U.S. Department of Justice

Criminal Division

Office of Enforcement Operations *Washington, D.C. 20530*

VIA Electronic Mail

May 15, 2020

Jonathan Manes, Esq.
Roderick & Solange MacArthur Justice Center
160 E. Grand Ave., Sixth Floor
Chicago, IL 60611
jonathan.manes@law.northwestern.edu

Request No. CRM-300680988
Privacy International et al. v. Federal Bureau of Investigation, et al.,18-cv-1488 (W.D.N.Y.)

Dear Mr. Manes:

This is the sixth installment of the Criminal Division's rolling production regarding your Freedom of Information Act request dated September 10, 2018, for certain records pertaining to "computer network exploitation" or "network investigative techniques." Your request is currently in litigation, Privacy International, et al. v. Federal Bureau of Investigation, et al., 18-cv-1488 (W.D.N.Y.). You should refer to this case number in any future correspondence with this Office. This request is being processed in accordance with the interpretation and parameters set forth by defendants in the July 12, 2019, letter to you from Senior Trial Counsel Marcia Sowles, as well as subsequent conversations regarding the Criminal Division's processing of the request.

Please be advised that a search has been conducted in the appropriate sections, and we are continuing to review and process potentially responsive records. After carefully reviewing 518 pages of records, I have determined that 63 pages are responsive to your request and are appropriate for release in full, copies of which are enclosed.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may contact Senior Trial Counsel Marcia K. Sowles by phone at (202) 514-4960, by email at Marcia.Sowles@usdoj.gov, or by mail at the Civil Division, Federal Programs Branch, 1100 L Street, N.W., Room 10028, Washington, D.C. 20005, for any further assistance and to discuss any aspect of your request.

Although I am aware that your request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you of your right to an administrative appeal of this determination. If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th

Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account on the following website: https://foiastar.doj.gov. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,

Gail Brodfuehrer for

Amanda Marchand Jones
Chief
FOIA/PA Unit

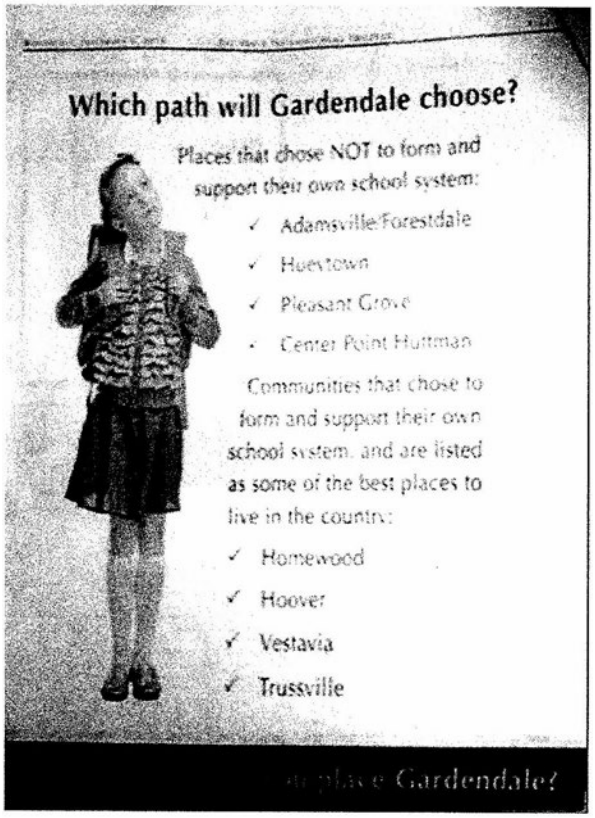
cc: Marcia K. Sowles
Senior Trial Counsel
Civil Division, Federal Programs Branch
1100 L Street, N.W., Room 11028
Washington, D.C. 20005
Marcia.Sowles@usdoj.gov

Michael S. Cerrone
michael.cerrone@usdoj.gov

Enclosures

Appendix R

Plaintiff Exhibit B



KEY NUMBER SYSTEM

UNITED STATES of America

v.

James Ryan TAYLOR, Defendant.

2:16–cr–00203–KOB–JEO–1

United States District Court,
N.D. Alabama, Southern Division.

Signed 04/24/2017

Background: Defendant, charged with receipt of child pornography and with possession and accessing child pornography with intent to view, moved to suppress evidence.

Holdings: The District Court, Karon Owen Bowdre, Chief District Judge, held that:

(1) warrant was supported by probable cause;

(2) warrant was sufficiently particular to satisfy Fourth Amendment requirements;

(3) warrant was void ab initio; but

(4) officers were objectively reasonable in relying on warrant.

Motion denied.

1. Searches and Seizures ⇨13.1

A search for purposes of the Fourth Amendment does not require a physical

trespass to property. U.S.C.A. Const. Amend. 4.

2. Searches and Seizures ⚿26

In absence of a trespass, application of the Fourth Amendment to a search depends on whether the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action. U.S.C.A. Const. Amend. 4.

3. Searches and Seizures ⚿26

An individual raising a Fourth Amendment challenge to a search must demonstrate both a subjective expectation of privacy in the object of the challenged search, and that society is prepared to accept that expectation as objectively reasonable. U.S.C.A. Const. Amend. 4.

4. Searches and Seizures ⚿26

Third-party doctrine applies in a Fourth Amendment challenge to a search when someone voluntarily disclosed information to a third party; an expectation of privacy in such information fails the objectively reasonable prong of test for determining whether a Fourth Amendment violation occurred. U.S.C.A. Const. Amend. 4.

5. Searches and Seizures ⚿21

Under the Fourth Amendment, Government may not employ sense-enhancing technology that is not in general public use to obtain information that could not otherwise have been obtained without physical intrusion into a constitutionally protected area. U.S.C.A. Const. Amend. 4.

6. Obscenity ⚿274(2)
Telecommunications ⚿1439

Defendant had an objectively reasonable expectation of privacy in information gathered by Government through its use of network investigative technique (NIT) to obtain identifying information for his computer, including his internet protocol (IP) address, as result of his act of logging into child pornography website, such that Government's actions in deploying NIT constituted a search within meaning of the Fourth Amendment; given his use of a computer program designed to provide internet privacy protections, defendant could reasonably expect that his computer's contents would remain private, and his computer was located in his home at time he used it to access a child pornography website. U.S.C.A. Const. Amend. 4.

7. Obscenity ⚿287(3)
Telecommunications ⚿1473

Use of network investigative technique (NIT) to obtain identifying information regarding computer users or administrators in other parts of the United States who logged into child pornography website being operated by Government computer server located in Eastern District of Virginia, was objectively reasonable and not a flagrant disregard of warrant's terms; warrant authorized search and seizure of the server and the activating computers, wherever located. U.S.C.A. Const. Amend. 4.

8. Criminal Law ⚿392.16(5)

Absent flagrant disregard of terms of search warrant, items seized outside scope of the warrant should not be suppressed; "flagrant disregard" means that executing officer's conduct exceeds any reasonable interpretation of warrant's provisions. U.S.C.A. Const. Amend. 4.

9. Criminal Law ⚿392.16(5)

Court seeking to determine whether such flagrant disregard of terms of search warrant occurred as to warrant suppression of items seized outside scope of the warrant examines whether executing officer's conduct exceeds any reasonable interpretation of the warrant's provisions, considering such things as scope of the warrant, behavior of the searching agents, conditions under which the search was

conducted, and nature of the evidence being sought. U.S.C.A. Const. Amend. 4.

10. Searches and Seizures ⚿123.1

Search warrant may incorporate by reference documents or affidavits attached to the warrant if warrant uses proper words of incorporation. U.S.C.A. Const. Amend. 4.

11. Obscenity ⚿282(2)
Telecommunications ⚿1466

Warrant authorizing use of network investigative technique (NIT) to obtain identifying information regarding computer users or administrators who logged into child pornography website being operated by computer server controlled by Government, was supported by probable cause to conclude that the computers of website members who logged into the website would contain evidence of at least one child pornography-related crime; website existed to enable access to child pornography and nature of the website was such that accessing it required numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble on the website without understanding its purpose and content. U.S.C.A. Const. Amend. 4.

12. Searches and Seizures ⚿113.1

In determining whether probable cause exists, a magistrate must simply make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place. U.S.C.A. Const. Amend. 4.

13. Searches and Seizures ⚿200

District court's job in determining whether a search warrant is supported by probable cause is not to conduct a de novo review, but to consider whether issuing magistrate judge had a substantial basis for concluding that probable cause existed. U.S.C.A. Const. Amend. 4.

