

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

vs.

Case No. 16-CR-38 (DEJ)

MARCUS A. OWENS,

Defendant.

**MOTION TO SUPPRESS BASED ON ISSUING MAGISTRATE JUDGE'S
LACK OF JURISDICTION**

As described in Mr. Owens's other motions, this case involved the execution of a historically unprecedented search warrant. Based on the government's interpretation, geographic boundaries fell aside. The warrant gave it the power to secretly search and alter over 100,000 computers anywhere in the world.

Whether the magistrate judge who signed this warrant was aware that the government would interpret it so expansively is unknown. But what is established is that if the warrant was geographically unlimited (as the government contends), it plainly violated Rule 41(b) of the Federal Rules of Criminal Procedure. What's more, this violation wasn't ministerial, like many Rule 41 violations. Based on the interplay between the Federal Magistrates Act and Rule 41, the magistrate judge

*Federal Defender Services
of Wisconsin, Inc.*

lacked the legal authority (the jurisdiction) to approve such a warrant.

This means that the warrant was invalid from the moment it was signed or, to use the Latin, void ab initio. An invalid warrant is, legally, no warrant at all. The government also knew that federal law did not permit the warrant it sought when it filed the application. So no good faith exception can or should apply. This Court should suppress all evidence derived from the original warrant, including the items taken from Mr. Owens's home and his statements to law enforcement.

Legal Background

The overall facts of this case are addressed in Mr. Owens's other motions. So the defense will briefly discuss the legal background underlying the issue raised below.

As the Court is likely aware, magistrate judges are creatures of statute. Congress created the positions in the Federal Magistrates Act of 1968, due to concerns about the overwhelming workload of federal district judges. *See* Federal Magistrates Act of 1968, Pub. L. No. 90-578, § 101 (1968). The act has been amended over the years, but it has always had a core section laying out the explicit powers of magistrate judges. *See* 28 U.S.C. § 636 (section titled "Jurisdiction, powers, and temporary assignment"). That section lists their various powers, including the power to sentence petty offenders, to hear pretrial matters (like this motion) when

designated by a district judge, and to preside over civil cases by consent. *See id.* Notably, the statute says nothing about search warrants. Rather, it states that magistrate judges have “all powers and duties” conferred “by the Rules of Criminal Procedure.” *See* 28 U.S.C. § 636(a)(1).

Only one Federal Rule of Criminal Procedure addresses a magistrate judge’s powers with regard to search warrants: Rule 41 of the Federal Rules of Criminal Procedure. Subsection (b) of that rule is titled “Authority To Issue A Warrant.” Fed. R. Crim. P. 41(b). As one would expect, it lists the situations where a magistrate judge has power to issue a warrant, describing different situations in each subsection. *Id.* And each subsection gives particular territorial limits. *See id.* at (b)(1)-(2) (“in this district”). That makes sense because magistrate judges work in specific districts and, except in “emergency” situations, can act only within their own districts. *See* 28 U.S.C. § 636(f). Rule 41(b) thus operates as an extension of the Federal Magistrates Act, along with the other Federal Rules of Criminal Procedure. In short, Rule 41(b) further itemizes a magistrate judge’s powers.

During the last few years, the government has sought to amend Rule 41 to give magistrate judges the ability to approve expansive online searches without regard to territorial limits. *See* Shannon Grammel, *Tor No More? Supreme Court*

Approves New Exception to Warrant Rule, The Stanford Daily (May 5, 2016).¹ That amendment is not yet effective, and may never become effective, since some members of Congress have objected to the proposed expansion. See Kate Conger, *Senators introduce bill to block controversial change to government hacking rule*, Tech Crunch (May 19, 2016).² This is the current legal landscape before the Court.

Argument

I. If the NIT warrant allowed searches anywhere in the world, then the magistrate judge lacked jurisdiction to issue it, as shown by Rule 41 and the Federal Magistrates Act.

As described in Mr. Owens's other motion to suppress, the NIT warrant authorized searches only in the Eastern District of Virginia. If the government nevertheless contends that the NIT warrant authorized searches of computers anywhere in the world, despite the warrant's plain language, then it must confront a different set of issues that also lead to suppression.

A. The NIT warrant plainly violated the territorial limits of Rule 41(b).

Rule 41(b) generally forbids a magistrate judge in one district from authorizing a search in another district. See *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) ("*In re Warrant*")

¹ Available at <http://www.stanforddaily.com/2016/05/05/tor-no-more-supreme-court-approves-new-exception-to-warrant-rule/>.

² Available at <https://techcrunch.com/2016/05/19/senators-to-block-controversial-hacking-rule-41/>.

(rejecting a NIT malware warrant application because issuing the warrant would have violated Rule 41). A few limited exceptions apply, but none are applicable in this case, as the rule's plain language shows, as other Courts have already held, and as will be discussed further below. *See id.*; Ex. A, *United States v. Levin*, Case No. 15-CR-10271-WGY, Doc. 69, at 9-14 (D. Mass. April 20, 2016) (none of Rule 41(b)'s territorial exceptions applied to Playpen NIT warrant, suppressing evidence); Ex. B, *United States v. Arterbury*, Case No. 15-CR-182-JHP, Doc. 42 (N.D. Ok. Apr. 25, 2016) at 9-17 (same); *see also* Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 Akron L. Rev. 315, 342 (2015) (discussing how the territorial exceptions to Rule 41(b) don't appear to apply to NIT-style warrants).

1. *The plain language of Rule 41(b) does not permit the search that occurred in this case.*

To begin, the government's violation of Rule 41(b) is plain from the face of the rule. Specifically, the rule allows magistrate judges to issue warrants to (1) search or seize property within the magistrate judge's judicial district; (2) search or seize property outside the district if the property is within the district when the warrant is issued, but might move outside the district before execution; (3) search or seize property in or outside the district if the investigation relates to terrorism; (4) install "within the district" a tracking device; or (5) search or seize property

that is within a U.S. territory, possession, or commonwealth, or is property owned or used by the U.S. government. *See* Fed. R. Crim. P. 41(b). The rule does not allow a magistrate judge to authorize searches or seizures in other districts in regular criminal investigations. *See id.*

In this case, the government has interpreted the warrant as giving it the power to search any computer anywhere. Since this was not a terrorism case, such a search was not permitted by Rule 41(b).

2. *In re Warrant explains why Rule 41(b) does not permit this exact type of search.*

The careful analysis *In re Warrant* explains why the search in this case exceeded the authority of Rule 41(b). In that case, the government was investigating a fraud and identity theft case perpetrated with an “unknown computer at an unknown location.” *In re Warrant*, 958 F. Supp. 2d at 755. Like the warrant here, the warrant sought in that case would have “surreptitiously install[ed] data extraction software” on a computer somewhere in the world using an older version of the NIT that was used to seize evidence from Mr. Owens’s home computer. *Id.*

The government contended that Rule 41(b)(1) permitted the search, which “allows a ‘magistrate judge with authority in the district . . . to issue a warrant to

search for and seize a person or property located within the district.’” *In re Warrant*, 958 F. Supp. 2d at 756 (quoting Rule 41). Although it didn’t know where the target computer was, the government claimed that “this subsection authorizes the warrant ‘because information obtained from the Target Computer will first be examined in this judicial district.’” *Id.* (quoting warrant application).

Not surprisingly, the court rejected the government’s novel theory that a search did not occur until investigators “examined” whatever information they had already seized. “Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location.” *Id.* at 757. The search and seizure of data occurs “not in the airy nothing of cyberspace, but in physical space with a local habitation and a name.” *Id.* Accordingly, the warrant sought by the Government would have permitted “FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district.” *Id.* at 757. Since the search for and collection of digital evidence would occur on a computer that might be located outside the district, the court concluded that a warrant was not permitted under Rule 41(b)(1) (or any other provision of the Rule).

In the present case, the government’s warrant application was less direct

about its actual targets. (The defense's contention, as described in Mr. Owens's other motion to suppress, is that the warrant authorized a search of a "person or property in the Eastern District of Virginia," not anywhere else.) Only after closely reading the entire lengthy warrant application can one discern that the FBI server in Virginia that was running the "Target Website" was not a search location at all, and the actual "place to be searched" could potentially include thousands of "activating computers" all over the world. Given these facts, the conclusion in *In re Warrant* that "the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)" is equally applicable here. *Id.* at 757.

In re Warrant is not controlling precedent. But its analysis is not only persuasive, it follows the plain language of Rule 41 and dealt with a similar request to what the Government asked for in this case. The conclusion is as manifest here as it was in *In re Warrant*: "the Government's application cannot satisfy the territorial limits" of Rule 41(b). *Id.* at 757.

3. *Other federal courts considering this same warrant have already held that it violated Rule 41(b).*

Presented with the same warrant at issue in this case, other courts have agreed. For example, a district court in Massachusetts concluded this spring that the warrant fell under none of Rule 41(b)'s current subsections. Ex. A at 9-14. Its

reasoning is thorough, and that court's decision is attached as an exhibit to this motion. *Id.* Similarly, three months ago a magistrate judge in the Northern District of Oklahoma reached the same conclusion. Ex. B at 15-18. (That report and recommendation was adopted by a district judge this May.) Several other courts have also reached the same conclusion. See *United States v. Werdene*, No. 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (holding that "Rule 41 did not authorize the issuance of the warrant in Virginia"); *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016) (same). This Court should do likewise.

4. *The government's efforts to amend Rule 41(b) and its statements about that rule show that it knew that the search in this case was impermissible.*

Finally, the conclusion that the warrant (given the government's reading) doesn't fit under Rule 41(b) is further cemented by the DOJ's long-standing efforts to amend that rule. See Grammel, *Tor no more?*, *supra*. The requested amendment would give magistrate judges the explicit power to permit the exact type of searches conducted in this case. Indeed, the DOJ made its request to amend the rules explicitly because of the *In re Warrant* decision. See Ex. C, Letter from Assistant Attorney General Mythili Raman to the Hon. Reena Raggi, at 2 (Sept. 18, 2013) (citing *In re Warrant*). In its request, the government admits that many

electronic searches do not seem to fit under Rule 41(b). *See id.* at 2-3 (acknowledging the need under the current rules “to coordinate” on warrants in multiple jurisdictions as part of one investigation). This stands as further proof that Rule 41(b) did not authorize the searches that occurred in this case.

In sum, the magistrate judge lacked authority under Rule 41(b) to grant the search conducted by the government.

B. Under the Federal Magistrates Act, the magistrate judge lacked legal authority to issue the NIT warrant and the evidence derived from it must be suppressed.

As this Court and Judge Pepper discussed previously in *United States v Epich*, the Seventh Circuit rule regarding Rule 41 violations is the harshest in the country: its precedent suggests that the rules are essentially unenforceable after a warrant has been issued, because no violations will result in suppression of evidence. Given this law, both this Court and Judge Pepper previously ruled that any Rule 41 violation stemming from the NIT warrant could not result in suppression.

But this position overlooks two matters. The Seventh Circuit’s statements that Rule 41 violations do not lead to suppression have not come in cases where the territorial restrictions of Rule 41(b) were violated. Rather, the cases have dealt with ministerial and procedural requirements. *See United States v. Cazares-Olivas*, 515 F.3d 726, 728 (7th Cir. 2008) (violation of Rule 41(e)(3)(A), requiring reading of

a “proposed duplicate original warrant” to magistrate); *United States v. Trost*, 152 F.3d 715, 721 (7th Cir. 1998) (violation of Rule 41(d), requiring prompt returns of warrant, and Rule 41(a), requiring that federal officer or attorney apply for warrant). Second and more importantly, the Seventh Circuit has not discussed the fact that, under the Federal Magistrates Act, a magistrate judge who issues a warrant in violation of Rule 41(b) acts *without jurisdiction*. This situation is rare, and a far more serious error.

As described above, magistrate judges have specifically circumscribed powers. *See* 28 U.S.C. § 636(a). Specifically, the law gives a magistrate judge the power to act: (1) “within the district” court where he or she has been appointed, (2) “at other places where that court may function,” and (3) as elsewhere authorized by statute, noting the powers of the Federal Rules of Criminal Procedure. *Id.*

With regard to the Eastern District of Wisconsin, the NIT warrant fell within none of these three categories. If the Eastern District of Virginia magistrate judge intended to allow searches in Wisconsin, then she did not act “within the district” where she had been appointed. The Eastern District of Wisconsin is not one of the alternate “places where that court may function.” *See United States v. Krueger*, 809 F.3d 1109, 1121 (10th Cir. 2015) (Gorsuch, J., concurring) (explaining that this

language was enacted after Hurricane Katrina, to assist federal judges based in Louisiana).

Nor was the magistrate judge authorized by some other law or rule to issue warrants that authorized searches far outside the Eastern District of Virginia. *See, e.g. id.* at 1117-24 (explaining that warrant issued by magistrate judge in the District of Kansas for a search in the District of Oklahoma violated § 636(a), and that the magistrate judge lacked jurisdiction to issue the warrant). As explained above and as held by other courts, § 636 doesn't grant magistrate judges broad search warrant powers. Those powers come through Rule 41(b) only. So when magistrate judges exceed the limits of Rule 41(b), they act without legal authority.

What's more, § 636(a) is a jurisdictional rule, and therefore a violation of that statute is more harmful than just a rule violation or even a regular statutory violation. *See Krueger*, 809 F.3d at 1122 (“[I]f §636(a)'s territorial restraints aren't jurisdictional, I struggle to image statutory restraints that would be.”). This jurisdictional nature of this rule is shown in many ways.

First, the title of the statute itself reads “Jurisdiction, powers, and temporary assignment.” *See* 28 U.S.C. § 636. That strongly suggests that the statute lays out magistrate judges' jurisdiction. Second, jurisdictional statutes deal with “statutory or constitutional power to adjudicate.” *Steel Co. v. Citizens for a Better Env't*, 523 U.S.

83, 89 (1998). That's precisely what § 636(a) addresses – the power of magistrate judges to act. Third, that provision is found within Title 28, the same title that contains other jurisdictional statutes. *See* 28 U.S.C. §§ 1331, 1332. Fourth and finally, other federal courts have concluded that § 636(a) is a jurisdictional statute, including the Seventh Circuit. *See, e.g., Pelton Casteel, Inc. v. Marshall*, 588 F.2d 1182, 1186 (7th Cir. 1978) (§ 636(a) establishes magistrate's jurisdiction); *N.L.R.B. v. A-Plus Roofing, Inc.*, 39 F.3d 1410, 1415-16 (9th Cir. 1994) (same); Ex. A at 18, n.11; *see also Krueger*, 809 F.3d at 1123 (Gorsuch, J. concurring).

