same disregard of traditional jurisdictional concerns as do terrorism investigations. A procedural rule change that applies to all federal criminal investigations is far inferior to the Title III model of legislation that limits extreme network intrusion to a defined subset of serious offenses. *Cf.* 18 U.S.C. § 2516(1)(a)-(t).

By removing the district-specific jurisdictional standard the rule dismisses the foundational principle that due process has a "place" dimension. The responsibilities of U.S. Magistrate Judges bring them into the closest contact with the broadest spectrum of individuals in their communities. There is a

deeply rooted history in Anglo-American jurisprudence as to why we are judged by a jury of our peers, *see* U.S. Const., Art. III, § 2, cl. 3; Amend. VI; for the same reason, the seizure of our persons and property is only authorized by a judge who is a member of our own community. Local jurisdiction is local accountability and deference to the diversity of regions and communities of which each Federal District is comprised is not to be lightly dismissed. The digital world is no less immediate and no less geographical than the physical communities in which it resides. The Internet may be accessible anywhere, but everything on the Internet is also most certainly somewhere. As much as we hear about "the Cloud," every digital cloud sleeps on the ground. Digital systems and the content within them cannot escape local jurisdiction. The question is only whether we build upon or ignore the virtues of local jurisdiction as Rule 41 and our Constitution currently define it.

It is estimated that almost 85% of TOR (anonymized router) users are in countries other than the United States.[3] To the government's credit, it does not rely on this fact (which would arguably place most searches for unknown computers on the Internet outside of *any* Fourth Amendment and Rule 41 regulation; see *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990); *In re Terrorist Bombings of U.S. Embassies*, 553 F.3d 150 (2d Cir. 2008, as amended 2009)) to eschew warrants entirely. The conferring of search jurisdiction based upon the technological concealment of location guarantees that invasive and potentially destructive actions will be taken against computer systems and storage media located outside the United States, as well as within. Other commentators have articulated how ill-advised such violations of other nations' sovereignty may be.[4] The range of application for the "network investigative techniques" – a polite term for court-authorized government hacks – extends well beyond the clear-cut "worst cases" that the government naturally cites.

The proposed limitation of the new Rule to two particular sorts of cases affords little protection against the dangers of searches *for* (and then *of*) computers in unknown locations.

The first of the two alternative prerequisites for a warrant to remotely search a targeted computer is met when "the district where the media or information is located has been concealed through technological means." Rule 41(b)(6)(A). Much of the Committee's concern is focused upon the technology of rendering "anonymous" the identifying information that would reveal the Internet

[3] Tor, TOR Metrics: Users, Top-10 countries by directly connecting users," https://metrics.torproject.org (83.76% overseas in 2015).

[4] *See* Center for Democracy & Technology, *supra* note 2, at 3.

Protocol address of the targeted digital device. Law enforcement must have device-specific IP address information to determine the physical location, and thus, the jurisdiction where the computer and its contents are located. If the goal of this warrant were only to hack through whatever means of technological concealment deprived investigating agents of the location data needed to find the device agents wished to search, the language of the proposed rule would be simpler: the search would be specific to location information only, and *not* authorize accessing the information *after* the location information establishing jurisdiction was obtained. The location of the targeted computer is not obtained solely for the purpose of identifying jurisdiction. Location information is an intermediate objective to the search and seizure of the contents of a computer or storage media that has been concealed by its owner-administrator. The extraordinary search authorized by the proposed Rule thus far exceeds in scope the special justification that is proffered for allowing it.

A target computer's anonymity may invoke a (b)(6)(A) warrant issued from any district where "activity related to a crime may have occurred," but it is ordinary probable cause to believe that a crime "may have occurred" that allows the warrant. Anonymity alone does not in any way add to the probable cause for a Fourth Amendment-qualified search and seizure. At most, it justifies going to a Magistrate Judge who might otherwise not have jurisdiction. The global framework of governments, industries, scientists, political activists, health care and legal professionals all conceal digital identity for lawful, justifiable reasons. Comparatively few hidden secrets are actually secret crimes.

One conundrum presented by the proposed amendment to Rule 41 is what scope of search and seizure is actually granted once the location of the target computer and its contents has been identified. As proposed to be amended, nothing in the Rule would clearly require that the highly intrusive search be limited to ascertaining the concealed location, or even to searching the particular media discovered at that location. A statute could provide that sort of restriction. Instead, a warrant issued under the amended Rule could seemingly grant a free pass to whatever resources are accessible from the targeted device, on the theory that access privileges are a sort of "information" in a stored media.