14. Searches and Seizures ⚿126

A warrant must be tailored to provide for a search only of those places agents have probable cause to believe contain evidence of a crime. U.S.C.A. Const. Amend. 4.

15. Obscenity ⚿286(4)
Telecommunications ⚿1470

Warrant authorizing use of network investigative technique (NIT) to obtain identifying information regarding computer users or administrators who logged into child pornography website being operated by computer server controlled by Government was sufficiently particular to satisfy Fourth Amendment requirements; attachments to warrant clearly identified places to be searched as the computer server and computers logging into the website, and identified information to be seized by means of an itemized list of seven pieces of information. U.S.C.A. Const. Amend. 4.

16. Searches and Seizures ⚿126

For purposes of Fourth Amendment's requirement that search warrant particularly describe place to be searched, the warrant need only describe the premises in such a way that searching officer may with reasonable effort ascertain and identify the place intended. U.S.C.A. Const. Amend. 4.

17. Searches and Seizures ⚿126

For purposes of Fourth Amendment's requirement that search warrant particularly describe items to be seized, a description is sufficiently particular when it enables searcher to reasonably ascertain and identify the things authorized to be seized; elaborate specificity is unnecessary. U.S.C.A. Const. Amend. 4.

18. Obscenity ⚿286(4)
Telecommunications ⚿1473

Warrant to search defendant's computer for images of child pornography suf-

ficiently authorized offsite forensic testing of the computer; affidavit attached to the warrant included non-exclusive list of techniques that might be used to search seized electronic information, and the Federal Rules of Criminal Procedure specifically authorized a later review of electronic storage media or electronically stored information consistent with the warrant. U.S.C.A. Const. Amend. 4; Fed. R. Crim. P. 41(e)(2)(B).

19. Obscenity ⚿280
Telecommunications ⚿1463

Warrant, issued in Eastern District of Virginia, where computer server that was operating a child pornography website was located, which authorized use of network investigative technique (NIT) to retrieve information from computers of persons who logged into the website, was void ab initio; warrant exceeded issuing magistrate's authority by authorizing a search of computers located in other Districts, and defendant's computer was located in Alabama. U.S.C.A. Const. Amend. 4; 28 U.S.C.A. § 636(a).

20. Obscenity ⚿280
Telecommunications ⚿1463

Warrant, issued in Eastern District of Virginia, where computer server that was operating a child pornography website was located, which authorized use of network investigative technique (NIT) to retrieve information from computers of persons who logged into the website, was issued in violation of Rule of Criminal Procedure governing authority to issue warrants; that Rule required that property to be searched be located in same District as the issuing magistrate, but defendant's computer was located in Alabama. U.S.C.A. Const. Amend. 4; Fed. R. Crim. P. 41(b).

21. Criminal Law ⚿392.16(1)

Unless a clear constitutional violation occurs, noncompliance with Rule of Criminal Procedure governing authority to issue warrants requires suppression of evidence only where (1) there was 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) there is evidence of intentional and deliberate disregard of a provision in the Rule. U.S.C.A. Const. Amend. 4; Fed. R. Crim. P. 41.

22. Criminal Law ⚿392.38(12)

Law enforcement officers were objectively reasonable in relying on warrant which authorized use of network investigative technique (NIT) to retrieve information from computers of persons who logged into child pornography website, and therefore good faith exception to the exclusionary rule applied to information obtained pursuant to that warrant; no information in warrant affidavit was false, magistrate judge did not wholly abandon her judicial role and did not make a determination completely outside the realm of reason, warrant was supported by probable cause and complied with Fourth Amendment's particularity requirements, making it facially valid, and exclusion of the evidence would serve little deterrent purpose, given that it was the mistaken conduct of the magistrate judge, rather than of the officers, that invalidated the warrant. U.S.C.A. Const. Amend. 4; Fed. R. Crim. P. 41(b).

23. Criminal Law ⚿392.37

Fact that a Fourth Amendment violation occurred does not necessarily mean that exclusionary rule applies to forbid use of improperly obtained evidence at trial. U.S.C.A. Const. Amend. 4.

24. Criminal Law ⚿392.37

To trigger exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice

system; this balancing test is an objective one that does not assess officers' subjective intent. U.S.C.A. Const. Amend. 4.

25. Criminal Law ⚿392.38(7)

As to warrants, the good faith exception does not apply where (1) issuing judge is misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth, (2) the judge wholly abandoned his judicial role, (3) affidavit on which warrant was based was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable, or (4) warrant is so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that executing officers cannot reasonably presume it to be valid. U.S.C.A. Const. Amend. 4.

26. Criminal Law ⚿392.16(1)

Magistrate judge's mistaken belief that she had jurisdiction to issue search warrant, absent any indicia of reckless conduct by the agents, does not warrant suppression. U.S.C.A. Const. Amend. 4.

United States Marshal, US Attorney Joyce White Vance, Jacquelyn Mather Hutzell, United States Attorney's Office, US Probation, United States Probation Office, Birmingham, AL, for United States of America.

Kevin L. Butler, Federal Public Defender, Birmingham, AL, for Defendant.

MEMORANDUM OPINION

KARON OWEN BOWDRE, CHIEF UNITED STATES DISTRICT JUDGE

The United States filed this and many other child pornography criminal cases following an extensive FBI sting operation that resulted in the seizure of a website, "Playpen," dedicated to the advertisement and distribution of child pornography. After taking over Playpen, the FBI first obtained a warrant in the Eastern District of Virginia that enabled it to seize Defendant's Internet Protocol (IP) address and other identifying information. With that information, the FBI obtained and executed a second warrant in the Northern District of Alabama to search Defendant's home and seize certain property, including a solid state drive that contained child pornography. The Government charged Defendant James Ryan Taylor with receipt of child pornography under 18 U.S.C. § 2252A(a)(2) and with possession and accessing child pornography with intent to view under 18 U.S.C. §§ 2252A(a)(5)(B) & (b)(2). (Doc. 1).

This case comes before the court on Defendant's Motion to Suppress Evidence. (Doc. 21). The Government has filed a Response (doc. 26) and Supplemental Response. (Doc. 30). The court **WILL DENY** the Motion to Suppress.

I. Statement of Facts

From September 2014 to February 2015, FBI agents monitored "Playpen," a website dedicated to the advertisement and distribution of child pornography. The Playpen website was only accessible via "The Onion Router" or "Tor" network, which is part of what is sometimes referred to as the "Dark Web" because of its anonymity features.[1] On February 20, 2015, the FBI obtained a warrant in the Eastern District of Virginia to deploy a Network Investigative Technique ("NIT") on the Playpen website to obtain identifying information about the computers accessing the site. That warrant lies at the

1. *See Hacker Lexicon: What is the Dark Web?,* WIRED, https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (Nov. 19, 2014).

heart of this case. The FBI's warrant application included the affidavit of FBI Special Agent Douglas Mcfarlane, who investigated the Playpen website. Agent Mcfarlane's affidavit describes in detail the website, the Tor network, and other relevant facts from the FBI's investigation.

A. The Tor Network

Tor is a program designed to provide Internet privacy protections by restricting the kinds of information a website can collect from a user, particularly a computer's IP address.[2] The Tor software permits a user to access the Tor network, a network of computers that obscures the identity of users by rerouting a user's IP address through "layers" of relay points, so that the IP address at which a signal exits (the "exit node") is not the IP address at which the signal originated. This process makes it impossible to "peel back the layers of the onion" to discover the originating IP address, which in turn marks the user's geographic location and can be used to identify the user.

Websites accessible only on the Tor network, termed "hidden services," are not searchable through Google or other search engines; rather, a user must employ the Tor software and know the exact address of a particular hidden service to access it. A user could obtain the address from communications with other individuals who use the hidden service or from an Internet posting describing the hidden service and giving its address. The Playpen website, for example, was listed on a Tor hidden service page dedicated to pedophilia and child pornography. Website addresses on the Tor network consist of a randomized series of characters produced by an algorithm and end in ".onion." Tor obscures the IP addresses of hidden services, meaning that law enforcement cannot determine the location of the computer hosting a hidden service.

Originally designed and employed by the U.S. Navy, the Tor network is used for many legal purposes and is freely available for download at https://www.torproject.org.