So this Court is presented with a situation where the magistrate judge who issued the NIT warrant lacked jurisdiction to do so. (Assuming that the warrant can be read to permit searches outside of the Eastern District of Virginia.) In such cases, the warrant is viewed as “void ab initio,” meaning invalid from the beginning. *See United States v. Houston*, No. CRIM.A. 3:13-09-DCR, 2014 WL 259085, at *26, n.14 (E.D. Tenn. Jan. 23, 2014) (“A search warrant issued by an individual without the legal authority to do so is “void ab initio,” which means that the Court never reaches the question of whether the search warrant is supported by probable cause.” (citation omitted)); *see also United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013) (the language of Rule 41(b)(2) is “crystal clear” and a “jurisdictional flaw” in the warrant cannot be excused as a “technical defect”); *United States v. Scott*, 260

F.3d 512, 515 & n. 2 (6th Cir.2001) (search warrant signed by a retired state judge “wholly without legal authority to issue a warrant” under state law was void ab initio) (*overruled on other grounds*); *Fed. Sav. & Loan Ins. Corp. v. PSL Realty Co.*, 630 F.2d 515, 521 (7th Cir. 1980) (“It is equally settled that where, as here, the court lacks jurisdiction to adjudicate the principal matter, its orders . . . are likewise beyond its jurisdiction and as such are void ab initio.”). With a void warrant, “the search stands on no firmer ground than if there had been no warrant at all.” *Coolidge v. New Hampshire*, 403 U.S. 443, 453 (1971) (holding that state official lacked power to issue search warrant and suppressing evidence). No exception to the warrant requirement applies to this case, and the evidence should be suppressed.

C. Evidence seized under this jurisdiction-less and void warrant should be suppressed.

The Government will presumably argue that suppression is too strong of a remedy for its reliance on a void warrant. But other courts that have examined this issue have concluded otherwise. Looking at this same warrant, and considering this same issue, District Judge Young in the District of Massachusetts held that suppression was required for two reasons. First, he noted that it was an open questions whether the good faith exception in *United States v. Leon*, 468 U.S. 897 (1984), applies to warrants issued without jurisdiction. He analyzed the issue and

held that it should not apply. *See* Ex. A at 24-31. Second, he explained that even if the good faith exception might apply to such jurisdiction-less warrants, that exception should not apply here. *Id.* at 32-33.

Indeed, no good faith exception should apply in this case, whatever the issue at hand. As Judge Young persuasively explains: “it was not objectively reasonable for law enforcement—particularly a ‘veteran FBI agent with 19 years of federal law enforcement experience’ . . . to believe that the NIT warrant was properly issued considering the plain mandate of Rule 41(b).” *Id.* at 32. The government’s letter to the rules committee also showed that it *knew* that Rule 41(b) didn’t permit what it wanted to do. *See* Ex. C. But it apparently didn’t care. It submitted the warrant application to the magistrate judge, packaged its request in a confusing way, and hoped that the warrant would get approved. When the magistrate judge signed off, the government was off to the races, despite knowing what Rule 41(b) requires.

When such obvious problems exist with the warrant (and the violation of Rule 41(b) was obvious given *In re Warrant* and the pending efforts to amend the rule), the Government cannot be said to have operated in “good faith.” It knew better. *See United States v. Slaey*, 433 F. Supp. 2d 494, 499 (E.D. Pa. 2006) (suppressing evidence when prosecutor obtained magistrate’s authorization not

to leave attachments to the warrant with the subject because “it was not reasonable for the agent to rely on a Magistrate Judge’s order authorizing him to disregard Rule 41(f)(3)(B)”. No good faith exists in this case, and the evidence derived from this void warrant should be suppressed.

Conclusion

The justice system criminal depends on trust, particularly the ability of the public, the courts, and the defense bar to trust the government. Courts rely on the government and particularly prosecutors, as quasi-judicial officers, to follow the letter of the law, to prevent errors before they occur, and to not conceal legal issues. That didn’t happen in this case. The government knew that Rule 41(b) didn’t permit the search it sought to conduct. Yet it requested the search warrant anyway, and failed to flag the issue for the magistrate judge.

Of course, with an amendment to Rule 41(b) pending, one could be tempted to write off what happened here as no big deal. But the principle is crucial: the government cannot ignore the law simply because it finds complying inconvenient or impractical. *See* Ex. C at 3 (referring to Rule 41(b) as “an unnecessary obstruction”). Its choices here led to the magistrate judge exceeding her jurisdiction, and the government searching thousands of people under a void warrant. The evidence derived from that void warrant should be suppressed.

Dated at Milwaukee, Wisconsin this 1st day of August, 2016.

Respectfully submitted,

/s/ Anderson M. Gansner

Anderson M. Gansner, Bar No. 1082334

FEDERAL DEFENDER SERVICES

OF WISCONSIN, INC.

517 E. Wisconsin Avenue, Room 182

Milwaukee, Wisconsin 53202

Telephone: 414-221-9900

Fax: 414-221-9901

E-mail: anderson_gansner@fd.org

Counsel for Defendant, Marcus A. Owens

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

<hr/>)	
UNITED STATES OF AMERICA,)	
)	
)	
)	
	v.)	CRIMINAL ACTION
)	NO. 15-10271-WGY
ALEX LEVIN,)	
)	
	Defendant.)	
<hr/>)	

YOUNG, D.J.

April 20, 2016

MEMORANDUM & ORDER

I. INTRODUCTION

Alex Levin is charged with possession of child pornography. Compl. 1, ECF No. 1. The government obtained evidence of Levin's alleged crime in three steps. First, it seized control of a website that distributed the illicit material at issue ("Website A"). Next, it obtained a series of search warrants that allowed the government to identify individual users who were accessing content on Website A. One of these warrants involved the deployment of a Network Investigative Technique (the "NIT Warrant"). Finally, the government searched¹ the computers of certain of these individuals, including Levin.

¹ The government has waived any argument that its investigative conduct here did not amount to a search by failing to raise this argument in its memorandum. The Court therefore assumes that Levin had a reasonable expectation of privacy as to

[1]

Levin has moved to suppress the evidence obtained as a result of the issuance of the NIT Warrant, arguing that the NIT Warrant is void for want of jurisdiction under the Federal Magistrates Act, 28 U.S.C. § 636(a), and additionally that it violated Federal Rule of Criminal Procedure 41(b). Def.'s Mot. Suppress Evidence ("Def.'s Mot.") 5-6, ECF No. 44. The government contends that the NIT Warrant was valid and that, in any event, suppression is not an appropriate remedy on these facts. Gov't's Resp. Def.'s Mot. Suppress ("Gov't's Resp.") 1, ECF No. 60.

II. FACTUAL BACKGROUND

This case involves a far-reaching and highly publicized investigation conducted by the Federal Bureau of Investigation in early 2015 to police child pornography.² The investigation focused on Website A, which was accessible to users only through

the information obtained through the execution of the various warrants.

² For coverage of this investigation, see, for example, Ellen Nakashima, This is How the Government is Catching People Who Use Child Porn Sites, Wash. Post, Jan 21, 2016, https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902_story.html; Mary-Ann Russon, FBI Crack Tor and Catch 1,500 Visitors to Biggest Child Pornography Website on the Dark Web, Int'l Bus. Times, Jan. 6, 2016, <http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417>.

the "Tor" network -- software designed to preserve users' anonymity by masking their IP addresses.³ See Def.'s Mot., Ex. 3, Aff. Supp. Application Search Warrant ("Aff. Supp. NIT Warrant") 10-12, ECF No. 44-3.

As an initial step in their investigation, FBI agents seized control of Website A in February 2015. See id. at 21-23. Rather than immediately shutting it down, agents opted to run the site out of a government facility in the Eastern District of Virginia for two weeks in order to identify -- and ultimately, to prosecute -- users of Website A. See id. at 23. To do this

³ "Tor," which stands for "The Onion Router," is "the main browser people use to access" the "Darknet" -- "a specific part of th[e] hidden Web where you can operate in total anonymity." Going Dark: The Internet Behind the Internet, Nat'l Pub. Radio, May 25, 2014, <http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet>. Tor itself is lawful and has various legitimate uses. See id. Indeed, it was developed by the United States Navy, which continues to use it "as a means of communicating with spies and informants[.]" John Lanchester, When Bitcoin Grows Up, 28 London R. Books No. 8, <http://www.lrb.co.uk/v38/n08/john-lanchester/when-bitcoin-grows-up>. Tor has, however, produced difficulties for law enforcement officials, "especially those pursuing child pornography, Internet fraud and black markets," since it allows criminals to evade detection. Martin Kaste, When a Dark Web Volunteer Gets Raided by the Police, Nat'l Pub. Radio, April 4, 2016, <http://www.npr.org/sections/alltechconsidered/2016/04/04/472992023/when-a-dark-web-volunteer-gets-raided-by-the-police>; see also Lanchester, supra (describing Tor as "the single most effective web tool for terrorists, criminals and paedos" and noting that it "gives anonymity and geographical unlocatability to all its users"). At the same time, its legal users have raised concerns about the privacy implications of government "sting" operations on the Tor network. See Kaste, supra.

required the deployment of certain investigative tools. See id. at 23-24.

To that end, the government sought and obtained a series of warrants. First, on February 20, 2015, the government procured an order pursuant to Title III from a district judge in the Eastern District of Virginia permitting the government to intercept communications between Website A users. Def.'s Mot., Ex. 2 ("Title III Warrant"), ECF No. 44-2. Second, also on that date, the government obtained a warrant from a magistrate judge in the Eastern District of Virginia to implement a Network Investigative Technique ("NIT") that would allow the government covertly to transmit computer code to Website A users.⁴ NIT Warrant, ECF No. 44-3. This computer code then generated a communication from those users' computers to the government-operated server containing various identifying information, including those users' IP addresses.⁵ See Aff. Supp. NIT Warrant 24-26.

⁴ For a discussion of the government's recent use of these types of warrants, see Brian L. Owsley, Beware of Government Agents Bearing Trojan Horses, 48 Akron L. Rev. 315 (2015).

⁵ The affidavit the government submitted in support of its application for the NIT Warrant describes this process:

In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant,

Through the use of the NIT, government agents determined that a Website A user called "Manakaralupa" had accessed several images of child pornography in early March 2015, and they traced the IP address of that user to Levin's home address in Norwood, Massachusetts. Def.'s Mot., Ex. 1 ("Residential Warrant"), Aff. Supp. Application for Search Warrant ("Aff. Supp. Residential

[Website A], which will be located . . . in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from [Website A] . . . the instructions, which comprise the NIT, are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government.

Aff. Supp. NIT Warrant 24. The particular information seized pursuant to the NIT Warrant included:

1. the 'activating' computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other 'activating' computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the 'activating' computer;
5. the 'activating' computer's Host Name;
6. the 'activating' computer's active operating system username; and
7. the 'activating' computer's media access control ('MAC') address[.]

NIT Warrant, Attach. B (Information to be Seized).

Warrant") 11-12, ECF No. 44-1. On August 11, 2015, law enforcement officials obtained a third and final warrant (the "Residential Warrant") from Magistrate Judge Bowler in this District to search Levin's home. See Residential Warrant. Agents executed the Residential Warrant on August 12, 2015, and in their search of Levin's computer, identified eight media files allegedly containing child pornography. See Compl., Ex. 2, Aff. Supp. Application Criminal Compl. ¶ 7, ECF No. 1-2.

Levin was subsequently indicted on one count of possession of child pornography, 18 U.S.C. § 2252A(a)(5)(B). Indictment, ECF No. 8. He has since moved to suppress all evidence seized pursuant to the NIT Warrant and the Residential Warrant.⁶ Def.'s Mot. After holding a hearing on March 25, 2016, the Court took Levin's motion under advisement. See Elec. Clerk's Notes, ECF No. 62.

III. ANALYSIS

In support of his motion to suppress, Levin contends that the NIT Warrant violated the territorial restrictions on the issuing magistrate judge's authority,⁷ and further that the

⁶ The government does not contest Levin's argument that absent the NIT Warrant, it would not have had probable cause to support its Residential Warrant application, see Def.'s Mot. 14. For the sake of simplicity, the Court uses the phrase "evidence seized pursuant to the NIT Warrant" to include evidence seized pursuant to the Residential Warrant because all of that evidence is derivative of the NIT Warrant.

evidence obtained pursuant to the NIT Warrant must be suppressed in light of law enforcement agents' deliberate disregard for the applicable rules and the prejudice Levin suffered as a consequence. See Def.'s Mot. 6-7. The government refutes each of these arguments, and additionally argues that the good-faith exception to the exclusionary rule renders suppression inappropriate. See Gov't's Resp. 1.

A. Magistrate Judge's Authority Under the Federal Magistrates Act and Rule 41(b)

Levin argues that the issuance of the NIT Warrant ran afoul of both Section 636(a) of the Federal Magistrates Act and Rule 41(b) of the Federal Rules of Criminal Procedure. See Def.'s Mot. 5-7, 12. The conduct underlying each of these alleged violations is identical: the magistrate judge's issuance of a warrant to search property located outside of her judicial

⁷ A more precise characterization of Levin's challenge would be that the magistrate judge who issued the NIT Warrant had no authority to do so under the relevant statutory framework and federal rules -- not that the issuance of the warrant "violated" these provisions, by, for example, failing to comply with procedural requirements. In the Court's view, this distinction is meaningful, see infra Part III(B)(1), though it is one that neither the parties nor other courts evaluating similar challenges seem to appreciate, see, e.g., United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 at *5-*7 (W.D. Wash. Jan. 28, 2016) (discussing whether the NIT Warrant "violates" Federal Rule of Criminal Procedure 41(b)). In the interest of consistency with the parties' briefings and prior caselaw, however, the Court continues the tradition of referring to actions by a magistrate judge that fall outside the scope of her authority as "violations" of the provisions that confer such authority.

district. See id. Moreover, because Section 636(a) expressly incorporates any authorities granted to magistrate judges by the Federal Rules of Criminal Procedure, see infra Part III(A)(1), the Court's analyses of whether the NIT Warrant was statutorily permissible and whether it was allowed under Rule 41(b) are necessarily intertwined.

1. Federal Magistrates Act

Section 636(a) of the Federal Magistrates Act establishes "jurisdictional limitations on the power of magistrate judges[.]" United States v. Krueger, 809 F.3d 1109, 1122 (10th Cir. 2015) (Gorsuch, J., concurring). It provides, in relevant part:

(a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law--

(1) all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure[.]