Anonymizing methods prevent identification of source. The language of the proposed Rule, tied to the precise problem at hand (identifying the appropriate Magistrate Judge), states that the remote access technique may be employed only if the *location* of the "the media" or "information" was concealed. The qualifying predicate for (b)(6)(A) warrants excludes all circumstances in which only the *content* in a storage media has been

concealed (for example, encrypted), since that form of concealment does not prevent ascertaining the IP address and thus the location. Although this plain language interpretation is unlikely to be the farthest reach attempted under the proposed amendment, if this change to Rule 41 is adopted the language should be revised to clearly restrict the scope of the warrant-authorized search to that media and content whose location was concealed, and only for the purpose of ascertaining their location. The warrant should not permit the agent using remote access techniques to reach into others systems, drives, computers and the like, nor to search or seize contents of computers that may have been concealed, other than location information for the device. (Similarly, information on a storage media that only cloaks the location of file content storage on the device media, such as steganographic measures,[5] should not trigger Rule 41(b)(6)(A) – or be the object of such a search – because such measures do not conceal the federal district in which the information is located.) Even on an anonymous server, any mode of concealment of media or information not disguising "the district where the media or information has been concealed" should not be subject to the remote access techniques of law enforcement under this proposed rule change.

The amendment should not be adopted unless revised to ensure that other computers connected to the anonymized computer cannot be within the scope of a warrant specially authorized under Rule 41(b)(6)(A). Accessibility from an anonymous device does not bestow anonymity upon all devices that it accesses. The proposed Advisory Committee Note likewise does not elaborate on the scope of its allowable or intended use. Again, we suggest that such limitations, while necessary, are more appropriately provided in a statute, which would not be restricted to provisions that can be called merely procedural.

The second proposed limiting class of cases, under Rule 41(b)(6)(B), raises equally problematic issues. The condition specified – that computers located in five or more different districts have been "damaged" – logically would seem to justify the proposed remedy – that is, allowing issuance of the warrant by a Magistrate Judge in any affected district – only if the investigative technique to be authorized is anticipated to involve a search of those numerous victim computers. Otherwise, why would the thing to be searched be considered to be outside the District? In other words, the persons whose privacy is to be invaded with tools of unknown (but predictably harmful) effect are putative victims, not even suspects much less probable perpetrators.

---

[5] Steganography is technique of concealment in which one type of message or file is hidden within another of a different type, such as concealing a text message, image, or video inside a computer file of a different type or format.

There are many discrete attacks in which the use of network investigative technology can identify and countermand the illicit requisitioning of computing resources and their use in criminal enterprises within the scope of 18 U.S.C. § 1030(a)(5) investigations. Beyond the "Botnet" example offered to the committee is any number of far more subtle and nuanced scenarios that will be tempting to solve with "network investigations" rather than more common police work where the boundaries of appropriate methods are well established. The limitation suggested at proposed (b)(6)(B) is therefore not a meaningful or effective restraint on the power that would be affirmed by this amendment.

The government's original proposal for a change to Rule 41 came in response to Magistrate Judge Stephen Wm. Smith's ruling in *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753 (S.D.Tex. 2013), where an FBI application for a warrant was denied. In references to this ruling before the Committee, the shorthand version of the holding focused on Rule 41 and the question of jurisdiction to issue a warrant to locate and then to search (and otherwise intrude) within an anonymized computer. That was one point that Judge Smith made, *id.* 756-58, but the opinion is more concerned with the FBI application's not satisfying the requirements of the Fourth Amendment, including the enabling of video surveillance through the target computer's built-in camera feature. *Id.* 758-61. Judge Smith's opinion reflects the problem that the Internet is not an amorphous area to be searched at large, but rather a vast community of persons utilizing technology to support an exchange of ideas, of commerce, and of invention, as well as sometimes being a repository of evidence of crime. The many particular uses to which each individual's own computer may be put require a careful measure of Fourth Amendment scrutiny.

It is surely possible to craft a constitutionally compliant procedure for searches in the virtual domain, but probably not within the confines of rulemaking. NACDL suspects that this *modus operandi* may require a series of graduated steps of iterative warrant applications as an investigation reveals the specific articles that are within reach of probable cause. This is analogous to the process under Title III, where 30-day reports are provided to justify renewals of a wiretap or extension of the tap to another phone number. Applying the guidance of the Supreme Court found in the *Berger* opinion, a legislative approach would be more apt. If, in the application of a procedural rule, a magistrate cannot know *a priori* the geographical reach, the ultimate scale, or the number of searches she is authorizing, a finding that Fourth Amendment requirements have been met is improbable. The proposed Rule 41 changes would inevitably send the opposite message, with the imprimatur of the federal judiciary. Because the very circumstances that

make problematic ascertaining the proper District within which a Magistrate Judge has jurisdiction are those which cause any digital search that could be authorized by an ordinary warrant to be open-ended and thus constitutionally unmanageable, the amendment should be rejected as currently drafted.

We thank the Committee for its efforts to improve our justice system and for this opportunity to contribute our thoughts.

Respectfully submitted,
THE NATIONAL ASSOCIATION
OF CRIMINAL DEFENSE LAWYERS

By: Samuel A. Guiberson
New York City, NY

*For the NACDL Committee on the Fourth Amendment*

Peter Goldberger
Ardmore, PA

William J. Genego
Santa Monica, CA

*Co-Chairs, Committee on Rules of Procedure*

*Please respond to:*
Peter Goldberger, Esq.
50 Rittenhouse Place
Ardmore, PA 19003
E: peter.goldberger@verizon.net