B. The Playpen Website

The Playpen website was located at different ".onion" URLs depending on when it was accessed; the administrator of Playpen periodically moved the website from one URL to another, without otherwise altering it, in part to avoid detection by law enforcement. The website's homepage featured the word "Playpen" and two images of partially clothed prepubescent females with their legs spread apart. Beneath the logo was text stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Special Agent Mcfarlane's affidavit explains that "[n]o cross-board reposts" refers to not posting files from other websites and ".7z preferred" denotes a method of compressing large files for distribution. The homepage also included a login section and a link to the registration page. The registration terms on the registration page instructed users to not enter a real email address and stated that "[f]or your own security" users should not post identifying information and should disable other potentially identifying browser features.

2. " 'Internet Protocol address' or 'IP address' refers to a unique number used by a computer to access the Internet. IP addresses can be 'dynamic,' meaning that the Internet Service Provider ('ISP') assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be 'static,' if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers." (Doc. 21–1 at 8–9).

Upon logging in, a user would be immediately directed to a Playpen directory that listed message boards divided into more than fifty topics and subtopics that largely referred to child pornography, child erotica, and child sexual abuse. For example, the topics included "Pre-teen Videos" and "Pre-teen Photos," both subdivided into "Girls HC [hardcore]" and "Girls SC [softcore]/NN [non-nude]" and "Boys HC" and "Boys SC/NN"; "Kinky Fetish," and "Family [Playpen]—Incest." [3] Agent Mcfarlane's affidavit details numerous examples of child pornography posted on the Playpen message boards under these topics and others.

C. The FBI Investigation & Network Investigative Technique ("NIT")

Upon receiving on a tip from a foreign law enforcement agency, the FBI identified the Playpen website's host IP address and seized a copy of the server containing the Playpen website, storing that copy on a server in the Eastern District of Virginia. The FBI arrested the Playpen website administrator and assumed administrative control of Playpen. Because traditional methods of obtaining IP addresses would only reveal the "exit node" IP addresses of Playpen users, the FBI sought and received permission to deploy a Network Investigative Technique (NIT) from the server in the Eastern District of Virginia to locate and identify Playpen users. A magistrate judge in the Eastern District of Virginia signed the warrant permitting the FBI to deploy the NIT.

The NIT consisted of computer code that instructed a user's computer to transmit specific information to a government-controlled computer. The NIT operated by downloading to a user's browser along with other content from the Playpen website. Though the warrant authorized the FBI to deploy the NIT to any computer logging into the Playpen website, in executing the warrant the FBI only deployed the NIT to computers accessing actual pornography in certain Playpen forums. *See* (Doc. 30–1 at 18–19). That is, when a user clicked on a designated pornographic image or video on Playpen, the website on the server in the Eastern District of Virginia transmitted the image or video along with the NIT code. Once downloaded to a user's browser, the NIT instructed a user's computer—the "activating computer"—to send specific information to the government computer.

In the section of the NIT warrant application requesting information about the person or property to be searched, the application refers to Attachment A. Attachment A explains that the warrant authorizes the use of a NIT on a computer server operating the Playpen website and that the server is located at a government facility in the Eastern District of Virginia. Attachment A also states that the NIT will obtain the information specified in Attachment B from the "activating computers" of any user or administrator who logs into the Playpen website.

Similarly, in the section requesting information about the property to be seized, the application refers to Attachment B. Attachment B explains that the NIT would collect the following seven pieces of information:

> 1. The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;

3. Agent Mcfarlane's affidavit explains that "hardcore" refers to depictions of sexually penetrative explicit conduct; "softcore" refers to depictions of non-penetrative sexually explicit conduct; and "non-nude" refers to depictions of fully or partially clothed subjects.

2. A unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating" computers. That unique identifier 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." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;

6. the "activating" computer's active operating system username; and

7. The "activating" computer's Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

Both Attachments A and B, along with Agent Mcfarlane's affidavit, were included with the NIT warrant application.

D. Motions to Suppress in Other Cases

As of today, at least 44 district courts have ruled on motions to suppress the information seized pursuant to the NIT warrant. Twelve of these courts have found that the warrant did not violate § 636(a) of the Federal Magistrates Act and/or Rule 41 of the Federal Rules of Criminal Procedure. *U.S. v. Jones*, No. 3:16–cr–026, 230 F.Supp.3d 819, 2017 WL 511883 (S.D. Ohio February 2, 2017); *U.S. v. Austin*, No. 3:16–cr–00068, 230 F.Supp.3d 828, 2017 WL 496374 (M.D. Tenn. Feb. 2, 2017); *U.S. v. Bee*, No. 16-00002-01-CR-W-GAF, 2017 WL 424889 (W.D. Mo. Jan. 31, 2017) (adopting magistrate judge's report and recommendation); *U.S. v. Sullivan*, No. 1:16–cr–270, 2017 WL 201332 (N.D. Ohio Jan. 18, 2017); *U.S. v. Dzwonczyk*, No. 4:16-CR-3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016) (adopting magistrate judge's report and recommendation); *U.S. v. McLamb*, No. 2:16cr92, 2016 WL 6963046 (E.D. Va. Nov. 28, 2016); *U.S. v. Lough*, No. 1:16CR18, 221 F.Supp.3d 770, 2016 WL 6834003 (N.D.W. Va. Nov. 18, 2016); *U.S. v. Johnson*, No. 15–00340–01–CR–W–GAF, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016) (adopting in part magistrate judge's report and recommendation); *U.S. v. Smith*, No. 4:15–CR–00467 (S.D. Tex. Sept. 28, 2016); *U.S. v. Jean*, 207 F.Supp.3d 920 (W.D. Ark. 2016); *U.S. v. Eure*, No. 2:16cr43, 2016 WL 4059663 (E.D. Va. July 28, 2016); *U.S. v. Matish*, 193 F.Supp.3d 585 (E.D. Va. 2016); *U.S. v. Darby*, 190 F.Supp.3d 520 (E.D. Va. 2016); *cf. U.S. v. Laurita*, No. 8:13CR107, 2016 WL 4179365 (D. Neb. Aug. 5, 2016) (adopting magistrate judge's report and recommendation) (finding no violation of the statute or Rule by a NIT warrant issued in a different pornography website investigation).

Twenty-two district courts have found that the warrant did violate § 636(a) and/or Rule 41(b), but that the violation did not warrant suppression. *U.S. v. Gaver*, 3:16–cr–88, 2017 WL 1134814 (S.D. Ohio Mar. 27, 2017); *U.S. v. Perdue*, No. 3:16-CR-305-D(1), 2017 WL 661378 (N.D.

Tex. Feb. 17, 2017); *U.S. v. Pawlak*, No. 3:16-CR-306-D(1), 2017 WL 661371 (N.D. Tex. Feb. 17, 2017); *U.S. v. Kahler*, No. 16–cr–20551, 2017 WL 586707 (E.D. Mich. Feb. 14, 2017); *U.S. v. Deichert*, No. 5:16-CR-201-FL-1, 232 F.Supp.3d 772, 2017 WL 398370 (E.D.N.C. Jan. 28, 2017); *U.S. v. Vortman*, No. 16–cr–00210–THE–1, 2016 WL 7324987 (N.D. Cal. Dec. 16, 2016); *U.S. v. Hammond*, No. 16–cr–00102–JD–1, —— F.Supp.3d ——, 2016 WL 7157762 (N.D. Cal. Dec. 8, 2016); *U.S. v. Duncan*, No. 3:15–cr–00414–JO, 2016 WL 7131475 (D. Or. Dec. 6, 2016); *U.S. v. Owens*, No. 16-CR-38-JPS, 2016 WL 7053195 (E.D. Wis. Dec. 5, 2016) (adopting magistrate judge's report and recommendation); *U.S. v. Stepus*, No. 15-30028-MGM, 2016 WL 6518427 (D. Mass. Oct. 28, 2016); *U.S. v. Scarbrough*, No. 3:16-CR-35, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016) (adopting magistrate judge's report and recommendation); *U.S. v. Allain*, No. 15–cr–10251, 2016 WL 5660452 (D. Mass. Sept. 29, 2016); *U.S. v. Broy*, 209 F.Supp.3d 1045 (C.D. Ill. 2016); *U.S. v. Knowles*, 207 F.Supp.3d 585 (D.S.C. 2016); *U.S. v. Ammons*, 207 F.Supp.3d 732 (W.D. Ky. 2016); *U.S. v. Torres*, No. 5:16-CR-285-DAE, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016); *U.S. v. Henderson*, No. 15–cr–00565–WHO–1, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *U.S. v. Adams*, No. 6:16–cr–11–Orl–40–GJK, 2016 WL 4212079 (M.D. Fla. Aug. 8, 2016); *U.S. v. Rivera*, 2:15–cr–00266–CJB–KWR (E.D. La. July 20, 2016); *U.S. v. Werdene*, 188 F.Supp.3d 431 (E.D. Penn. 2016); *U.S. v. Stamper*, No. 1:15cr109, 2016 WL 695660 (S.D. Ohio February 19, 2016); *U.S. v. Michaud*, No. 3:15–cr–05351–RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