28 U.S.C. § 636(a). Levin argues that the magistrate judge's issuance of a warrant to search property outside of her judicial district violated the territorial restrictions provided in the first paragraph of Section 636(a). Def.'s Mot. 12. In other words, because the NIT Warrant approved a search of property outside the Eastern District of Virginia ("the district in which sessions are held by the court that appointed the magistrate"),

and neither of the other clauses in the first paragraph of Section 636(a) applies, Levin contends that the magistrate judge lacked jurisdiction to issue it. See id. The government, for its part, notes that Levin does not meaningfully distinguish between the requirements of the statute and of Rule 41(b), and advances the same arguments to support the magistrate judge's authority to issue the NIT Warrant under Section 636(a) and under Rule 41(b). Gov't's Resp. 21.

As discussed in more detail infra Part III(A)(2)(i), the Court is persuaded by Levin's argument that the NIT Warrant indeed purported to authorize a search of property located outside the district where the issuing magistrate judge sat. The magistrate judge had no jurisdiction to issue such a warrant under the first paragraph of Section 636(a). The Court also concludes that Section 636(a)(1) is inapposite because Rule 41(b) did not confer on the magistrate judge authority to issue the NIT Warrant Levin challenges here, see infra Part III(A)(2), and the government points to no other "law or . . . Rule[] of Criminal Procedure" on which the magistrate judge could have based its jurisdiction pursuant to Section 636(a)(1), see infra note 11. Consequently, the Court holds that the Federal Magistrates Act did not authorize the magistrate judge to issue the NIT Warrant here.

2. Rule 41(b)

Rule 41(b), titled "Authority to Issue a Warrant,"

provides as follows:

At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge -- in an investigation of domestic terrorism or international terrorism -- with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises -- no matter who owns them -- of a United States diplomatic or consular mission in a foreign state, including any appurtenant

building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b).

The government argues for a liberal construction of Rule 41(b) that would authorize the type of search that occurred here pursuant to the NIT Warrant. See Gov't's Resp. 18-20.

Specifically, it argues that subsections (1), (2), and (4) of Rule 41(b) are each sufficient to support the magistrate judge's issuance of the NIT Warrant. Id. This Court is unpersuaded by the government's arguments. Because the NIT Warrant purported to authorize a search of property located outside the Eastern District of Virginia, and because none of the exceptions to the general territorial limitation of Rule 41(b)(1) applies, the Court holds that the magistrate judge lacked authority under Rule 41(b) to issue the NIT Warrant.

i. Rule 41(b)(1)

The government advances two distinct lines of argument as to why Rule 41(b)(1) authorizes the NIT Warrant. One is that all of the property that was searched pursuant to the NIT Warrant was actually located within the Eastern District of Virginia, where the magistrate judge sat: since Levin -- as a

user of Website A -- "retrieved the NIT from a server in the Eastern District of Virginia, and the NIT sent [Levin's] network information back to a server in that district," the government argues the search it conducted pursuant to the NIT Warrant properly can be understood as occurring within the Eastern District of Virginia. Gov't's Resp. 20. This is nothing but a strained, after-the-fact rationalization. In its explanation of the "Place to be Searched," the NIT Warrant made clear that the NIT would be used to "obtain[] information" from various "activating computers[.]"⁸ NIT Warrant 32. As is clear from Levin's case -- his computer was located in Massachusetts -- at least some of the activating computers were located outside of the Eastern District of Virginia. That the Website A server is located in the Eastern District of Virginia is, for purposes of Rule 41(b)(1), immaterial, since it is not the server itself from which the relevant information was sought. See United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 at *6 (W.D. Wash. Jan. 28, 2016) (examining the permissibility of the

⁸ That the cover page of the NIT Warrant application indicated that the property to be searched was located in the Eastern District of Virginia, see NIT Warrant 1, does not alter this conclusion. See Michaud, 2016 WL 337263 at *4 (observing that to read this NIT Warrant as authorizing a search of property located exclusively within the Eastern District of Virginia, on the basis of its cover page, is "an overly narrow reading of the NIT Warrant that ignores the sum total of its content.").

same NIT Warrant and concluding that Rule 41(b)(1) did not authorize the search "because the object of the search and seizure was Mr. Michaud's computer, not located in the Eastern District of Virginia").

The government's other argument is that where, as here, it is impossible to identify in advance the location of the property to be searched, Rule 41(b)(1) ought be interpreted to allow "a judge in the district with the strongest known connection to the search" to issue a warrant. See Gov't's Resp. 20. This argument fails, though, because it adds words to the Rule. See Lopez-Soto v. Hawayek, 175 F.3d 170, 173 (1st Cir. 1999) ("Courts have an obligation to refrain from embellishing statutes by inserting language that Congress opted to omit.").

ii. Rule 41(b)(2)

Rule 41(b)(2) confers on magistrate judges the authority "to issue a warrant of a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Fed. R. Crim. P. 41(b)(2). The government argues that because the NIT (i.e., the computer code used to generate the identifying information from users' computers) was located in the Eastern District of Virginia at the time the warrant was issued, this subsection applies. Gov't's Resp. 19. As discussed above, however, the

actual property to be searched was not the NIT nor the server on which it was located, but rather the users' computers. Therefore, Rule 41(b)(2) is inapposite.

iii. Rule 41(b)(4)

The Court is similarly unpersuaded by the government's argument regarding Rule 41(b)(4), which authorizes magistrate judges in a particular district "to issue a warrant to install within the district a tracking device," even where the person or property on whom the device is installed later moves outside the district, see Fed. R. Crim. P. 41(b)(4). The government likens the transmittal of the NIT to Website A users' computers to the installation of a tracking device in a container holding contraband, insofar as each permits the government to identify the location of illegal material that has moved outside the relevant jurisdiction. Gov't's Resp. 19-20. This analogy does not persuade the Court that the NIT properly may be considered a tracking device, regardless of where the "installation" occurred.⁹

⁹ Indeed, as the court pointed out in Michaud, which involved the same NIT Warrant:

If the 'installation' occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because [users of Website A] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on [the

B. Suppression

Having concluded that neither the Federal Magistrates Act nor Rule 41(b) authorized the issuance of the NIT Warrant, the Court now turns to the question of whether suppression of the evidence obtained pursuant to the NIT Warrant is an appropriate remedy. Levin argues that this evidence ought be suppressed because the magistrate judge lacked jurisdiction to issue the NIT Warrant and because Levin was prejudiced by the Rule 41 violation. Def.'s Mot. 13-14. The government argues that even if the issuance of the NIT Warrant was not sanctioned by Rule 41 or Section 636(a), suppression is too extreme a remedy, as any violation of the relevant rule or statute was merely ministerial and there was no resulting prejudice to Levin. Gov't's Resp.

individual Website A user's] computer, applying the tracking device exception again fails, because [the user's] computer was never physically located within the Eastern District of Virginia.

2016 WL 337263 at *6. In any case, the Court is persuaded by the Southern District of Texas's interpretation of "installation." See In re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d 753, 758 (S.D. Tex. 2013) (rejecting government's application for a warrant remotely to extract identifying information from a computer in an unknown location, noting that "there is no showing that the installation of the 'tracking device' (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet."). Under that approach, the "installation" of the NIT occurred not within the Eastern District of Virginia, where the server is located, but rather at the site of each user's computer. See id.

16. Further, the government contends that the good-faith exception to the exclusionary rule ought preclude suppression of the evidence seized. Id. at 21-23.

The Court concludes that the violation at issue here is distinct from the technical Rule 41 violations that have been deemed insufficient to warrant suppression in past cases, and, in any event, Levin was prejudiced by the violation. Moreover, the Court holds that the good-faith exception is inapplicable because the warrant at issue here was void ab initio.

1. Nature of the Rule 41 Violation

A violation of Rule 41 that is purely technical or ministerial gives rise to suppression only where the defendant demonstrates that he suffered prejudice as a result of the violation. See United States v. Bonner, 808 F.2d 864, 869 (1st Cir. 1986). The government apparently submits that all Rule 41 violations "are essentially ministerial," and accordingly that suppression is an inappropriate remedy absent a showing of prejudice. Gov't's Resp. 16 (citing United States v. Burgos-Montes, 786 F.3d 92, 109 (1st Cir. 2015)).

Rule 41, however, has both procedural and substantive provisions -- and the difference matters. Courts faced with violations of Rule 41's procedural requirements have generally found such violations to be merely ministerial or technical, and

as a result have determined suppression to be unwarranted.¹⁰ By contrast, this case involves a violation of Rule 41(b), which is “a substantive provision[.]” United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008); see also United States v. Krueger, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015) (noting that Rule 41(b)(1) “is unique from other provisions of Rule 41 because it implicates substantive judicial authority,” and accordingly concluding that past cases involving violations of other subsections of Rule 41 “offer limited guidance”) (internal quotation marks and citation omitted). Thus, it does not follow from cases involving violations of Rule 41’s procedural provisions that the Rule 41(b) violation at issue here -- which involves the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the

¹⁰ These violations implicate the various subsections of Rule 41, with the exception of subsection (b). See, e.g., Burgos-Montes, 786 F.3d at 108-09 (magistrate judge’s “failure . . . to define the time period of the search when the form itself provides that the search is to be completed within [10 days], and . . . failure to designate a magistrate to whom the form should be returned” was technical violation of Rule 41(e)); Bonner, 808 F.2d at 869 (officers’ failure to comply with Rule 41(f) requirement of leaving a copy of the warrant at the place to be searched was ministerial and did not call for suppression of resulting evidence); United States v. Dauphinee, 538 F.2d 1, 3 (1st Cir. 1976) (“The various procedural steps required by Rule 41(d) are basically ministerial[,]” and therefore suppression of evidence obtained in violation of that provision was not warranted absent showing of prejudice); United States v. Pryor, 652 F.Supp. 1353, 1365-66, (D. Me. 1987) (violation of Rule 41(c)’s procedural requirements regarding nighttime searches did not call for suppression).

warrant -- was simply ministerial. See United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013) (concluding that a Rule 41(b) violation constitutes a "jurisdictional flaw" that cannot "be excused as a 'technical defect'").

Because the violation here involved "substantive judicial authority" rather than simply "the procedures for obtaining and issuing warrants," Krueger, 809 F.3d at 1115 n.7, the Court cannot conclude that it was merely ministerial; in fact, because Rule 41(b) did not grant her authority to issue the NIT warrant, the magistrate judge was without jurisdiction to do so.¹¹ The government characterizes Levin's challenge as targeting "the location of the search, not probable cause or the absence of judicial approval." Gov't's Resp. 16. Here, however, because the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT Warrant, there simply was no judicial approval. See United States v. Houston, 965 F.Supp.2d 855, 902 n.12 (E.D. Tenn. 2013) ("A search warrant issued by an individual without

¹¹ For the magistrate judge to have had jurisdiction to issue the warrant under Section 636(a), she must have had authority to do so under Rule 41(b), as the government has pointed to no alternative statutory authority or federal rule that could serve as the basis for such jurisdiction. Moreover, the government's argument regarding courts' inherent authority to issue warrants, see Gov't's Resp. 20-21, does not extend to magistrate judges, whose authority derives from -- and is bounded by -- the specific statutory provisions and rules discussed herein.

legal authority to do so is 'void ab initio'") (quoting United States v. Master, 614 F.3d 236, 241 (6th Cir. 2010)); United States v. Peltier, 344 F.Supp.2d 539, 548 (E.D. Mich. 2004) ("A search warrant signed by a person who lacks the authority to issue it is void as a matter of law.") (citation omitted); cf. State v. Surowiecki, 440 A.2d 798, 799 (Mont. 1981) ("[A] lawful signature on the search warrant by the person authorized to issue it [is] essential to its issuance[,] such that an unsigned warrant is void under state law and confers no authority to act, despite existence of probable cause).

NITs, while raising serious concerns,¹² are legitimate law enforcement tools. Indeed, perhaps magistrate judges should have the authority to issue these types of warrants. See In re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d at 761 (noting that "there may well be a good reason

¹² The Court expresses no opinion on the use of this particular police tactic under these circumstances, but notes that its use in the context of investigating and prosecuting child pornography has given rise to significant debate. See, e.g., The Ethics of a Child Pornography Sting, N.Y. Times, Jan. 27, 2016, <http://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting>. The continuing harm to the victims of this hideous form of child abuse is the distribution of the photographs and videos in which the victims appear. See, e.g., United States v. Kearney, 672 F.3d 81, 94 (1st Cir. 2012) (internal citations omitted). Unlike those undercover stings where the government buys contraband drugs to catch the dealers, here the government disseminated the child obscenity to catch the purchasers -- something akin to the government itself selling drugs to make the sting.

to update the territorial limits of [Rule 41] in light of advancing computer search technology").¹³ Today, however, no

¹³ Whether magistrate judges should have the authority to issue warrants to search property located outside of their districts under circumstances like the ones presented here has been the subject of recent deliberations by the Advisory Committee on Criminal Rules. See Memorandum from Hon. Reena Raggi, Advisory Committee on Criminal Rules, to Hon. Jeffrey S. Sutton, Chair, Committee on Rules of Practice and Procedure ("Raggi Mem.") (May 5, 2014); Letter from Mythili Raman, Acting Assistant Attorney General, to Hon. Reena Raggi, Chair, Advisory Committee on the Criminal Rules ("Raman Letter") (Sept. 18, 2013); cf. Zach Lerner, A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, 18 Yale J. L. & Tech. 26 (2016). As Levin points out in his motion, see Def.'s Mot. 18-19, the following proposed amendment to Rule 41(b) is currently under consideration:

- (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
 - (A) the district where the media or information is located has been concealed through technological means; or
 - (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure 337-38 ("Proposed Rule 41 Amendment"), Committee on Rules of Practice and Procedure of the Judicial Conference of the United States (August 2014), <http://www.uscourts.gov/file/preliminary-draft-proposed-amendments-federal-rules-appellate-bankruptcy-civil-and-criminal>.

magistrate judge has the authority to issue this NIT warrant. Accordingly, the warrant here was void.

2. Prejudice

Even were the Court to conclude that the Rule 41(b) violation was ministerial, suppression would still be appropriate, as Levin has demonstrated that he suffered prejudice. See Burgos-Montes, 786 F.3d at 109 (a Rule 41 violation "does not require suppression unless the defendant can demonstrate prejudice") (emphasis added); cf. Krueger, 809 F.3d at 1117 (affirming district court's order granting defendant's motion to suppress "[b]ecause [the defendant] met his burden of establishing prejudice and because suppression furthers the purpose of the exclusionary rule by deterring law enforcement from seeking and obtaining warrants that clearly violate Rule

Proponents of the amendment contend that it ought be adopted in order "to address two increasingly common situations: (1) where the warrant sufficiently describes the computer to be searched but the district within which that computer is located is unknown, and (2) where the investigation requires law enforcement to coordinate searches of numerous computers in numerous districts." Raman Letter 1.

While the Advisory Committee on Criminal Rules unanimously approved the proposed amendment, Raggi Mem. 5, it has drawn criticism from stakeholders ranging from the American Civil Liberties Union, see Letter from American Civil Liberties Union to Members of the Advisory Committee on Criminal Rules (Oct. 31, 2014), to Google, see Letter from Richard Salgado, Director, Law Enforcement and Information Security, Google Inc., to Judicial Conference Advisory Committee on Criminal Rules (Feb. 13, 2015).

41(b)(1)"). "To show prejudice, defendants must show that they were subjected to a search that might not have occurred or would not have been so abrasive had Rule 41[] been followed."¹⁴

Bonner, 808 F.2d at 869. Here, had Rule 41(b) been followed, the magistrate judge¹⁵ would not have issued the NIT Warrant, and therefore the search conducted pursuant to that Warrant might

¹⁴ Courts outside this district faced with Rule 41(b) violations have considered (and in some cases, adopted) alternative formulations of the prejudice inquiry. See, e.g., Krueger, 809 F.3d at 1116 (evaluating government's proposed prejudice standard, "which would preclude defendants from establishing prejudice in this context so long as the [g]overnment hypothetically could have obtained the warrant from a different federal magistrate judge with warrant-issuing authority under the Rule"); Michaud, 2016 WL 337263 at *6-7. In Michaud, the court reasoned that the most "sensible interpretation" of the prejudice standard in this context is asking "whether the evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means[.]" 2016 WL 337263 at *6 (emphasis added). This Court respectfully declines to follow the Michaud court's approach, instead adhering to the prejudice standard generally applicable to Rule 41 violations. Cf. Krueger, 809 F.3d at 1116 (rejecting government's proposed prejudice standard, which "would preclude defendants from establishing prejudice in this context so long as the Government hypothetically could have obtained the warrant from a different federal magistrate judge with warrant-issuing authority under the Rule[,]" reasoning that "[w]hen it comes to something as basic as who can issue a warrant, we simply cannot accept such a speculative approach" and that instead the standard "should be anchored to the facts as they actually occurred").

¹⁵ This is not to say that a district judge could not have issued the NIT Warrant, since Rule 41(b) and Section 636(a) bear only on the authority of magistrate judges to issue warrants. See infra Part III(B)(4).

not have occurred.¹⁶ See Krueger, 809 F.3d at 1116 (holding that defendant suffered prejudice as a result of having been subjected to a search that violated Rule 41(b), since that search "might not have occurred because the Government would not have obtained [the warrant] had Rule 41(b)(1) been followed."). Contrast United States v. Scott, 83 F.Supp.2d 187, 203 (D. Mass. 2000) (Rule 41(d) violation did not prejudice defendant, since "the nature of the search would not have changed even if [the defendant] had been given a copy of the warrant prior to the search, as required under the rules); United States v. Jones, 949 F.Supp.2d 316, 323 (D. Mass. 2013) (Saris, C.J.) (law enforcement officer's failure to leave the defendant with a copy of the warrant, as required by Rule 41(f), was not prejudicial).

To rebut Levin's prejudice argument, the government appears to ignore the NIT Warrant altogether, baldly stating that "[w]here there is probable cause, judicial approval, and the computer server which the defendant accessed to view child pornography was physically located in the jurisdiction where the issuing magistrate was located, there can be no prejudice to the

¹⁶ It follows from this that the government might not have obtained the evidence it seized pursuant to the Residential Warrant, since the application for that warrant was based on information it acquired through the execution of the NIT Warrant. As the government itself points out, it "had no way to know where the defendant was without first using the NIT[.]" Gov't's Resp. 15.

defendant." Gov't's Resp. 16. Simply put, this is not the standard for determining prejudice, and the government directs the Court to no authority to support its assertion. Moreover, as discussed above, the Rule 41(b) violation here had the effect of vitiating the purported judicial approval so, even by this standard, the government's argument against prejudice must fail.

3. Good-Faith Exception

Finally, the government argues that, even if the NIT Warrant violated the Federal Magistrates Act and Rule 41(b), the Court ought not exclude the evidence seized pursuant to the NIT Warrant because the law enforcement officers here acted in good faith. See Gov't's Resp. 21 (citing United States v. Leon, 468 U.S. 897, 918, 926 (1984)). Whether the good-faith exception applies where a warrant was void is a question of first impression in this Circuit, and an unresolved question more broadly. See Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment, § 1.3(f) n.60 ("It is unclear whether the [Leon good-faith] rule extends to a warrant 'that was essentially void ab initio' because of 'the issuing court's lack of jurisdiction to authorize the search in the first instance.'") (quoting United States v. Baker, 894 F.2d 1144, 1147 (10th Cir. 1990)). This Court holds that it does not.

In Leon, the Supreme Court held that suppression was unwarranted where evidence was obtained pursuant to a search

warrant that was later determined to be unsupported by probable cause, since the executing officers acted in objectively reasonable reliance on the warrant's validity. See 468 U.S. at 922. In reaching this conclusion, the Supreme Court observed that "[r]easonable minds frequently may differ on the question whether a particular affidavit establishes probable cause, and we have thus concluded that the preference for warrants is most appropriately effectuated by according great deference to a magistrate judge's determination." Id. at 914 (internal quotation marks and citation omitted).

Leon contains not the slightest suggestion, however, that the same deference ought apply when magistrate judges determine their own jurisdiction. Indeed, the Supreme Court's conclusion presupposes that the issuing magistrate judge was authorized to issue the challenged warrant. Cf. United States v. Houston, No. 3:13-09-DCR, 2014 WL 259085 at *26 n.14 (E.D. Tenn. Jan. 23, 2014) (where a warrant is "void ab initio . . . the [c]ourt never reaches the question of whether the search warrant is supported by probable cause") (internal citation omitted). Moreover, Leon deals explicitly with a "subsequently invalidated warrant," 468 U.S. at 918 (emphasis added), rather than a warrant that was void at the time of its issuance. The latter

raises qualitatively different concerns, as several post-Leon courts have recognized.¹⁷

Over the years since Leon, the Supreme Court has expanded the good-faith exception to contexts beyond those Leon specifically addressed.¹⁸ None of the Supreme Court's post-Leon good-faith cases, however, involved a warrant that was void ab initio, and therefore none direct the conclusion that the good-

¹⁷ Courts interpreting the scope of Leon have repeatedly held or acknowledged in dicta that where evidence is obtained pursuant to a warrant that is void ab initio, the good-faith exception has no application. See, e.g., State v. Wilson, 618 N.W.2d 513, 520 (S.D. 2000) (holding that good-faith exception could not save evidence obtained pursuant to warrant issued by state judge acting outside territorial jurisdiction, since "[a]ctions by a police officer cannot be used to create jurisdiction, even when done in good faith"); State v. Nunez, 634 A.2d 1167, 1171 (R.I. 1993) (stating in dicta that Leon good-faith exception "would be inapplicable to this case because" it involved a warrant issued by a retired judge without authority to do so, and thus was "void ab initio"); Commonwealth v. Shelton, 766 S.W.2d 628, 629-30 (Ky. 1989) (noting in dicta that Leon would not be applicable since "in the case at bar, we are not confronted with a technical deficiency; but rather a question of jurisdiction"); United States v. Vinnie, 683 F.Supp. 285, 288-89 (D. Mass. 1988) (Skinner, J.) (holding Leon's good-faith exception inapplicable since the case involved not the "determination of what quantum of evidence constitutes probable cause" but rather "the more fundamental problem of a magistrate judge acting without subject matter jurisdiction").

¹⁸ Leon, along with its companion case, Massachusetts v. Sheppard, 468 U.S. 981 (1984), "contemplated two circumstances: one in which a warrant is issued and is subsequently found to be unsupported by probable cause and the other in which a warrant is supported by probable cause, but is technically deficient." Vinnie, 683 F.Supp. at 288.

faith exception ought apply to this case.¹⁹ This Court is aware of only one federal circuit court to address the question of whether Leon's good-faith exception applies in these circumstances: the Sixth Circuit. See Master, 614 F.3d 236; United States v. Scott, 260 F.3d 512 (6th Cir. 2001). Scott involved a search warrant issued by a retired judge who lacked authority to do so. 260 F.3d at 513. After holding that such warrant was necessarily void ab initio, id. at 515, the court concluded that, "[d]espite the dearth of case law, we are confident that Leon did not contemplate a situation where a

¹⁹ The good-faith exception has been held to apply where officers execute a warrant in reliance on existing law. See Davis v. United States, 131 S. Ct. 2419 (2011) (good-faith exception precluded suppression of evidence obtained through a search incident to arrest that was proper under binding appellate precedent at the time of the search but which was later held to be unlawful); Illinois v. Krull, 480 U.S. 340 (1987) (good-faith exception applied to a warrantless administrative search conducted pursuant to a statute later found to be unconstitutional, where the officer's reliance on the constitutionality of the statute was objectively reasonable). Unlike in those cases, here there was no "intervening change in the law that made the good-faith exception relevant." United States v. Wurie, 728 F.3d 1 (1st Cir. 2013).

The Supreme Court has also applied the good-faith exception in circumstances involving one-off mistakes of fact that implicate the validity of a warrant at the time of its execution. See Herring v. United States, 555 U.S. 135 (2009) (good-faith exception applied to evidence improperly obtained as a result of law enforcement's negligent record-keeping practices); Arizona v. Evans, 514 U.S. 1 (1995) (evidence seized in violation of the Fourth Amendment as a result of a clerical error on the part of court personnel was covered by good-faith exception and thus did not warrant suppression). Here, in contrast, the warrant was void at its inception.

warrant is issued by a person lacking the requisite legal authority." Id.

Nine years later, the Sixth Circuit effectively reversed itself in Master, which involved a warrant issued by a state judge to search property outside his district, which was unauthorized under Tennessee law. 614 F.3d at 239. The court held that the warrant was invalid for the same reason as was the warrant in Scott,²⁰ id. at 240, but that the good-faith exception to the exclusionary rule applied because Scott's reasoning was "no longer clearly consistent with current Supreme Court doctrine." Id. at 242. In particular, it noted that "[t]he Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violation, 'the benefits of deterrence must outweigh the costs.'" Id. at 243 (quoting Herring v. United States, 555 U.S. 135, 142 (2009)).

The Master court read the Supreme Court's recent good-faith cases too broadly.²¹ This Court is persuaded instead by the

²⁰ The difference between the issuer of the warrant in Scott and in Master -- namely, a retired judge with "no authority to approve any warrants," and an active judge with authority to issue warrants within his district, respectively -- was "immaterial" for the purpose of determining whether the warrant was valid. Master, 614 F.3d at 240.

²¹ Even in Master, it should be noted, the court acknowledged that the recent Supreme Court cases addressing the

rationale in Scott and cases applying the holding of that decision, see, e.g., United States v. Neering, 194 F.Supp.2d 620 (E.D. Mich. 2002) (warrant issued by an official who was not properly appointed and therefore lacked issuing authority was void, and under Scott, the good-faith exception did not apply). Neither Hudson nor Herring -- both of which the Master court cited in support of its conclusion that Scott's holding is no longer tenable, see 614 F.3d at 242 -- requires the conclusion that the good-faith exception applies to evidence seized pursuant to a warrant that was void ab initio.²²

good-faith exception "do[] not directly overrule our previous decision in Scott." 614 F.3d at 243.

²² In Hudson, 547 U.S. 586 (2006), the Supreme Court held that suppression was not an appropriate remedy for a violation of the knock-and-announce rule. See id. at 599. In reaching this conclusion, the plurality explicitly distinguished the interests protected by the warrant requirement and the knock-and-announce requirement. See id. at 593. With respect to the warrant requirement, it noted that "[u]ntil a valid warrant has issued, citizens are entitled to shield their persons, houses, papers, and effects . . . from the government's scrutiny[,] and that "[e]xclusion of the evidence obtained by a warrantless search vindicates that entitlement." Id. (internal quotation marks and citations omitted) (emphasis added). As no valid warrant was ever issued here, and the government does not argue that an exception to the warrant requirement applies, exclusion is appropriate.

Herring, too, is distinguishable. There, law enforcement officers executed an arrest warrant that had been rescinded. 555 U.S. at 138. The Supreme Court held that since the mistake was attributable to "isolated negligence attenuated from the arrest" -- specifically, a recordkeeping error -- the good-faith exception to the exclusionary rule applied. Id. at 137. Although that case makes much of the connection between the exclusionary rule and the goal of deterrence and culpability of

Because a warrant that was void at the outset is akin to no warrant at all, cases involving the application of the good-faith exception to evidence seized pursuant to a warrantless search are especially instructive. In United States v. Curzi, 867 F.2d 36 (1st Cir. 1989), the First Circuit declined to “recognize[] a good-faith exception in respect to warrantless searches.” Id. at 44.²³ To hold that the good-faith exception is applicable here would collapse the distinction between a voidable and a void warrant. But this distinction is meaningful: the former involves “judicial error,” such as “misjudging the sufficiency of the evidence or the warrant

law enforcement, see id. at 141-43, it says nothing about whether the same calculus ought apply where there was never jurisdiction to issue a valid warrant in the first place.