A few courts have declined to decide whether the statute and/or the Rule authorized the warrant but found that exclusion was unwarranted regardless. *U.S. v. Schuster*, No. 1:16–cr–51, 2017 WL 1154088 (S.D. Ohio Mar. 28, 2017); *U.S. v. Tran*, No. 16-10010-PBS, 226 F.Supp.3d 58, 2016 WL 7468005 (D. Mass. Dec. 28, 2016); *U.S. v. Kienast*, No. 16-CR-103, 2016 WL 6683481 (E.D. Wis. Nov. 14, 2016); *U.S. v. Anzalone*, 208 F.Supp.3d 358 (D. Mass. 2016); *U.S. v. Acevedo–Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *U.S. v. Epich*, No. 15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016) (adopting magistrate judge's report and recommendation).

Four courts have suppressed the evidence. *U.S. v. Croghan*, 209 F.Supp.3d 1080 (S.D. Iowa 2016); *U.S. v. Workman*, 205 F.Supp.3d 1256 (D. Colo. 2016); *U.S. v. Arterbury*, No. 15–CR–182–JHP (N.D. Okla. May 17, 2016) (adopting magistrate judge's report and recommendation); *U.S. v. Levin*, 186 F.Supp.3d 26 (D. Mass. 2016).

E. Search of Mr. Taylor's Residence & Indictment

The data gathered from the NIT revealed that Playpen user "Wilcox1" was linked to a computer with the host name "RyansComputer," with computer login name "Ryan." (Doc. 26–2 at 31). Wilcox1 accessed several images of child pornography on Playpen on March 1, 2015. Through an administrative subpoena, the FBI further determined that the IP address associated with "Wilcox1" was assigned to Mr. Taylor at his residence in Birmingham, Alabama. A magistrate judge in the Northern District of Alabama authorized a search warrant for Mr. Taylor's residence, which the FBI executed on January 4, 2016.

The FBI seized a laptop, a hard drive, a solid state drive, and a USB drive from Mr. Taylor's residence. Both parties acknowledge that the initial FBI analysis of these devices did not reveal any child pornography stored on them; however, a sec-

ond analysis of the devices at the FBI's Digital Analysis and Research Center found child pornography on the solid state drive. The Government subsequently indicted Mr. Taylor. (Doc. 1).

II. Discussion

Mr. Taylor argues that the search and seizure of his property in the Northern District of Alabama exceeded the scope of the NIT warrant. He further argues that the warrant was invalid under the Fourth Amendment's probable cause and particularity mandates, Rule 41(b) of the Federal Rules of Criminal Procedure, and 28 U.S.C. § 636(a), a provision of the Federal Magistrates Act. Mr. Taylor asserts that the pornography seized pursuant to the residential warrant, which was authorized based on the information seized by the NIT, should be suppressed as fruit of the poisonous tree.

However, the court will first examine the question of whether the FBI's execution of the NIT warrant constituted a search within the meaning of the Fourth Amendment, such that the Government required a warrant at all. In addition to determining whether the Fourth Amendment governs this case, this inquiry addresses precisely what property was searched and seized, which is necessary to the Rule 41(b) and § 636(a) analysis.

A. Whether Execution of the NIT Constituted a Fourth Amendment Search

[1, 2] The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. A search for purposes of the Fourth Amendment does not require a physical trespass to property. *See Katz v. U.S.*, 389 U.S. 347, 353, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). In the absence of a trespass, "the application of the Fourth Amendment depends on whether the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action." *See Smith v. Maryland*, 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979).

[3, 4] Under the two-part *Katz* test, an individual must demonstrate both a subjective expectation of privacy in the object of the challenged search, and that society is prepared to accept that expectation as objectively reasonable. *California v. Ciraolo*, 476 U.S. 207, 211, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986). The third-party doctrine applies when someone voluntarily disclosed information to a third party; an expectation of privacy in such information fails the objectively reasonable prong. *See Smith*, 442 U.S. at 743–44, 99 S.Ct. 2577; *see, e.g.*, *U.S. v. Davis*, 785 F.3d 498, 511–12 (11th Cir. 2015).

The Supreme Court has applied the third-party doctrine to permit electronic tracking of certain information without a warrant. *See U.S. v. Knotts*, 460 U.S. 276, 285, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983) (holding that officers' installation, prior to purchase, of a "beeper" in a barrel purchased by one of the codefendants and the officers' subsequent monitoring of the signals from that beeper as the codefendant transported it by vehicle to its final destination did not constitute a Fourth Amendment search, because a car's movements are public information); *but see U.S. v. Jones*, 565 U.S. 400, 404, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (distinguishing *Knotts* and holding that the use of a GPS tracker to monitor a car's movements over 28 days constituted a search because the monitor installation was a physical trespass—the car was already in the defendant's possession at the time the tracker was installed). Even though the information acquired by the Government in *Jones* was public, like that in *Knotts*, the *place searched* was

constitutionally protected. *See id.* at 409, 132 S.Ct. 945 (in dicta, noting that the Court knew of no case that would support the position that "what would otherwise be an unconstitutional search is not such where it produces only public information").

[5] Similarly, the Government may not employ "sense-enhancing technology" that is not in general public use to obtain information that "could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . ." *Kyllo v. U.S.*, 533 U.S. 27, 34 (2001) (quoting *Silverman v. U.S.*, 365 U.S. 505, 512 (1961)). The technology at issue in *Kyllo* was a thermal imager that produced images showing heat distributions within the defendant's home and in comparison with his neighbors' homes. *Id.* at 29–30, 121 S.Ct. 2038. Based on their thermal imaging scan of Kyllo's residence, officers determined that Kyllo was using halide lights to grow marijuana in his house. *Id.* at 30, 121 S.Ct. 2038. Though the officers obtained additional information about Kyllo's increased electricity usage by subpoenaing his utility company, the Court determined that the officers' use of the thermal imager constituted a search under the Fourth Amendment. *See id.* at 40, 121 S.Ct. 2038; *id.* at 44, 121 S.Ct. 2038 (Stevens, J., dissenting).

Lower courts uniformly agree that, because of the third-party doctrine, computer users lack a reasonable expectation of privacy in their IP addresses, subscriber information, and similar descriptive information they disclose to third parties (such as ISPs) to facilitate Internet service. *See, e.g.*, *U.S. v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016) (internal citations omitted) ("The Fourth Amendment protects the content of the modern-day letter, the email. But courts have not (yet, at least) extended those protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like sender and recipient addresses on an email, or IP addresses."); *U.S. v. Weast*, 811 F.3d 743, 748 (5th Cir. 2016) (holding that the Fourth Amendment does not protect IP addresses or peer-to-peer shared files); *U.S. v. Beckett*, 369 Fed. Appx. 52, 56 (11th Cir. 2010) (non-precedential) (holding that an individual has no reasonable expectation of privacy in identifying information transmitted for ISPs and phone providers to provide service).

In contrast, courts agree that individuals do have a reasonable expectation of privacy in the contents of their computers. *See, e.g.*, *U.S. v. Turner*, 839 F.3d 429, 434 (5th Cir. 2016) (citing *Riley v. California*, —— U.S. ——, 134 S.Ct. 2473, 2485, 189 L.Ed.2d 430 (2014)) (noting the recognized privacy interest in the electronic contents of computers and cell phones); *U.S. v. Buckner*, 473 F.3d 551, 554 (4th Cir. 2007) (citing *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001)) (finding a reasonable expectation of privacy in password-protected files). In a case involving a remote search of a computer, the Ninth Circuit held that a reasonable privacy interest in a personal computer (password-protected and located in the owner's residence) was not extinguished by the owner's connecting to a wireless network, even though others occasionally had access to the computer, because the computer owner was not alerted that his computer usage might be monitored. *U.S. v. Heckenkamp*, 482 F.3d 1142, 1147 (2007).