²³ While no case has directly disturbed this holding, the First Circuit has since held that the good-faith exception may exempt from exclusion evidence seized pursuant to an unconstitutional warrantless search “‘conducted in objectively reasonable reliance on binding appellate precedent[.]’” United States v. Sparks, 711 F.3d 58, 62 (1st Cir. 2013) (quoting Davis, 131 S.Ct. at 2434). Cases like Sparks, though, are readily distinguishable: the officers in Sparks were entitled to rely on circuit precedent indicating that they could conduct the challenged search without a warrant; by contrast, here no binding appellate precedent authorized the officers to undertake the search either without a warrant or pursuant to one that was void at the outset. To determine whether the good-faith exception applied in Sparks, the court asked: “what universe of cases can the police rely on? And how clearly must those cases govern the current case for that reliance to be objectively reasonable?” 711 F.3d at 64. Such questions are wholly inapposite here.

application's fulfillment of the statutory requirements[,]" while the latter involves "judicial authority," i.e., a judge "act[ing] outside of the law, outside of the authority granted to judges in the first place." State v. Hess, 770 N.W.2d 769, 776 (Ct. App. Wis. 2009) (emphasis added); cf. Scott, 260 F.3d at 515 ("Leon presupposed that the warrant was issued by a magistrate or judge clothed in the proper legal authority, defining the issue as whether the exclusionary rule applied to 'evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be unsupported by probable cause.'") (quoting Leon, 468 U.S. at 900); State v. Vickers, 964 P.2d 756, 762 (Mont. 1998) (distinguishing Leon and concluding that "[i]f a search warrant is void ab initio, the inquiry stops and all other issues pertaining to the validity of the search warrant, such as whether the purpose of the exclusionary rule is served, are moot."). Were the good-faith exception to apply here, courts would have to tolerate evidence obtained when an officer submitted something that reasonably looked like a valid warrant application, to someone who, to the officer, appeared to have authority to approve that warrant application. Cf. Krueger, 809 F.3d at 1126 (Gorsuch, J., concurring). This Court holds that

such an expansion of the good-faith exception is improvident, and not required by current precedent.²⁴

Even were the Court to hold that the good-faith exception could apply to circumstances involving a search pursuant to a warrant issued without jurisdiction, it would decline to rule such exception applicable here. For one, it was not objectively reasonable for law enforcement -- particularly "a veteran FBI agent with 19 years of federal law enforcement experience[,]" Gov't's Resp. 7-8 -- to believe that the NIT Warrant was properly issued considering the plain mandate of Rule 41(b). See Glover, 736 F.3d at 516 ("[I]t is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by 'good faith.'"); cf. United States v. McKeever, 894 F.2d 712, 717 (5th Cir. 1990) (good-faith exception did not apply where sheriff "who was the prime mover in obtaining and executing the search . . . knew both that

²⁴ While the exclusionary rule has its detractors, see, e.g., Akhil Reed Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 785-800 (1994) (arguing that suppression is an "awkward and embarrassing remedy" that is unsupported by the text of the Fourth Amendment), "when a criminal conviction is predicated on a violation of the Constitution's criminal procedure requirements, including the Fourth Amendment, the conviction works an ongoing deprivation of liberty without due process," Richard M. Re, The Due Process Exclusionary Rule, 127 Harv. L. Rev. 1885, 1887 (2014); see also Carol S. Steiker, Second Thoughts About First Principles, 107 Harv. L. Rev. 820, 848-852 (1994).

he had to obtain a warrant from a court of record . . . and that [the issuing judge] was not a judge of a court of record.”).²⁵ Moreover, even analyzed under Herring, the conduct at issue here can be described as “systemic error or reckless disregard of

²⁵ In its oral argument opposing this motion, Elec. Clerk’s Notes, ECF No. 62, the government indicated that the particular officers executing the search cannot be charged with the knowledge that the warrant was issued in violation of the Federal Magistrates Act and Rule 41(b). But it would be incongruous to view these officers’ conduct in isolation. As Professor Amsterdam articulated:

[S]urely it is unreal to treat the offending officer as a private malefactor who just happens to receive a government paycheck. It is the government that sends him out on the streets with the job of repressing crime and of gathering criminal evidence in order to repress it. It is the government that motivates him to conduct searches and seizures as a part of his job, empowers him and equips him to conduct them. If it also receives the products of those searches and seizures without regard to their constitutionality and uses them as the means of convicting people whom the officer conceives it to be his job to get convicted, it is not merely tolerating but inducing unconstitutional searches and seizures.

Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 432 (1974).

constitutional requirements,"²⁶ 555 U.S. at 147, and the Court thus concludes that suppression is appropriate.²⁷

4. Policy Ramifications

Notwithstanding the Court's doctrinal analysis -- which has now concluded -- the Court is mindful of the thorny practical questions this motion raises. The government asserts that to hold that the magistrate judge lacked authority to issue the NIT

²⁶ The Supreme Court does not define "systemic negligence," Herring, 555 U.S. at 144, or "systemic error," id. at 147, and the former, at least, is apparently a new term in the Supreme Court's lexicon, see Wayne R. Lafave, The Smell of Herring: A Critique of the Supreme Court's Latest Assault on the Exclusionary Rule, 99 J. Crim. L. & Criminology 757, 784 (2009). It is difficult to ascertain the frequency with which similar warrants -- i.e., warrants to conduct remote searches of property located outside a magistrate judge's judicial district -- are granted, since these warrants are typically issued and remain under seal. See Owsley, supra note 4, at 4-5. Nonetheless, it is clear to the Court that this is far from the sole instance in which the government has sought and obtained an NIT warrant. See id. (listing cases involving NIT warrants or similar); Gov't's Resp. 23.

²⁷ The Court acknowledges that suppression is an extreme remedy, and consequently it considered whether, on this occasion -- but never again under these circumstances -- the evidence at issue ought be let in under the good-faith exception. See State v. Hardy, No. 16964, 1998 WL 543368, at *6-7 (Ct. App. Ohio Aug. 28, 1998) (Fain, J., concurring in the judgment) (concluding that good-faith exception should apply to evidence obtained pursuant to a warrant issued without proper jurisdiction, but noting that "[o]nce we allow time for reasonable police officers within this jurisdiction to become acquainted with the territorial limits upon a magistrate judge's authority to issue search warrants, however, claims of good-faith exceptions to the warrant requirement are likely to be unavailing."). Upon further deliberation, however, the Court concluded that to hold that Leon's good-faith exception applies here, where there never existed a valid warrant, would stretch that exception too far.

Warrant, and accordingly to suppress the evidence obtained pursuant thereto, would create "an insurmountable legal barrier" to law enforcement efforts in this realm. Gov't's Resp. 16. The Court is unmoved by the government's argument for two reasons.

First, it cannot fairly be said that the legal barrier to obtaining this type of NIT Warrant from a magistrate judge is "insurmountable," because the government itself has come up with a way of surmounting it -- namely, to change Rule 41(b), see supra note 13.

Second, it does not follow from this opinion that there was no way for the government to have obtained the NIT Warrant. Section 636(a) and Rule 41(b) limit the territorial scope of magistrate judges -- they say nothing about the authority of district judges to issue warrants to search property located outside their judicial districts. Indeed, the quotation from United States v. Villegas, 899 F.2d 1324 (2d Cir. 1990), included in the government's own brief, is revealing: "Rule 41 does not define the extent of the court's power to issue a search warrant. . . . Given the Fourth Amendment's warrant requirements and assuming no statutory prohibition, the courts must be deemed to have inherent power to issue a warrant when the requirements of that Amendment are met." Gov't's Resp. 20-21 (quoting Villegas, 899 F.2d at 1334). With respect to

district judges, neither Rule 41(b) nor Section 636(a) of the Federal Magistrates Act restricts their inherent authority to issue warrants consistent with the Fourth Amendment. See Krueger, 809 F.3d at 1125 n.6 (noting that analysis of a magistrate judge's lack of statutory authority to issue warrants to search outside his district has no bearing on "the statutory authorities of a district judge to issue a warrant for an out-of-district search[,] and pointing out that "[u]nlike magistrates, the jurisdiction of district courts is usually defined by subject matter and parties rather than strictly by geography."); cf. Matter of Application and Affidavit for a Search Warrant, 923 F.2d 324, 326 (4th Cir. 1991) (contrasting a district judge's "inherent power" with a magistrate's power, which is either delegated by a district judge or expressly provided by statute).²⁸

²⁸ Surprisingly, a number of courts have apparently understood Rule 41(b) to apply to district judges. See, e.g., United States v. Golson, 743 F.3d 44, 51 (3d Cir. 2014) ("Rule 41(b) grants the authority to issue search warrants to federal judges and judges of state courts of record."); Glover, 736 F.3d at 515 (concluding that a warrant issued by a district judge to search property outside that judge's district violated Rule 41(b)(2)); cf. United States v. Krawiec, 627 F.2d 577, 580 (1st Cir. 1980) (indicating that all "federal warrants" are required to comply with Rule 41). On its face, however, Rule 41(b) applies only to "a magistrate judge" and "a judge of a state court of record." The authority of district judges to issue warrants arises elsewhere, see Villegas, 899 F.2d at 1334; 18 U.S.C. § 3102, and district judges are not subject to the limitations set forth in Rule 41(b).

The magistrate judge who issued this warrant sits primarily in Alexandria, Virginia. See NIT Warrant. Four district judges and three senior judges sit routinely in that courthouse. See Alexandria Courthouse, United States District Court Eastern District of Virginia, <http://www.vaed.uscourts.gov/locations/alex.htm> (last visited Apr. 20, 2016). Here, the government had already involved one of those district judges in its investigation, albeit to obtain the Title III warrant. See Title III Warrant.

Of course, were the government to present its NIT Warrant application to a district judge, it would still have to meet the requirements of the Fourth Amendment, which guarantees that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched.” U.S. Const. amend. IV. Of special concern here is the particularity requirement, since, as the government points out, “the defendant’s use of the Tor hidden service made it impossible for investigators to know what other districts, if any, the execution of the warrant would take place in,” Gov’t’s Resp. 20.²⁹ While this Court need not decide whether the

²⁹ Indeed, objectors to the proposed amendment to Rule 41(b), see supra note 13, have argued that a warrant that permitted law enforcement to remotely search computers at unknown locations would violate the Fourth Amendment’s particularity requirement. See, e.g., Written Statement of the

particularity requirement was met here, it notes that despite the difficulty highlighted by the government, at least two courts have determined that this precise warrant was sufficiently particular to pass constitutional muster. See United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016); United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 at *4-*5 (W.D. Wash. Jan. 28, 2016). But cf. In re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d at 755-58 (warrant to "surreptitiously install[] software designed . . . to extract certain stored electronic records" from "an unknown computer at an unknown location" did not satisfy Fourth Amendment particularity requirement).

IV. CONCLUSION

Based on the foregoing analysis, the Court concludes that the NIT Warrant was issued without jurisdiction and thus was void ab initio. It follows that the resulting search was conducted as though there were no warrant at all. Since warrantless searches are presumptively unreasonable, and the good-faith exception is inapplicable, the evidence must be excluded. Accordingly, Levin's motion to suppress, ECF No. 44, is GRANTED.

Center for Democracy & Technology Before the Judicial Conference Advisory Committee on Criminal Rules 2, Oct. 24, 2014.

SO ORDERED.

/s/ William G. Young
WILLIAM G. YOUNG
DISTRICT JUDGE

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

UNITED STATES OF AMERICA,)
)
 Plaintiff,)
)
 v.)
)
 SCOTT FREDRICK ARTERBURY,)
)
 Defendant.)

Case No. 15-CR-182-JHP

REPORT AND RECOMMENDATION

Before the Court is the Motion to Suppress Evidence Seized from Residence (“Motion to Suppress”) and Request for an Evidentiary Hearing of Defendant Scott Fredrick Arterbury (“Arterbury”). [Dkt. No. 33]. On March 23, 2016, the matter was referred to the undersigned United States Magistrate Judge for Report and Recommendation on the Motion to Suppress. [Dkt. No. 35]. The Motion for hearing has been **GRANTED**, and a hearing conducted on April 25, 2016. After considering the submissions of the parties and the arguments of counsel, the undersigned makes the following findings and recommendation to the District Court.

**I.
FACTUAL BACKGROUND – THE “DARK NET” OR TOR**

This case involves what is known as the “The Dark Net,” the “Tor Network” or “Tor” for short.¹ “Tor is an open-source tool that aims to provide

¹ The Dark Net generally refers to “an area of the Internet only accessible by using an encryption tool called The Onion Router (Tor). Tor is a tool aimed at those desiring privacy online, although frequently attracting those with criminal intentions.” Gareth Owen and Nick Savage, “The Tor Dark Net”, at 1

anonymity and privacy to those using the Internet. It prevents someone who is observing the user from identifying which sites they are visiting and it prevents sites from identifying the user. Some users value Tor's anonymity because it makes it difficult for governments to censor sites or content that may be hosted elsewhere in the world." Owen and Savage, at 1. An individual living under a repressive government such as North Korea, for example, might make use of Tor to access or post certain information while avoiding government surveillance. However, after analyzing Tor Dark net sites over a six-month period, Owen and Savage found that "the majority of sites were criminally oriented, with drug marketplaces featuring prominently. Notably, however, it was found that sites hosting child abuse imagery were the most frequently requested." *Id.*

The Tor network is designed to route communications through multiple computers, protecting the confidentiality of Internet Protocol ("IP") addresses and other identifying information. See, Keith D. Watson, *The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*, 11 Wash. U. Global Stud. L. Rev. 715 (2012) (hereafter, "Watson"). See, for example, *U.S. v. Frater*, 2016 WL 795839, *3 (D. Ariz. March 1, 2016).

Tor allows users to send data over the Internet anonymously by shielding the source's location. This is accomplished by a complex encryption network that dissociates Internet communication from its source's IP address. Tor achieves user anonymity through so-called "onion routing," which bounces all communications routed through the Tor network to various different "nodes" before delivering them to their destination. These "nodes" are proxy

[Centre for International Governance Innovation and Royal Institute of International Affairs, September 2015) (hereafter, "Owen & Savage").

servers scattered across the globe. Tor users connect to the network by first pulling in a list of nodes from a directory server. The user's computer then accesses the Tor network through a random node. The user's information is then routed through a random series of relay nodes before finally routing to an exit node, which sends the user's information to the actual Internet. What is significant about the Tor network is that each node communicates only with the nodes immediately preceding and following it in the chain. Therefore, the user's computer has direct contact with only the first node in the chain, and the actual Internet communicates only with the exit node. The entry node does not know the ultimate destination of the data, and the exit node is unaware of the data's origin. Because exit nodes are the only nodes that communicate directly with the public Internet, any traffic routed through the Tor network is traceable only to the exit node. Each communication is encrypted in a new layer of code before passing to the next node. The communication is eventually ensconced in several layers of code, which are then "peeled away" by the exit node, hence the onion metaphor.

Thus, Computer A submits data through the Tor network, the communication will pass through the network and exit onto the actual Internet through the exit node, Computer B. Any data sent by Computer A will appear to anyone tracing the communication as if it has come from Computer B. This essentially allows the user of Computer A to surf the Internet with complete anonymity, assuming the user never submits any information that is linked to her identity, such as accessing her standard e-mail account.

Watson, at 721-23.

To combat illegal activity using the Tor network, the Government has developed so-called "Trojan horse devices." These may include: "data extraction software, network investigative technique, port reader, harvesting program, remote search, CIPAV for Computer and Internet Protocol Address Verifier, or IPAV for Internet Protocol Address Verifier." Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 Akron L. Rev. 315, 316 (2015). In the instant case, the parties have referred to the warrant issued by the U.S. magistrate judge in the Eastern District of Virginia as a Network

Investigative Technique (“NIT”) warrant, and the Court will adopt that terminology.