1. Nature of the Property Searched & Seized

In their briefs, both parties address Mr. Taylor's constitutional privacy interests in the property searched and seized in the context of a Rule 41 violation. Mr. Taylor maintains that the NIT search violated his reasonable expectation of privacy in his home and personal computers, while the

Government argues that Mr. Taylor lacked a reasonable privacy interest in his IP address. Identification of precisely what property was searched and seized is a necessary prerequisite to making the reasonable expectation of privacy inquiry.

Like many of its sister district courts, this court concludes that the NIT searched the contents of Mr. Taylor's computer and seized the information that was listed in Attachment B to the NIT warrant. *Accord, e.g.*, *Adams*, 2016 WL 4212079, at *4 ("The NIT searches the user's computer to discover the IP address associated with that device."); *Arterbury*, No. 15–CR–182–JHP (N.D. Okla. May 17, 2016), at 14 (determining that the property searched and seized was the defendant's computer, not the "packets of data" he sent to the Eastern District of Virginia). Defendant's IP address and other identifying information were not exclusively "located" on his computer because (1) an IP address is, like a phone number to a phone, both internal and external to one's computer, and (2) by accessing the Internet and logging into Playpen Mr. Taylor transmitted some of his information on the "highways" of the Internet.[4] However, the FBI could not obtain Mr. Taylor's information without directing the NIT to "invade" his computer. *See Acevedo–Lemus*, 2016 WL 4208436, at *5–6 (describing the IP address as "a feature of Defendant's connection," not something located on his computer).

2. Whether Mr. Taylor's Expectation of Privacy Was Reasonable

[6] First, the court finds that Mr. Taylor exhibited a subjective expectation of privacy in the information gathered by the NIT because he either did not disclose it to a third party at all[5] or employed the Tor software to conceal it from the public.

The NIT warrant raises not simply the question of whether Mr. Taylor had a reasonable expectation that his IP address and other data would remain private, but whether Mr. Taylor held a reasonable privacy expectation in those pieces of information because of the extra steps he took to preserve the anonymity of his location and identifying information while he browsed the Internet. This Motion presents a different situation than most third-party doctrine questions, because the information seized could not be acquired directly from a third party. *See, e.g.*, *U.S. v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (noting that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party *and conveyed by him to Government authorities*. . . ." (emphasis added)).

Some other district courts ruling on the NIT warrant have found that the use of Tor does not create in the Tor user has a subjective and/or a reasonable expectation that his IP address remains private, because a Tor user must still disclose his real IP address to a third party ISP and to an initial Tor relay computer. *See, e.g.*, *Broy*, 209 F.Supp.3d at 1053 (finding that the defendant lacked a reasonable expectation of privacy in his IP address because "[t]he fact that [the defendant] may have felt his identity was anonymous does not negate the fact that, in order to gain that feeling of anonymity, he voluntarily disclosed his IP address to the operator of the first Tor node."); *Michaud*, 2016 WL 337263, at *7 (finding that the defendant could have no reasonable expectation of privacy in his IP address, which "was public information, like an unlisted telephone number, and eventually could have been discovered").

4. For example, the Host Name, as described in the affidavit, would identify an activating computer in Internet communications.

5. The court questions, for instance, whether and when the activating computer's username would be transmitted over the Internet.

Other courts have rejected that analysis. Those courts found that the fact that the NIT required interaction with a user's private computer to obtain information, or the practical impossibility of peeling back the layers hiding a Tor user's original IP location without technology like the NIT, means that a Tor user has a subjective and objectively reasonable expectation of privacy in his IP address and other information gathered by the NIT. *See, e.g.*, *Adams*, 2016 WL 4212079, at *4 (citing *U.S. v. Lanford*, 838 F.2d 1351, 1353 (5th Cir. 1988)) ("[O]ne's expectation of privacy in [the user's computer] is the proper focus of the analysis . . . . a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage."); *Arterbury*, No. 15–CR–182–JHP (N.D. Okla. May 17, 2016), at 12 n.6, 14–15, 22 n.10, 23 (noting that, absent the NIT's interaction with the defendant's computer, the Government could not have obtained the defendant's IP address, and finding that the defendant's expectation of privacy was reasonable).

This court agrees with the latter contingent of courts and finds that, given his use of Tor, Mr. Taylor's expectation in the privacy of the information seized by the NIT was objectively reasonable. Mr. Taylor could reasonably expect that his computer's contents would remain private. And his computer was located in his home at the time he accessed Playpen, making this case more like *Jones* and not *Knotts*—the NIT was deployed to Mr. Taylor's property (his computer) while it was already in his possession, in a place whose protection lies at the heart of the Fourth Amendment (the home). As the Court observed in *Jones*, no case law exists permitting the government to invade a constitutionally protected place (here, either the computer or the home) to obtain even public information. *See Jones*, 565 U.S. at 409, 132 S.Ct. 945. And though no physical trespass occurred here as it did in *Jones*, the reasoning in *Kyllo* demonstrates that the Government may not rely upon technology that is not in general public use (and the NIT certainly is not) to search locations that would otherwise remain private, even if similar information could be gathered from a third party. *See Kyllo*, 533 U.S. at 34, 121 S.Ct. 2038.

In addressing prejudice under Rule 41, the Government argues that Mr. Taylor cannot, after having employed Tor to shield his location from investigators, "wield it as a sword" to prevent the government from obtaining a warrant to search his computer. (Doc. 26 at 42). Similarly, some courts have stated that an individual can have no reasonable expectation of privacy in property used to conduct illegal activity. *See, e.g.*, *Werdene*, 188 F.Supp.3d at 446; *cf. U.S. v. Stanley*, 753 F.3d 114, 120–21 (3d Cir. 2014) (finding that an individual who used his neighbor's wireless network to distribute child pornography had no objectively reasonable expectation of privacy in his wireless signal, especially because the purpose of the unauthorized connection was itself illegal). One district court ruling on the NIT warrant went a step farther and determined that, because of the ubiquity of hacking, an individual no longer has a reasonable expectation that his computer will not be hacked. *See Matish*, 193 F.Supp.3d at 620 (comparing the NIT's exploitation of a vulnerability in the Tor system to a police officer peering through broken blinds).

But these conclusions are a bridge too far for this court. The nature of Mr. Taylor's privacy interest cannot depend on whether he was engaging in illegal activity, or the Fourth Amendment would lose all meaning. And the use of Tor itself is legal.

Moreover, this court declines to hold that an individual never has a reasonable expectation that the contents of his com-

puter will remain private simply because hackers' skills may outpace the development of cybersecurity. Indeed, federal law reflects a strong stance that hacking violates personal privacy, and that individuals' personal information is entitled to protection by the parties with whom they share it. *See, e.g.*, Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(5) (2012) (criminalizing the knowing transmission of "a program, information, code, or command" to and the intentional access of a protected computer without authorization, so as to cause damage); Telecommunications Act of 1996, 47 U.S.C. § 222, 501 (2012) (requiring telecommunications carriers to protect the confidentiality of customers' information, including location data, and providing for criminal penalties).[6]

In sum, given the nature of the Tor program, the Government could discover the information seized here *only* by entering Mr. Taylor's personal computer through a back door—only by taking over the website itself. The NIT is not akin to a police officer peering through broken blinds into a house; it is more like a police officer acquiring a key to the house and entering through the back door to secretly observe activity in the living room. *Cf. Workman*, 205 F.Supp.3d at 1265 (noting that the government could not conduct a warrantless search of the defendant's home to seize an IP address written on a piece of paper).

This court finds that, although Mr. Taylor may not have had a reasonable expectation in the privacy of his IP address in the abstract, he did have a reasonable expectation of privacy in information that could be gleaned only from his computer. Thus, the Government required a warrant to execute the NIT, and the guarantees of the Fourth Amendment apply to the NIT warrant issued in the Eastern District of Virginia, as well as to the residential warrant issued in the Northern District of Alabama. The fact that the Government obtained a warrant, however, does not end the analysis.

B. Fourth Amendment Warrant Requirements

The focal point of analysis of this issue remains the Fourth Amendment: "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. Mr. Taylor posits that the NIT warrant violated the Fourth Amendment in three different respects: officers' execution of the warrant exceeded its scope; the warrant lacked probable cause; and the warrant was insufficiently particular. Mr. Taylor also asserts that the Northern District of Alabama residential warrant operated as an unconstitutional general warrant.