Once approved, the NIT is installed on the target Website. “Once installed on Website A, each time a user accessed any page of Website A, the NIT sent one or more communications to the user's computer which caused the receiving computer to deliver data to a computer controlled by the FBI, which would help identify the computer which was accessing Website A.” *U.S. v. Pierce*, 2014 WL 5173035, *3 (D.Neb. Oct. 14, 2014). In some cases, the Government has even activated a target computer’s built-in camera to take photographs of the persons using that computer and send the photos back to the Government. *E.g., In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013).

The critical point is that without the use of such techniques as NIT, agents seeking to track a Tor user to his home computer will not be able to take that pursuit beyond the exit node from which the Tor user accessed the regular Internet.² NIT allows the Government to surreptitiously send a message back through the Tor network to the home computer directing it to provide information from which the user may be identified.

² See for example, the Affidavit of Douglas Macfarlane offered in support of the Warrant Application in the Eastern District of Virginia. [Dkt. No. 34-1]. Macfarlane states that because of the Tor Network, “traditional IP identification techniques are not viable.” [*Id.*, at ¶ 8]. “An exit node is the last computer through which a user’s communications were routed. There is no practical way to trace the user’s actual IP back through that Tor exit node IP.” [*Id.*].

II. FACTUAL BACKGROUND OF THIS CASE

The Government obtained evidence regarding Arterbury's alleged criminal conduct through a multi-step process that began in the Fall of 2014. At that time, Agents of the Federal Bureau of Investigation ("FBI") began investigating the Playpen website, a global online forum believed to be hosting users for purposes of distributing and accessing child pornography.³ In February 2015, agents apprehended the administrator of Playpen in Naples, Fla., took control of the site, and moved it to Virginia. Rather than shut Playpen down immediately, agents decided to allow the site to continue operation for 12 days (February 20, 2015 to March 4, 2015) in the hopes of identifying and prosecuting Playpen users. In furtherance of the investigation, the Government sought to use a Network Investigative Technique that would covertly transmit computer code to Playpen users. That code would direct users' computers to provide investigators with information which could then be used to locate and identify the users. In order to employ the NIT, however, the Government needed to obtain an "NIT search warrant."

In February 2015, a warrant application was prepared and presented to a magistrate judge in the Eastern District of Virginia. Absent the use of the NIT, the Government had no ability to locate and identify users of the Playpen

³ In affidavits in support for the NIT warrant at issue, as well as various pleadings, the parties refer to "Website A." It is now widely known that Website A refers to the "Playpen," a website offering those who access it the opportunity to view and download child pornography. The Court will refer to Playpen, since the identity of the website has been widely publicized.

website. Special Agent Douglas Macfarlane, in his Affidavit in Support of Application for the NIT Search Warrant, stated:

Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple computers or “nodes” . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

[Dkt. No. 34-1, Affidavit in Support of Application for Search Warrant, at 28-29, ¶ 31].

On February 20, 2015, U.S. Magistrate Judge Theresa Carroll Buchanan issued the NIT warrant. When users accessed Playpen, the NIT caused data extraction software to be installed on the user’s computer – wherever it was located. The computer then sent – without Defendant’s knowledge or permission – requested information to a Government-controlled computer.⁴ In this way, the Government could determine the identity of the person accessing Playpen – even when that person was using a computer that was located outside the Eastern District of Virginia.

Using NIT, agents determined that a Playpen registrant with the user name “johnnyb5” and an IP address of 70.177.122.133 had logged on to the website from February 20 to March 4, 2015. Agents were able to determine that the IP address was operated by Cox Communications, Inc. Using an administrative subpoena directed at Cox, they secured the name and address of the account holder. This information was included in the affidavit of Special

⁴ This information included the IP address of the home computer, its type of operating system, the computer’s “Host Name”, its active operating system username and its media access control (“MAC”) address.

Agent Joseph Cecchini in support of a search warrant application presented to U.S. Magistrate Judge T. Lane Wilson in the Northern District of Oklahoma (the “Oklahoma warrant”) on November 2, 2015. *See* 15-mj-196-TLW, [Dkt. 1]. The affidavit supporting the Oklahoma warrant is quite similar to the affidavit supporting the NIT warrant application. However, the Oklahoma warrant details the Defendant’s alleged conduct regarding the Playpen website and the information obtained as a result of the NIT.

Judge Wilson issued the search warrant for 1515 S. Nyssa Place, Broken Arrow, Oklahoma. Agents executed the warrant, and located and seized alleged child pornography. Judge Wilson then executed a Criminal Complaint and a warrant for the Defendant’s arrest.

Defendant appeared before the undersigned on November 16, 2015, at which time, he was released on conditions of supervision.

Defendant’s Motion to Suppress seeks to preclude use of any material discovered through the search of his home, arguing, *inter alia*, that the warrant issued by the magistrate judge in Virginia is fatally flawed, and, thus, taints the Oklahoma warrant.

Plaintiff offers three arguments in support of his Motion to Suppress:

- First, that the magistrate judge in Virginia exceeded her authority under Fed. R. Crim. P. 41 by issuing a warrant for property outside her jurisdiction.

- Second, that the affidavit supporting the NIT warrant application falsely represented that the Playpen home page contained a depiction of “prepubescent females, partially clothed with their legs spread.”
- Third, the NIT warrant was overbroad because there was not probable cause to justify a search of all “activating computers” on the mere basis of registering with Playpen.

III. APPLICABLE LEGAL PRINCIPLES

Clearly, a search occurs within the meaning of the Fourth Amendment when “the Government obtains information by physically intruding on a constitutionally protected area.” *U.S. v. Jones*, -- U.S. --, 132 S.Ct. 945, 950 n.3 (2012). However, the Fourth Amendment is not concerned just with “trespassory intrusions” on property. *Id.*, at 954 (Sotomayor, J. concurring). The reach of the Fourth Amendment does not “turn upon the presence or absence of a physical intrusion.” *Id.* (citing *Katz v. U.S.*, 389 U.S. 347, 353 (1967)). As Justice Sotomayor pointed out in *Jones*, we now have a variety of forms of electronic and other “novel modes” of surveillance that do not depend upon a physical intrusion of one’s property. Such is the case presented here, where it may not be entirely clear what “property” is being searched or seized or even where that search or seizure occurred.

The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

describing the place to be searched, and the person or things to be seized.

U.S. Const. amend. IV.

A search occurs “when the Government acquires information by either ‘physically intruding’ on persons, houses, papers or effects,’ ‘or otherwise invading an area in which the individual has a reasonable expectation of privacy’.” *U.S. v. Scully*, 108 F.Supp.3d 59, 75 (E.D.N.Y. 2015). “A seizure occurs when the Government interferes in some meaningful way with the individual’s possession of property.” *Id.* (quoting *U.S. v. Ganius*, 755 F.3d 125, 133 (2d Cir. 2014)). Pursuant to the Federal Rules of Criminal Procedure, the term “property” includes “documents, books, papers, any other tangible objects, and *information*.” Fed. R. Crim. P. 41(a)(2)(A) (emphasis added). The Rule permits seizure of electronic and digital data. “Rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses...” *U.S. v. New York Tel. Co.*, 434 U.S. 159, 170 (1977).

The legality of a search is predicated upon a finding that the warrant authorizing the search comports with constitutional requirements and the provisions of Rule 41 which is “designed to protect the integrity of the federal courts or to govern the conduct of federal officers.” *U.S. v. Pennington*, 635 F.2d 1387, 1389 (10th Cir. 1980) (quoting *U.S. v. Millar*, 543 F.2d 1280, 1284 (10th Cir. 1976) and *U.S. v. Sellers*, 483 F.2d 37, 43 (5th Cir. 1973), *cert. denied*, 417 U.S. 908 (1974)).

Rule 41 provides in pertinent part:

Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

- (1) a magistrate judge with authority in the district ... has authority to issue a warrant to search for and seize a person or property located within the district;
- (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
- (3) a magistrate judge -- in an investigation of domestic terrorism or international terrorism -- with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
- (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
- (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
 - (A) a United States territory, possession, or commonwealth;
 - (B) the premises -- of matter who owns them -- of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
 - (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b)(1)-(5).⁵

If the court finds a violation of Rule 41, this does not automatically mean the evidence seized must be suppressed. “Suppression of evidence ... has always been our last resort, not our first impulse.” *U.S. v. Leon*, 468 U.S. 897, 907 (1984). The exclusionary rule generates “substantial social costs,” which sometimes include setting the guilty free and the dangerous at large. We have therefore been “cautio[us] against expanding” it, and “have repeatedly emphasized that the rule’s ‘costly toll’ upon truth-seeking and law enforcement objectives presents a high obstacle for those urging [its] application,” *Pennsylvania Bd. of Probation and Parole v. Scott*, 524 U.S. 357, 364–365 (1998) (internal citations omitted).

IV. RECENT CASES

Several recent decisions arising from the same facts and circumstances before this Court are instructive. These include: *U.S. v. Michaud*, 2016 WL 337263 (W.D.Wash. Jan. 28, 2016); *U.S. v. Stamper*, Case No. 1:15cr109 (S.D.Ohio Feb. 19, 2016); *U.S. v. Epich*, 2016 WL 953269 (E.D.Wis. March 14, 2016); and, *U.S. v. Levin*, 2016 WL 1589824 (D.Mass. April 20, 106).

All of these cases involve the same “sting” operation that netted Defendant Arterbury. All of the cases involve the NIT warrant that was issued by a magistrate judge in the Eastern District of Virginia. In each case, the NIT warrant sent computer malware to an “activating computer” in a district

⁵ Here, the warrant was issued pursuant to Rule 41(b)(1) – requesting a search/seizure of property “located in the Eastern District of Virginia.” [Dkt. No. 34-1, at 3].

outside of Virginia. That malware seized control of the defendants' computers and caused them to send identifying information to another Government computer in the Eastern District of Virginia. That identifying information was then used to secure a second warrant from a magistrate judge in the defendant's home district authorizing the search and seizure of the defendant's computer.

All of these four cases found that the NIT warrant violated Fed. R. Crim. P. 41(b). However, in *Michaud* and *Stamper*, the courts held that the violation of Rule 41 was a mere "technical violation" that did not prejudice the defendant. *Stamper* adopted the reasoning of *Michaud* that one has no reasonable expectation of privacy in one's IP address and such information, even when extraordinary means have been taken to secret that information. *Michaud* likened the IP address to an unlisted telephone number and opined that the Government would have ultimately been able to get this information without the NIT process.⁶

Epich is of little assistance to this Court because it is governed by Seventh Circuit law holding that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause...." *U.S. v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008). "The remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant would be 'wildly out of proportion to the

⁶ I find this conclusion wholly at odds with the Affidavit submitted in support of the NIT warrant wherein the Government stated that absent use of the NIT, it would be impossible to secure the IP address.

wrong’.” *U.S. v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008) (quoting *Cazares-Olivas*, 515 F.3d at 730)).

In light of *Leon*, it is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the Fourth Amendment, that would call for suppression. Many remedies may be appropriate for deliberate violations of the rules, but freedom for the offender is not among them.

U.S. v. Trost, 152 F.3d 715, 722 (7th Cir. 1998) (quoting *U.S. v. Hornick*, 815 F.2d 1156, 1158 (7th Cir. 1987)).

The Tenth Circuit does not follow the Seventh Circuit in this regard. In *Krueger*, for example, the Tenth Circuit suppressed evidence on the basis of a Rule 41(b) violation; thus, *Epich* is of little assistance to the Court’s analysis.

The remaining case is *Levin*, in which the district court – relying heavily on *Krueger* – found a fundamental jurisdictional defect in issuing the NIT warrant in violation of the provisions of Rule 41(b). Because the NIT warrant was void *ab initio*, the Court held, the good faith exception did not apply and the evidence had to be suppressed.

V DISCUSSION

Because the undersigned believes that the validity of the NIT warrant issued in Virginia is determinative of the Defendant’s motion, the Court has focused its attention on that issue and the coincident suppression/good faith issues.

The Court begins by addressing two preliminary issues. First, the warrant under challenge is the NIT warrant issued in the Eastern District of Virginia. That warrant provided probable cause for the issuance of the second, Oklahoma warrant. The Government admitted at the April 25 hearing, that if the NIT warrant is fatally flawed, there would not be probable cause to support the Oklahoma warrant.

Second, the Court seeks to clarify what “property” was seized pursuant to the NIT warrant. The Government contends that in accessing the Playpen website Arterbury sent “packets of data” into the Eastern District of Virginia, and that this digital or electronic data is the property at issue. The Defendant contends that his home computer was the seized property. Essentially, he contends that the computer was first seized pursuant to the NIT warrant when the government, through malware, entered his home, took control of his computer and “searched” it for private information he had endeavored to keep confidential. Subsequently, the computer was physically seized when agents took it pursuant to the Oklahoma warrant.

The Court holds that the property seized was Arterbury’s computer. The Government did not seize the “packets of data” Arterbury sent to the Eastern District of Virginia, because it was unable to do so. Since there was no way to get this data, the Government employed the NIT to seize Arterbury’s computer and direct it to provide the identifying information without his knowledge. Had the Government seized Arterbury’s encrypted information in the Eastern District of Virginia, and, through some sort of forensic tool, un-encrypted it to

learn his identifying information, the Court would be inclined toward the Government's position, but that is not what happened. The Macfarlane affidavit makes it clear that the Government could not obtain Arterbury's IP address until its malware made its way back to his computer in Oklahoma and directed it to provide information to the Government.

A. The Virginia Judge Lacked Rule 41 Authority to Issue the NIT Warrant.

Defendant contends that the magistrate judge in Virginia lacked authority under Fed. R. Crim. P. 41 to issue a warrant seeking to seize/search property outside her judicial district. Rule 41 provides five grounds authorizing a magistrate judge to issue a warrant. Rule 41(b)(1)-(5). The parties agree that subsections (b)(3) and (b)(5) have no application here. Thus the analysis will be confined to subsections (b)(1), (b)(2) & (b)(4).

Subsection 41(b)(1) does not provide authority for the Virginia warrant because Arterbury's computer was not located in or seized in the Eastern District of Virginia.

The Government argues that subsections (b)(2) & b(4) provide authority for the NIT warrant. The Court disagrees.

Subsection (b)(2) applies where a judge signs a warrant to seize property that is within his/her jurisdiction at the time the warrant is signed, but has been re-located outside that jurisdiction at the time the warrant is actually executed. The Government contends that by electronically reaching into the Eastern District of Virginia, Arterbury brought "property" into that district that was subject to the NIT warrant. The Government argues that the property was

then removed from Virginia to Oklahoma, thus, the NIT warrant comports with subsection (b)(2).

The Court is not persuaded by this argument. The property seized in this instance was Arterbury's computer, which at all relevant times remained in Oklahoma. The NIT warrant allowed the Government to send computer code or data extraction instructions to Arterbury's computer, wherever it was located. The Government "seized" that computer and directed it to send certain information to the Government – all without Arterbury's knowledge or permission. Arterbury's computer was never in the Eastern District of Virginia and subsection (b)(2), therefore, does not apply. Furthermore, even if the property seized was electronic information, that property was not located in the Eastern District of Virginia at the time the warrant was signed. This information only appeared in Virginia *after* the Warrant was signed and executed and the Government seized control of Defendant's computer in Oklahoma.

The Court is also unpersuaded by the Government's argument that the NIT warrant is valid under Rule 41(b)(4) as a "tracking warrant." The NIT did not track Defendant's computer as it moved. In *Michaud*, the district court rejected the Government's argument as applied to the same NIT operation, stating, "If the 'installation' occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because Mr. Michaud never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular

district,” and “[i]f the installation occurred on Mr. Michaud’s computer, applying the tracking device exception again fails, because Mr. Michaud’s computer was never physically located within the Eastern District of Virginia.” This Court agrees with *Michaud* in this regard and concludes Subsection 41(b)(4) is not applicable. The NIT warrant was not for the purpose of installing a device that would permit authorities to track the movements of Defendant or his property.

Furthermore, the drafters of Rule 41 knew how to avoid the territorial limit on issuance of warrants when they wished to do so. Rule 41(b)(3) removes the territorial limitation in cases involving domestic or international terrorism. In such cases, a magistrate judge “with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district.” Rule 41(b)(3). The drafters of Rule 41 could easily have included child pornography in Rule 41(b)(3) and, thereby, avoided the territorial limitation of Rule 41(b)(1) & (2). They did not do so. The Court can only conclude that they did not intend to remove the territorial limit in cases such as the one before the Court.

Authority to issue warrants exists only insofar as granted by the rules, and no further. Accordingly, just as the court concluded in *Michaud*, this Court finds that the NIT warrant was not authorized by any of the applicable provisions of Rule 41.⁷ Thus, the court concludes that the issuance of the

⁷ Apparently, the Government is aware of the problem of authorizing NIT warrants under the current Rules of Criminal Procedure. The Department of Justice has proposed amendments to Rule 41 that would resolve this issue.

warrant violated Rule 41(b).⁸

B. The Virginia Judge Lacked Authority Under the Federal Magistrate Judges Act.

There is another fundamental problem with the Virginia magistrate judge's authority to issue the NIT warrant. As Judge Gorsuch noted in his concurring opinion in *Krueger*, the Government's problem goes to the heart of the magistrate judge's statutory source of power. The Federal Magistrate Judges Act provides three territorial limits on a magistrate judge's power:

Each United States magistrate judge serving under this chapter shall have [1] within the district in which sessions are held by the court that appointed the magistrate judge, [2] at other places where that court may function, and [3] elsewhere as authorized by law ... all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts....

Id. at 1118 (*citing* 28 U.S.C. § 636(a)).⁹

As in *Krueger*, the magistrate judge “purported to exercise power in none of these places.” 809 F.3d at 1118. Thus, Judge Gorsuch notes, “The warrant on which the government seeks to justify its search in this case was no warrant at all when looking to the statutes of the United States.” *Id.* (emphasis added).

⁸ Defendant also asserts the NIT Warrant lacked statutory jurisdiction and therefore violated the Fourth Amendment. [Dkt. No. 33 at pp. 10-11 (*citing* Judge Gorsuch's concurring opinion in *Krueger*, 809 F.3d at 1117-26)]. However, consistent with the majority opinion in *Krueger*, since the court has determined that there was a clear Rule 41(b) violation, it declines to reach this issue. *Id.* at 1104-05 (“[C]onsistent with the fundamental rule of judicial restraint, we decline to reach a constitutional question that is not necessary for our resolution of this appeal (citation omitted)).

⁹ In *Krueger*, the government secured a warrant from a magistrate judge in Kansas permitting the seizure and search of property located in Oklahoma. The Tenth Circuit affirmed the lower court's finding that the warrant violated Rule 41 and the court's suppression of the evidence seized pursuant to the invalid warrant. *See*, discussion at p. 19-21, *infra*.

C. Under *Krueger*, Suppression is Warranted Because the Search Would Not Have Occurred But For the Breach of Rule 41(b).

The court must next consider whether suppression is justified. To establish the case for suppression, Defendant must show that he was prejudiced by the violation of Rule 41. The prejudice standard adopted in *Krueger* allows defendant to show either “(1) prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) intentional disregard for a provision of the Rule.” *Krueger*, 809 F.3d at 1115 (citing *United States v. Pennington*, 635 F.2d 1387, 1390 (10th Cir. 1980)). As set forth above, the court does not address whether the warrant fails for constitutional reasons, but limits its analysis to the violation of Rule 41(b). Specifically, does a violation of Rule 41(b) justify suppression of evidence?

In *Krueger*, the Tenth Circuit addressed this question for the first time. (“The Court has not yet had occasion to consider whether suppression is justified when a warrant is issued by a federal magistrate judge who clearly lacks authority to do so under Rule 41(b)(1).” *Krueger*, 809 F.3d at 1115). The court answered that question affirmatively.

In *Krueger*, a Homeland Security Investigations (“HSI”) agent learned that child pornography was being distributed over the internet from an IP address registered to Krueger, a Kansas resident. *Id.* at 1111. The agent obtained a warrant (“Warrant 1”) from a United States magistrate judge in the District of Kansas to search defendant Krueger’s Kansas residence for items such as

computers and cell phones that might be used to depict child pornography. *Id.* Upon executing the warrant, the agent was told by Krueger's roommate that Krueger was in Oklahoma City and may have taken his computer and cell phone with him. *Id.* After an HSI agent in Oklahoma verified Krueger's whereabouts, the agent in Kansas sought and obtained a second warrant ("Warrant 2") from a different magistrate judge in the District of Kansas. *Id.* The second warrant authorized law enforcement to search the Oklahoma residence where Krueger was staying and Krueger's automobile. The warrant was immediately transmitted to an HSI agent in Oklahoma, who executed the warrant and seized Krueger's computer and external hard drive. *Id.* A subsequent search of the devices revealed evidence that Krueger had downloaded and traded child pornography using his peer-to-peer networking account and, as a result, Krueger was charged with distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2). *Id.* at 1112. Krueger filed a motion to suppress, asserting Warrant 2 violated Rule 41(b)(1) because the magistrate judge in the District of Kansas did not have authority to issue a warrant for property already located in Oklahoma. *Id.* After a suppression hearing, the district court granted the motion, concluding that the warrant violated Rule 41(b)(1) and Krueger had demonstrated prejudice in the sense that the Kansas magistrate judge would not have issued Warrant 2 had Rule 41 "been followed to the letter." *Id.* at 1112-13.

On appeal, the Government conceded that Warrant 2 violated Rule 41(b)(1) because the magistrate judge in Kansas had no authority to issue a

warrant for property already located in Oklahoma but argued the district court applied the wrong legal standard in determining that Krueger demonstrated prejudice as a result of the violation. *Id.* at 1113. The Government asserted the appropriate question was not whether any judge in the District of *Kansas* could have issued Warrant 2, but instead was whether any judge in the Western District of *Oklahoma* could have issued the warrant. *Id.* at 1116. The Tenth Circuit disagreed, concluding the Government's proposed approach was too speculative. *Id.* It stated, "[I]nstead of focusing on what the Government *could have* done to comply with Rule 41(b)(1), we conclude that prejudice in this context should be anchored to the facts as they actually occurred." *Id.* Accordingly, it adopted the district court's standard for determining whether defendant had established prejudice and asked "whether the issuing federal magistrate judge could have complied with the Rule." *Id.*

The Government argues *Krueger* is inapposite because there, the agent knew the exact location of the evidence being sought, and was aware the location was in Oklahoma, when he obtained Warrant 2 from a Kansas magistrate judge. Here, in contrast, the agent did not know and could not have known the physical location of Playpen registrants due to the affirmative steps taken by Playpen administrators and users to conceal their illegal activity.

The Government's position finds some support in *Michaud, supra*. In *Michaud*, the district court concluded that although a technical violation of Rule 41 had occurred, suppression was not warranted because the record did

not show that defendant was prejudiced or that the FBI acted intentionally and with deliberate disregard of Rule 41(b). Applying the Ninth Circuit’s definition of prejudice, i.e., “prejudice ‘in the sense that the **search** would not have occurred . . . if the rule had been followed,’” the district court found that the defendant had “no reasonable expectation of privacy of the most significant information gathered by deployment of the **NIT**, Mr. Michaud’s assigned IP address, which ultimately led to Mr. Michaud’s geographic location.” *Id.* at **6-7. Furthermore, the court concluded that “[t]he IP address was public information, like an unlisted telephone number, and eventually could have been discovered.” *Id.* at *7.¹⁰

The Tenth Circuit’s definition of “prejudice” – i.e., “prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed” – is similar to the Ninth Circuit definition. *See Krueger*, 809 F.3d at 1115. Here, the searches of Arterbury’s computer would not have occurred had Rule 41(b) been followed. Absent deployment of the NIT, the physical location of Playpen registrants was not discoverable. *See Macfarlane Affidavit*, Dkt. No. 34-1]. Under the *Krueger/Pennington* framework, the evidence must be suppressed. Rule 41 was clearly violated, and the Oklahoma search would not have occurred had Rule 41(b) been

¹⁰ The court in *Michaud* offered no citation or support for these conclusions. The court indicated that the Government would have no difficulty discovering the IP address for an individual using the Tor network. This is contrary to the undersigned’s understanding of how the Tor network works and is specifically contradicted by the statements set forth in Special Agent Macfarlane’s Affidavit seeking the NIT Warrant in the Eastern District of Virginia. [Dkt. No. 34-1, ¶¶ 8, 9, & 31].

followed. Furthermore, *Krueger* articulates the appropriate inquiry as whether any magistrate judge in the Eastern District of Virginia could have complied with Rule 41 given the facts of this case. The answer to that question is “no.”

The Government also argues that there was no prejudice to Arterbury because he had no reasonable expectation of privacy in his IP address. The Government asserts that the IP address is actually the property of the Internet Service Provider, and that one must disclose this IP address to a third-party in order to access the Internet. Were the IP address obtained from a third-party, the Court might have sympathy for this position. However, here the IP address was obtained through use of computer malware that entered Defendant’s home, seized his computer and directed it to provide information that the Macfarlane affidavit states was unobtainable in any other way. Defendant endeavored to maintain the confidentiality of his IP address, and had an expectation that the Government would not surreptitiously enter his home and secure the information from his computer.

D. The “Good Faith Exception Does Not Apply.”

The most troubling aspect of this case is whether suppression of evidence can be avoided through application of the “good-faith” exception to the exclusionary rule. Having determined that the NIT warrant was void as against Arterbury, the Court must determine whether suppression of the evidence found during the search of his home is warranted. In *U.S. v. Leon*, 468 U.S. 897 (1984), and its companion case, *Mass. v. Sheppard*, 468 U.S. 981 (1984), the Supreme Court recognized a “good faith” or *Leon* exception to the Fourth

Amendment exclusionary rule.¹¹ Under the *Leon* exception, evidence obtained pursuant to a warrant later found to be invalid may be introduced in the government's case-in-chief at the defendant's trial, if a reasonably well-trained officer would have believed that the warrant was valid. The premise for the exception is that there is inadequate justification to apply the exclusionary rule when police obtain a warrant, reasonably relying on its validity, only to later learn that the judge erred in authorizing the search. The court noted in *Leon*, "Penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Leon*, 468 U.S. at 921.

In *Krueger*, the Tenth Circuit held that violation of Rule 41(b) justified suppression of evidence; however, *Krueger* dealt with a single warrant – a warrant issued by a Kansas magistrate judge authorizing search and seizure of property in Oklahoma. This case – and those cited above in ¶IV – presents a different scenario: a second warrant is secured in the appropriate jurisdiction, but probable cause for the second warrant was secured by means of an earlier, invalid warrant. Should the good-faith exception permit officers to rely on the second, valid warrant? Or is the second warrant fatally flawed because of the invalidity of the first warrant?

¹¹ *Leon* "contemplated two circumstances: one in which a warrant is issued and is subsequently found to be unsupported by probable cause and the other in which a warrant is supported by probable cause, but is technically deficient." *U.S. v. Levin*, 2016 WL 1589824 (D.Mass. April 20, 2016) (*quoting U.S. v. Vinnie*, 683 F.Supp. 285, 288 (D. Mass. 1988)).

The Government first contends that the *Leon* exception should apply here because the NIT warrant is a “technical violation” of Rule 41(b). The Court rejects the notion that this case presents nothing more than a “technical violation” of Rule 41. It is true that courts have found that suppression is not warranted in some cases of a Rule 41 violation; however, these have generally involved violations of procedural requirements under Rule 41(a), (c), (d), or (e). *E.g.*, *U.S. v. Rome*, 809 F.2d 665 (10th Cir. 1987) (violation of Rule 41(c)). *See Krueger*, 809 F.3d at 1115, n.7 (collecting cases). However, in this case the violation of Rule 41 goes to the fundamental jurisdiction and “substantive judicial authority” of the magistrate judge to issue the NIT warrant. *Krueger*, 809 F.3d at 1115, n.7 (*citing Berkos*, 543 F.3d at 397).

In *Levin*, the Court relied on *Krueger* and *Berkos* to distinguish technical violations of Rule 41 from the type of violation presented here:

Rule 41, however, has both procedural and substantive provisions — and the difference matters. Courts faced with violations of Rule 41's procedural requirements have generally found such violations to be merely ministerial or technical, and as a result have determined suppression to be unwarranted. By contrast, this case involves a violation of Rule 41(b), which is “a substantive provision[.]” *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008); *see also United States v. Krueger*, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015) (noting that Rule 41(b)(1) “is unique from other provisions of Rule 41 because it implicates substantive judicial authority,” and accordingly concluding that past cases involving violations of other subsections of Rule 41 “offer limited guidance”) (internal quotation marks and citation omitted). Thus, it does not follow from cases involving violations of Rule 41's procedural provisions that the Rule 41(b) violation at issue here — which involves the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the warrant — was simply ministerial. *See United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013) (concluding that a Rule 41(b) violation constitutes

a “jurisdictional flaw” that cannot “be excused as a ‘technical defect’”).