1. Execution of the NIT Warrant

[7] Defendant argues that the NIT warrant on its face does not authorize the search of computers located outside of the Eastern District of Virginia. The Government responds that "[t]he warrant and accompanying attachments made clear to the magistrate that the NIT was to be deployed initially to the web server hosting Playpen in the Eastern District of Virginia and then obtain information from computers that logged into Playpen, wherever they may be located." (Doc. 26 at 16). The

6. The court acknowledges that the Tor website cautions users that the Tor network cannot ensure total anonymity. *See Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited Feb. 14, 2016). However, that fact alone does not alter the conclusion that Defendant's interest in the privacy of his computer's contents is recognized by society as reasonable.

Government cites language from the warrant and Attachment A and particularly from the NIT warrant's attached affidavit, which explains that the NIT was necessary to obtain the identities and locations of Playpen users and would operate by deploying to computers of any users who logged into the site without reference to where those computers and users were located.

[8–10] Whether the method of execution of the warrant was reasonable provides the touchstone of this issue. Absent "flagrant disregard" of the terms of the warrant, items seized outside the scope of the warrant should not be suppressed. *U.S. v. Wuagneux*, 683 F.2d 1343, 1354 (11th Cir. 1982) (internal citations omitted). "Flagrant disregard" means that "the executing officer's conduct exceeds any reasonable interpretation of the warrant's provisions." *See id.* (internal citation omitted). The court should consider "[s]uch things as the scope of the warrant, the behavior of the searching agents, the conditions under which the search was conducted, and the nature of the evidence being sought" in determining whether the search was reasonable. *U.S. v. Schandl*, 947 F.2d 462, 465 (11th Cir. 1991) (citing *U.S. v. Heldt*, 668 F.2d 1238, 1254 (D.C. Cir. 1981)). A warrant may incorporate by reference documents or affidavits attached to the warrant if the warrant uses proper words of incorporation. *See Groh v. Ramirez*, 540 U.S. 551, 557–558, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004).

Like every other district court to examine this question, this court finds that the FBI's execution of the NIT warrant was objectively reasonable. *See, e.g.*, *Rivera*, 2:15–cr–00266–CJB–KWR (E.D. La. July 20, 2016), at 10; *Michaud*, 2016 WL 337263 at *4. The warrant on its face makes clear that Attachment A to the warrant describes the place to be searched. Attachment A explains that the NIT was to be deployed on a computer server in the Eastern District of Virginia and that the activating computers were "those of any user or administrator who logs into [Playpen]"—regardless of where those computers were physically located. (Doc. 26–1 at 1, 33). The attached affidavit further clarifies the nature of the NIT and specifies that deployment of the NIT is necessary *because* Playpen users' locations are unknown.

Given the text of the warrant, its attachments, and the circumstances surrounding the NIT search, this court cannot conclude that the FBI's reliance on the warrant to deploy the NIT to obtain Mr. Taylor's IP address and other identifying information was executed in flagrant disregard of the warrant's terms.

2. Probable Cause

[11] Mr. Taylor argues that the FBI had probable cause to search and seize the website server itself but not computers that merely logged in to the server, because logging in does not necessarily mean that a user viewed child pornography; but under the warrant a computer was deemed an "activating computer" under the warrant if it merely logged in to the website. The Government responds that Agent Mcfarlane's affidavit, which describes the nature of the Playpen website and the steps a user had to take before logging into it, supported a determination of probable cause that any computer from which a person logged into the Playpen website would provide evidence of child pornography-related crimes.

[12, 13] In determining whether probable cause exists, a magistrate must "simply . . . make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462

U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). A district court's job is not to conduct a de novo review, but to consider whether the issuing magistrate judge had a "substantial basis" for concluding that probable cause existed. *Id.* at 236; 238–39, 103 S.Ct. 2317 (quoting *Jones v. U.S.*, 362 U.S. 257, 271, 80 S.Ct. 725, 4 L.Ed.2d 697 (1960), *overruled on other grounds* by *U.S. v. Salvucci*, 448 U.S. 83, 100 S.Ct. 2547, 65 L.Ed.2d 619 (1980)).

[14] Probable cause governs the warrant. A warrant must be tailored to provide for a search only of those places agents have probable cause to believe contain evidence of a crime:

> [T]he scope of a lawful search is "defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase."

Maryland v. Garrison, 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987) (quoting *U.S. v. Ross*, 456 U.S. 798, 824, 102 S.Ct. 2157, 72 L.Ed.2d 572 (1982)).

Like every other court to address this issue, the court finds that the NIT warrant was supported by sufficient probable cause. *See, e.g.*, *Henderson*, 2016 WL 4549108, at *4 (N.D. Cal. Sept. 1, 2016) (internal citations omitted) ("The courts that have analyzed the NIT warrant have all found that it was supported by probable cause."). First, Playpen existed to enable access to child pornography. Second, the nature of Playpen was such that "[a]ccessing [it] ... require[d] numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon [Playpen] without understanding its purpose and content." (Doc. 26–1 at 13–14).

Any user logging into the Playpen hidden service would have had to take these steps: (1) download Tor software; (2) acquire the website's unique algorithm-generated address (most likely from a Playpen user or from another Tor hidden service page, like the one dedicated to child pornography described in the affidavit); (3) navigate to the Playpen homepage, featuring suggestive images of prepubescent females with directions regarding file uploading and posting; (4) create a Playpen account, which required viewing the instructions to enter a fake email address and take other steps to preserve one's identity; and (5) arrive at the main Playpen directory, which included forum titles that clearly alluded to illicit pornographic content of children. These "numerous affirmative steps" provided a more than substantial basis for the magistrate judge to find sufficient probable cause that any user logging into Playpen did so with the intent to access, view, and/or distribute child pornography; i.e., to engage in criminal conduct. (Doc. 26–1 at 13).

Moreover, several circuit courts have held that membership in a child pornography website alone sufficiently establishes probable cause, reasoning that an individual who took the affirmative steps necessary to become a member probably accessed or contributed to the site's illegal content. *See, e.g.*, *U.S. v. Shields*, 458 F.3d 269, 278 (3d Cir. 2006) (finding sufficient probable cause to search the defendant's home where defendant used a suggestive email address to join two online groups dedicated to exchanging child pornography); *U.S. v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004) ("[I]t is common sense that a person who voluntarily joins a group such as Candyman [a website whose sole purpose was the exchange of child pornog-

raphy], remains a member of the group for approximately a month without cancelling his subscription, and uses screen names that reflect his interest in child pornography, would download such pornography from the website and have it in his possession.").[7] This court finds these decisions persuasive and concludes that Playpen membership independently constituted sufficient probable cause for the magistrate judge to conclude that the computers of Playpen members who logged into the website would contain evidence of at least one child pornography-related crime.

Accordingly, the court concludes that the NIT warrant satisfied the probable cause requirement.

3. Particularity

[15] Mr. Taylor argues that the warrant itself lacks sufficient specificity because it refers to "Attachment A" and "Attachment B" to describe the property to be searched and seized. The Government avers that these two documents were attached to the warrant, not the affidavit, and that the Supreme Court has specifically permitted this kind of incorporation by reference and attachment. (Doc. 26 at 20 (citing *Groh*, 540 U.S. 551 at 557–58, 124 S.Ct. 1284, 157 L.Ed.2d 1068)).

[16, 17] A warrant must particularly describe the place to be searched and the items to be seized. U.S. CONST. amend. IV. Regarding place, the warrant must only "describe the premises in such a way that the searching officer may 'with reasonable effort ascertain and identify the place intended.' " *U.S. v. Burke*, 784 F.2d 1090, 1092 (11th Cir. 1986) (quoting *U.S. v. Weinstein*, 762 F.2d 1522, 1532 (11th Cir. 1985)). Regarding items to be seized, "[a] description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized." *Wuagneux*, 683 F.2d at 1348 (citing *U.S. v. Cook*, 657 F.2d 730, 733 (5th Cir. 1981)). The Eleventh Circuit recognizes that "[e]laborate specificity is unnecessary." *U.S. v. Strauss*, 678 F.2d 886, 892 (11th Cir. 1982).

The court in *Anzalone* observed that "[e]very court to consider this question has found the NIT search warrant sufficiently particular." 208 F.Supp.3d at 368 (internal citations omitted). As discussed previously, the attachments were correctly incorporated into the NIT warrant by reference. Attachments A and B clearly identified the "place" to be searched (the NIT would be deployed to the computer server in the Eastern District of Virginia and then to computers logging into the Playpen website) and the information to be seized (Attachment B includes an itemized list of the seven pieces of information to be seized). Though the Constitution does not require elaborate specificity, the court finds it difficult to imagine how much more specific the descriptions of the place to be searched and the items to be seized could have been. The NIT warrant was sufficiently particular.