Levin, 2016 WL 1589824, at *7

In *Krueger*, the trial Court noted, “[I]t is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by ‘good faith.’ ” *U.S. v. Krueger*, 998 F.Supp.2d 1032, 1036 (D.Kan. 2014) (quoting *U.S. v. Glover*, 736 F.3d 509, 516 (D.C.Cir. 2013)).

Levin concluded that the good-faith exception was inapplicable to a warrant held to be void *ab initio* under Rule 41(b). *Id.* Other courts have indicated, in dicta, that where evidence is obtained pursuant to a warrant that is void *ab initio*, the good-faith exception does not apply. *See, Levin*, at *10 & n.17 (collecting cases). *See also, State v. Wilson*, 618 N.W.2d 513, 520 (S.D. 2000) (good-faith exception inapplicable to warrant by state judge acting outside territorial jurisdiction); *State v. Nunez*, 634 A.2d 1167, 1171 (D.R.I. 1993) (good faith exception would not apply to a warrant that is void *ab initio*).

Based on the holdings of *Krueger* and *Levin*, I conclude that where the Rule 41 violation goes directly to the magistrate judge’s fundamental authority to issue the warrant, as in the violation presented here, it is not a “technical violation” of the Rule. The warrant is void *ab initio*, suppression is warranted and the good-faith exception is inapplicable.

The Government also argues that because of exigent circumstances the NIT search would have been justified, even had the magistrate judge in Virginia refused to sign it. The Court is not persuaded by this argument either. The

exigent circumstances were the on-going downloading and distribution of child pornography. In this instance, the specific activity at issue was on-going only because the Government opted to keep the Playpen site operating while it employed the NIT. The Government cannot assert exigent circumstances when it had a hand in creating the emergency.

Exclusion of the evidence in this case will serve the remedial and prophylactic purposes of the exclusionary rule, by serving notice to the Government that use of an NIT warrant under the circumstances presented here exceeds a magistrate judge's authority under the Federal Magistrate Judges Act and Rule 41(b) of the Rules of Criminal Procedure.

The NIT Warrant clearly did not comport with Fed. R. Crim. P. 41(b), and, therefore, was invalid *ab initio*. Arterbury was prejudiced by issuance of the NIT Warrant and the Court finds no basis for application of the good faith exception to the exclusionary rule. Accordingly, Defendant's motion to suppress [Dkt. No. 33] must be granted.¹²

V. CONCLUSION

The purpose of Rule 41 is to carry out the mandate of the Fourth Amendment. It binds federal courts and federal law enforcement officers. *Navarro v. U.S.*, 400 F.2d 315, 318-19 (5th Cir 1968), *overruled on other grounds*, *U.S. v. McKeever*, 905 F.2d 829, 833 (5th Cir. 1990)):

¹² Having determined the United States magistrate judge in Virginia exceeded her authority under Fed. R. Crim. P. 41, the court declines to address defendant's remaining arguments in support of suppression.

The obligation of the federal agent is to obey the Rules. They are drawn for the innocent and guilty alike. They prescribe standards for law enforcement. They are designed to protect the privacy of the citizen, unless the strict standards set for searches and seizures are satisfied. That policy is defeated if the federal agent can flout them and use the fruits of his unlawful act either in federal or state proceedings.

Rea v. United States, 350 U.S. 214, 217-18 (1956).

- o The NIT warrant was issued in violation of Rule 41(b).
- o The violation was not a “technical violation” because it implicates “substantive judicial authority.” *Krueger*, 809 F.3d at 1115, n.7.
- o The NIT warrant was, therefore, void *ab initio*. *Levin*, at *8.
- o The *Leon* exception does not apply when an underlying warrant is void *ab initio*. *Levin*, at *11-*12.

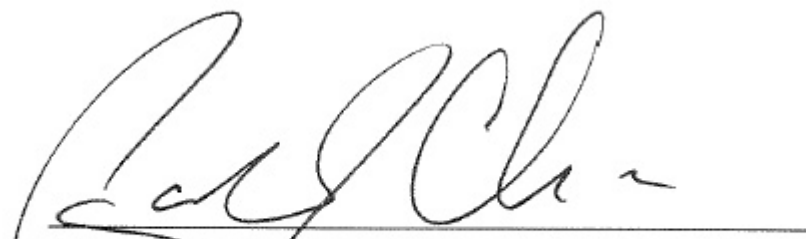
Accordingly, for the reasons set forth above, I recommend the Defendant’s Motion to Suppress [Dkt. No. 33] be **GRANTED**.

OBJECTIONS

The District Judge assigned to this case will conduct a de novo review of the record and determine whether to adopt or revise this Report and Recommendation or whether to recommit the matter to the undersigned. As part of his/her review of the record, the District Judge will consider the parties’ written objections to this Report and Recommendation. In order to expedite this matter for consideration by the District Judge, the period for objections must be shortened. *See* Fed. R. Crim P. 59(b). Therefore, a party wishing to file objections to this Report and Recommendation must do so **by May 2, 2016**. *See* 28 U.S.C. § 636(b)(1) and Fed. R. Crim. P. 59(b). The failure to file timely

written objections to this Report and Recommendation waives a party's right to review. Fed. R. Crim P. 59(b).

DATED this 25th day of April 2016.



Paul J. Cleary
United States Magistrate Judge



U.S. Department of Justice

Criminal Division

13-CR-B

Assistant Attorney General

Washington, D.C. 20530

September 18, 2013

The Honorable Reena Raggi
Chair, Advisory Committee on the Criminal Rules
704S United States Courthouse
225 Cadman Plaza East
Brooklyn, NY 11201-1818

Dear Judge Raggi:

The Department of Justice recommends an amendment to Rule 41 of the Federal Rules of Criminal Procedure to update the provisions relating to the territorial limits for searches of electronic storage media. The amendment would establish a court-supervised framework through which law enforcement can successfully investigate and prosecute sophisticated Internet crimes, by authorizing a court in a district where activities related to a crime have occurred to issue a warrant – to be executed via remote access – for electronic storage media and electronically stored information located within or outside that district. The proposed amendment would better enable law enforcement to investigate and prosecute botnets and crimes involving Internet anonymizing technologies, both which pose substantial threats to members of the public.

Background

Rule 41(b) of the Federal Rules of Criminal Procedure authorizes magistrate judges to issue search warrants. In most circumstances, search warrants issue for property that is located within the judge's district. Currently, Rule 41(b) authorizes out-of-district search warrants for: (1) property in the district when the warrant is issued that might be moved outside the district before the warrant is executed; (2) tracking devices, which may be monitored outside the district if installed within the district; (3) investigations of domestic or international terrorism; and (4) property located in a United States territory or a United States diplomatic or consular mission.

Rule 41(b) does not directly address the special circumstances that arise when officers execute search warrants, via remote access, over modern communications networks such as the Internet. Rule 41 should be amended to address two increasingly common situations: (1) where the warrant sufficiently describes the computer to be searched but the district within which that computer is located is unknown, and (2) where the investigation requires law enforcement to coordinate searches of numerous computers in numerous districts.

The first of these circumstances – where investigators can identify the target computer, but not the district in which it is located – is occurring with greater frequency in recent years. Criminals are increasingly using sophisticated anonymizing technologies when they engage in crime over the Internet. For example, a fraudster exchanging email with an intended victim or a child abuser sharing child pornography over the Internet may use proxy services designed to hide his or her true IP address. Proxy services function as intermediaries for Internet communications: when one communicates through an anonymizing proxy service, the communications pass through the proxy, and the recipient of the communications receives the proxy's IP address, rather than the originator's true IP address. There is a substantial public interest in catching and prosecuting criminals who use anonymizing technologies, but locating them can be impossible for law enforcement absent the ability to conduct a remote search of the criminal's computer. Law enforcement may in some circumstances employ software that enables it through a remote search to determine the true IP address or other identifying information associated with the criminal's computer.

Yet even when investigators can satisfy the Fourth Amendment's threshold for obtaining a warrant for the remote search – by describing the computer to be searched with particularity and demonstrating probable cause to believe that the evidence sought via the remote search will aid in a particular apprehension or conviction for a particular offense – a magistrate judge may decline to issue the requested warrant. For example, in a fraud investigation, one magistrate judge recently ruled that an application for a warrant for a remote search did not satisfy the territorial jurisdiction requirements of Rule 41. *See In re Warrant to Search a Target Computer at Premises Unknown*, ___ F. Supp. 2d ___, 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013) (noting that “there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology”).

Second, criminals are using multiple computers in many districts simultaneously as part of complex criminal schemes, and effective investigation and disruption of these schemes often requires remote access to Internet-connected computers in many different districts. For example, thefts in one district may be facilitated by sophisticated attacks launched from computers in multiple other districts. An increasingly common form of online crime involves the surreptitious infection of multiple computers with malicious software that makes them part of a “botnet” – a collection of compromised computers under the remote command and control of a criminal. Botnets may range in size from hundreds to millions of compromised computers, including home, business, and government systems. Botnets are a significant threat to the public: they are used to conduct large-scale denial of service attacks, steal personal and financial data, and distribute malware designed to invade the privacy of users of the host computers.

Effective investigations of these sophisticated crimes often require law enforcement to act in many judicial districts simultaneously. Under the current Rule 41, however, except in cases of domestic or international terrorism, investigators may need to coordinate with agents,

prosecutors, and magistrate judges in every judicial district in which the computers are known to be located to obtain warrants authorizing the remote access of those computers. For example, a large botnet investigation is likely to require action in all 94 districts, but coordinating 94 simultaneous warrants in the 94 districts would be impossible as a practical matter. At a minimum, requiring so many magistrate judges to review virtually identical probable cause affidavits wastes judicial and investigative resources and creates delays that may have adverse consequences for the investigation. Authorizing a court in a district where activities related to a crime have occurred to issue a warrant for electronic storage media within or outside the district would better align Rule 41 with the extent of constitutionally permissible warrants and remove an unnecessary obstruction currently impairing the ability of law enforcement to investigate botnets and other multi-district Internet crimes.

Thus, while the Fourth Amendment permits warrants to issue for remote access to electronic storage media or electronically stored information, Rule 41's language does not anticipate those types of warrants in all cases. Amendment is necessary to clarify the procedural rules that the government should follow when it wishes to apply for these types of warrant.

Language of Proposed Amendment

Our proposed amendment includes two parts. First, we propose adding the following language at the end of subsection (b):

and (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant, to be executed via remote access, for electronic storage media or electronically stored information located within or outside that district.

Second, we propose adding the following language at the end of subsection (f)(1)(C):

In a case involving a warrant for remote access to electronic storage media or electronically stored information, the officer executing the warrant must make reasonable efforts to serve a copy of the warrant on an owner or operator of the storage media. Service may be accomplished by any means, including electronic means, reasonably calculated to reach the owner or operator of the storage media. Upon request of the government, the magistrate judge may delay notice as provided in Rule 41(f)(3).

Discussion of Proposed Amendment

The proposed amendment authorizes a court with jurisdiction over the offense being investigated to issue a warrant to remotely search a computer if activities related to the crime under investigation have occurred in the court's district. In other circumstances, the Rules or federal law recognize that it can be appropriate to give magistrate judges nationwide authority to issue search warrants. For example, in terrorism investigations, the current Rule 41(b)(3) allows a magistrate judge "in any district in which activities related to the terrorism may have occurred" to issue a warrant "for a person or property within or outside that district." This approach is also similar to the current rule for a warrant requiring communication service providers to disclose electronic communications: a court with "jurisdiction over the offense being investigated" can issue such a warrant. *See* 18 U.S.C. §§ 2703(a) & 2711(3)(A)(I); *United States v. Bansal*, 663 F.3d 634, 662 (3d Cir. 2011); *United States v. Berkos*, 543 F.3d 392, 397-98 (7th Cir. 2008). Mobile tracking device warrants may authorize the use of tracking devices outside the jurisdiction of the court, so long as the device was installed in that jurisdiction. Fed. R. Crim. P. 41(b)(4); 18 U.S.C. § 3117(a). In the proposed amendment, the phrase "any district where activities related to a crime may have occurred" is the same as the language setting out the jurisdictional scope of Rule 41(b)(3).

The amendment provides that notice of the warrant may be accomplished by any means reasonably calculated to reach an owner or operator of the computer or – as stated in the amendment, which uses existing Rule 41 language – the "storage media or electronically stored information." In many cases, notice is likely to be accomplished electronically; law enforcement may not have a computer owner's name and street address to provide notice through traditional mechanisms. The amendment also requires that the executing officer make reasonable efforts to provide notice. This standard recognizes that in unusual cases, such as where the officer cannot reasonably determine the identity or whereabouts of the owner of the storage media, the officer may be unable to provide notice of the warrant. *Cf.* 18 U.S.C. § 3771(c)(1) (officers "shall make their best efforts to see that the crime victims are notified of ... the rights described in subsection (a)").

In light of the presumption against international extraterritorial application, and consistent with the existing language of Rule 41(b)(3), this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries. The Fourth Amendment does not apply to searches of the property of non-United States persons outside the United States, *see United States v. Verdugo-Urquidez*, 494 U.S. 259, 261 (1990), and the Fourth Amendment's warrant requirement does not apply to searches of United States persons outside the United States. *See United States v. Stokes*, ___ F.3d ___, 2013 WL 3948949 at *8-*9 (7th Cir. Aug. 1, 2013); *In re Terrorist Bombings*, 552 F.3d 157, 170-71 (2d Cir. 2008). Instead, extraterritorial searches of United States persons are subject to the Fourth Amendment's "basic requirement of reasonableness." *Stokes*, 2013 WL 3948949 at

The Honorable Reena Raggi

Page 5

*9; *see also In re Terrorist Bombings*, 552 F.3d at 170 n.7. Under this proposed amendment, law enforcement could seek a warrant either where the electronic media to be searched are within the United States or where the location of the electronic media is unknown. In the latter case, should the media searched prove to be outside the United States, the warrant would have no extraterritorial effect, but the existence of the warrant would support the reasonableness of the search.

* * *

We believe that timely and thorough consideration of this proposed amendment by the Advisory Committee is appropriate. We therefore ask that the Committee act at its November meeting to establish a subcommittee to examine this important issue. Criminals are increasingly using sophisticated technologies that pose technical challenges to law enforcement, and remote searches of computers are often essential to the successful investigation of botnets and crimes involving Internet anonymizing technologies. Moreover, this proposal would ensure a court-supervised framework through which law enforcement could successfully investigate and prosecute such crimes.

We look forward to discussing this with you and the Committee.

Sincerely,



Mythili Raman
Acting Assistant Attorney General

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