4. Northern District of Alabama Warrant

[18] Additionally, Mr. Taylor maintains that the FBI's seizure of his personal property, pursuant to the Northern District of Alabama residential warrant, for offsite forensic testing when an initial search did not yield any pornographic images constituted unconstitutional exploratory "rummaging." *See Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S.Ct.

7. The Eleventh Circuit has not directly addressed this membership question but cited the *Shields* and *Froman* reasoning in two opinions addressing different ultimate issues. *Davidson v. U.S.*, 213 Fed.Appx. 769, 771–72 (11th Cir. 2007) (citing *Shields* and *Froman*); *U.S. v. Williams*, 444 F.3d 1286, 1304 n.87 (11th Cir. 2006), *rev'd on other grounds*, *U.S. v. Williams*, 553 U.S. 285, 128 S.Ct. 1830, 170 L.Ed.2d 650 (2008) (citing *Froman*).

2022, 29 L.Ed.2d 564 (1971). The Government correctly points out that the affidavit attached to the Northern District of Alabama residential search warrant included a non-exclusive list of techniques that might be used to search seized electronic information. *See* (Doc. 26–2 at 41–43). Further, as to electronic storage media or electronically stored information, the Federal Rules of Criminal Procedure specifically authorize "a later review of the media or information consistent with the warrant." FED. R. CRIM. P. 41(e)(2)(B). The court concludes that the Northern District of Alabama warrant and the officers' execution of it fell within constitutional bounds.

C. Section 636(a) of the Federal Magistrates Act & Rule 41(b)

[19] Mr. Taylor argues that the NIT warrant was issued without authorization from § 636(a) of the Federal Magistrates Act, 28 U.S.C. § 631 et seq. (2012), and Federal Rule of Criminal Procedure 41. He contends that the warrant was thus void *ab initio* and that he was prejudiced by the seizure of evidence pursuant to it, warranting suppression. The Government responds that Rule 41 and § 636(a) authorized the magistrate to issue the NIT warrant; that, alternatively, any violation was merely technical, not constitutional, in nature and did not prejudice Mr. Taylor and the officers did not act in bad faith; and that, alternatively, the good faith exception to the exclusionary rule should prevent suppression in any case.

1. Whether the NIT Warrant Was Issued in Violation of § 636(a)

Section 636(a) of the Federal Magistrates Act provides that "[e]ach 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 ... all powers and duties conferred or imposed upon United States commissioners by law or **by the Rules of Criminal Procedure**...." 28 U.S.C. § 636(a)(1) (2012) (emphasis added).[8] Many other district courts ruling on the NIT warrant have analyzed the alleged § 636(a) and Rule 41(b) violations together, reasoning that the statute incorporates Rule 41(b) by virtue of granting to magistrate judges the power given to them by the Federal Rules; thus, the purported Rule 41(b) violation becomes the ultimate question. *See, e.g.*, *Levin*, 186 F.Supp.3d at 31–32 (stating that "Section 636(a) expressly incorporates any authorities granted to magistrate judges by the Federal Rules of Criminal Procedure" and concluding that "Section 636(a)(1) is inapposite because Rule 41(b) did not confer on the magistrate judge authority to issue the NIT warrant"); *Tran*, 226 F.Supp.3d at 65, 2016 WL 7468005, at *5 (citing *Levin* for the proposition that "[w]hether the Federal Magistrates Act was violated can be answered by asking if the warrant complies with Rule 41").

This court declines to read the independent jurisdictional limitations out of the statute. The Act limits the exercise of magistrate judges' power and duties to "within the district" of the appointing court. "[T]he grammatical structure of the sentence indicates that magistrate judges shall have those powers specified by rule or other law (e.g., Rule 41), but those powers are effective only in certain specified geographic areas—and, as we've seen, none of those areas is implicated here." *U.S. v. Krueger*, 809 F.3d 1109, 1119 (10th

8. The statute also provides that magistrate judges shall have power "at other places where that court may function, and elsewhere as authorized by law," but neither such area is at issue here. *See* § 636(a).

Cir. 2015) (Gorsuch, J., concurring) (affirming the district court's grant of a motion to suppress evidence seized pursuant to a warrant to search property in Oklahoma that had been issued by a magistrate judge in Kansas). If the mandates of the statute and the rule are not examined separately, "[t]he statute might as well be written this way: Magistrate judges shall have all powers and duties conferred or imposed by law or by the rules." *See id.*

The Government argues that § 636(a) does not limit the locations in which a magistrate judge's exercise of power may have *effect*, which is correct; however, it presumes that the search and seizure here took place in the Eastern District of Virginia and had effects in the Northern District of Alabama. But the court has already determined that the search itself took place in Alabama. The Government's argument illustrates why most courts have analyzed the statute and Rule together—as goes the magistrate's authority under § 636(a), so goes her authority under Rule 41, because the Rule cannot give the magistrate more power than does the statute. *See* Rules Enabling Act, 28 U.S.C. § 2072 (2012) (providing that rules of procedure may not "abridge, enlarge or modify any substantive right"); *cf. Krueger*, 809 F.3d at 1125 (Gorsuch, J., concurring) (explaining that our government is one of divided power and that because magistrate judges do not enjoy Article III protections, Congress has curbed their geographic authority). Thus, whether the authority of the magistrate judge to issue the NIT warrant fell within the statute or the Rule, or neither, turns on where the search took place.

The court finds that the "within the district" language of § 636(a) is not surplusage; the magistrate judge had no jurisdiction to issue a warrant for a search in another district than where she sat. Because the NIT warrant authorized a search in a district different from that in which the magistrate judge may exercise her Rule 41 power to issue a search warrant, it was "no warrant at all," or void *ab initio* for want of jurisdiction. *See Krueger*, 809 F.3d at 1118, 1123 (Gorsuch, J., concurring).

2. Whether the NIT Warrant Was Issued in Violation of Rule 41(b)

[20] In the alternative, the court concludes that the warrant was issued without authority under Federal Rule of Criminal Procedure 41(b). Titled "Authority to Issue a Warrant," [9] that rule provides in relevant part that a magistrate judge has authority to issue a warrant (1) "to search for and seize a person or property located within the district"; (2) "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"; and (4) "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." [10]

Sections 41(b)(1) and (b)(2) did not imbue the magistrate with issuing authority. Both these subsections require that the property to be searched/seized be located in the same district as the issuing magistrate at the time the warrant is issued; but the location of the property searched—Mr. Taylor's computer—and seized—his IP address and other identifying information—were unknown by the FBI at the time it applied for the warrant. Mr. Taylor's computer was at all relevant times

9. The December 1, 2016 amendments to the Rule changed this title to "Venue for a Warrant Application." *See* FED. R. CRIM. P. 41(b).

10. Subsections (3) and (5) of Rule 41(b) are inapplicable here.

located in the Northern District of Alabama, and many of the other activating computers were located outside of the Eastern District of Virginia. True, as the Government notes, the FBI installed the NIT on the server in the Eastern District of Virginia. But as the court has already determined, the Defendant's computer was the object of the search and that search occurred in Alabama.

Similarly, Rule 41(b)(4) did not empower the magistrate judge to issue the NIT warrant. First, the NIT is not a "tracking device," which is defined in Rule 41(a)(2)(E) by reference to 18 U.S.C. § 3117(b) as "an electronic or mechanical device which permits the tracking of the movement of a person or object." FED. R. CRIM. P. 41(a)(2)(E); 18 U.S.C. § 3117(b) (2012). The NIT did not track **movement** like the beeper in *Knotts*; rather, it conducted a search for several pieces of identifying information from activating computers, each in one static location. *See Adams*, 2016 WL 4212079, at *6 ("[T]he NIT does not track; it searches."); *Rivera*, 2:15–cr–00266–CJB–KWR (E.D. La. July 20, 2016), at 15 (noting that "the NIT could do much more than simply track a computer's location").

Second, even if the NIT were a tracking device, it was not "installed" in the Eastern District of Virginia, but at the location of the activating computer, in this case, in the Northern District of Alabama. The Government characterizes the NIT as a tracking device because it was attached to Playpen content in the Eastern District of Virginia, traveled to Defendant's computer in the Northern District of Alabama, and permitted the Government to identify Mr. Taylor's computer and his location.

Though this question is a close call, the court concludes that the Government's position ultimately misconstrues the nature of the property tracked; the contents of Mr. Taylor's computer, not the Playpen content he downloaded, would be the property "tracked" by the NIT, and neither his computer nor its contents ever entered into the Eastern District of Virginia for installation of the tracking device. *See Michaud*, 2016 WL 337263, at *6 (observing that the tracking device analogy "breaks down" if the installation is deemed to have occurred on the server in the Eastern District of Virginia, because the defendant "never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district," and similarly fails if the installation occurred on the defendant's computer outside of the issuing district); *but see, e.g.*, *Matish*, 193 F.Supp.3d at 612 (describing the process of logging into Playpen as taking a "virtual trip" to Virginia and so permitting the installation of the NIT in the Eastern District of Virginia).

The Government additionally argues that the NIT warrant was issued by a magistrate judge in the district with the strongest known connection to the search. While this point may be true, it does not follow that Rule 41 authorized the magistrate judge to issue the warrant. The court is bound to interpret Rule 41 as it is written, not to approve any warrants for which the issuing venue merely appears reasonable. Further, the Government contends that Rule 41 has been interpreted flexibly and has been read as permitting searches not expressly prohibited by the rule or by statute. *See U.S. v. New York Tel. Co.*, 434 U.S. 159, 169, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977); *U.S. v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (en banc).

However, the *New York Telephone* and *Koyomejian* cases both involved a *kind* of search not addressed one way or the other by the text of Rule 41 (the use of a pen register to collect telephone numbers when the definition of "property" did not yet include information and video surveillance,

respectively), not the *location* of a search, which is addressed by the wording of Rule 41. This court in any case declines to legislate by reading into the statute language that Congress did not place there.[11]

a. Nature of the Rule 41 Violation

[21] A Rule 41 violation is either "technical" or "procedural," as courts have phrased it, or constitutional. *See, e.g.*, *Adams*, 2016 WL 4212079, at *6 ("The Court views a Rule 41(b) violation to be a technical or procedural violation. . . ."). "[U]nless a clear constitutional violation occurs, noncompliance with Rule 41 requires suppression of evidence only where (1) there was 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) there is evidence of intentional and deliberate disregard of a provision in the Rule." *U.S. v. Gerber*, 994 F.2d 1556, 1560 (11th Cir. 1993) (quoting *U.S. v. Loyd*, 721 F.2d 331, 333 (11th Cir. 1983) (per curiam)).

First, the Rule 41 violation here was constitutional. True, as the Government points out, the Fourth Amendment does not impose a venue requirement; rather, it requires only that a warrant be (1) signed by a neutral, detached magistrate; (2) supported by probable cause; and (3) sufficiently particular. *See Dalia v. U.S.*, 441 U.S. 238, 255, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979). But inherent in the notion of a "neutral, detached magistrate" is that the magistrate have **authority** to issue the warrant. *See Shadwick v. City of Tampa*, 407 U.S. 345, 352, 92 S.Ct. 2119, 32 L.Ed.2d 783 (1972) (holding, in answer to "[t]he single question [of] whether power has been lawfully **vested**," that municipal court clerks may issue warrants) (emphasis added); *U.S. v. Glover*, 736 F.3d 509, 515 (D.D.C. 2013) (holding that a Rule 41(b) violation constituted a "jurisdictional flaw" inexcusable as a "technical defect"); *U.S. v. Master*, 614 F.3d 236, 241 (6th Cir. 2010) (holding that a warrant issued by a judge lacking authority violated defendant's Fourth Amendment rights).

Second, even if not a constitutional violation, Mr. Taylor was prejudiced by the Rule 41 violation. Although the Eleventh Circuit has not interpreted "the search might not have occurred" to the same extent as other circuits, this court concurs with the majority's reasoning in *Krueger* that the correct standard inquires "whether the issuing federal magistrate judge could have complied with the rule." *See Krueger*, 809 F.3d at 1116; *Adams*, 2016 WL 4212079, at *8 (M.D. Fla.) (holding that the defendant was prejudiced by the Rule 41 violation because "[h]ad the magistrate judge followed Rule 41(b), the search of Defendant's computer would not have occurred").

The use of Tor made recovering Defendant's IP address and other identifying information without the NIT impossible; Mr. Taylor had a reasonable expectation of privacy in the contents of his computer, meaning that the seven pieces of information seized by the NIT warrant could not have been obtained in the absence of the NIT warrant. The issuing magistrate judge could not comply with Rule 41 because it did not empower her to authorize searches outside of her district. Mr. Tay-

11. Further bolstering this conclusion is the addition to Rule 41 that became law on December 1, 2016, permitting a magistrate judge 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. . . ." FED. R. CRIM. P. 41(b)(6). The addition of this text suggests that the prior version of the Rule did not permit a magistrate judge to issue a warrant in such a situation.

lor, therefore, was prejudiced by the Rule 41(b) violation.

However, no evidence supports a finding of intentional and deliberate disregard of the Rule. The very existence of divergent interpretations of Rule 41(b) by district court judges across the country demonstrates that reasonable minds may interpret the Rule, and where the searches under the NIT took place, differently.

3. Suppression

a. Suppression of Evidence Seized Pursuant to a Warrant Void *Ab Initio*

[22–24] Under the statute and Rule 41, both of which limit a magistrate judge's authority to issue a warrant, the NIT warrant was void *ab initio*, meaning that the FBI's search of Mr. Taylor's computer and the seizure of evidence pursuant to it were conducted without a valid warrant and thus were unreasonable in violation of the Fourth Amendment. But "[t]he fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies" to "forbid[ ] the use of improperly obtained evidence at trial." *Herring v. U.S.*, 555 U.S. 135, 139–140, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009). Rather, "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144, 129 S.Ct. 695. This balancing test is an objective one that does not assess officers' subjective intent. *Id.* at 145, 129 S.Ct. 695.

The "good faith" line of cases, beginning with *U.S. v. Leon* in 1984, implements the balancing of these factors by carving out an exception to the exclusionary rule where the search was the result of objectively reasonable behavior by officers. *See Davis v. U.S.*, 564 U.S. 229, 238–39, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011). The Supreme Court in *Leon* itself held that when officers are objectively reasonable in relying on a search warrant that is later invalidated, any evidence seized pursuant to that search warrant should not be suppressed. *U.S. v. Leon*, 468 U.S. 897, 922, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).

Whether the good faith exception is available for a warrant that is void *ab initio* is an open question in the Eleventh Circuit. Many of the district courts ruling on the NIT warrant have addressed the issue, as have a handful of other state and federal courts. *See, e.g.*, *Master*, 614 F.3d at 242–43 (overruling its previous holding that the good faith exception does not apply to a warrant issued without jurisdiction and remanding for consideration of the deterrent value and costs of suppression); *Werdene*, 188 F.Supp.3d at 449–453 (following *Master* and ultimately finding suppression not warranted); *Levin*, 186 F.Supp.3d at 41 (finding that the good faith exception did not apply to the void *ab initio* NIT warrant).

The court concurs with the reasoning of the court in *Werdene* that, given the balancing test articulated in *Leon* and its progeny, including *Herring*, "the legal status of the warrant under the Fourth Amendment does not inform the decision of whether the good faith exception is available in a given case; that inquiry is separate and must be considered in light of the exclusionary rule's purpose and the officers' conduct at issue." 188 F.Supp.3d at 451 (citing *Master*, 614 F.3d at 243). Thus, the court proceeds to the good faith inquiry.

b. Application of the Good Faith Exception

Assuming either a constitutional violation or prejudice under Rule 41(b), the court finds that the good faith exception to the exclusionary rule applies here; the officers were objectively reasonable in relying on the NIT warrant.

As the court in *Werdene* found:

> [T]o the extent a mistake was made in this case, it was not made by the agents.... Rather, it was made by the magistrate when she mistakenly issued a warrant outside her jurisdiction. The agents consulted with federal attorneys before preparing the warrant application. They presented the magistrate judge with all relevant information to allow her to make a decision as to whether Rule 41(b) permitted her to issue the warrant. The FBI agents did not misrepresent how the search would be conducted or, most importantly, where it would be conducted.

188 F.Supp.3d at 452–453 (internal citations omitted).[12]

[25] As to warrants, the good faith exception does not apply where (1) the issuing judge is "misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) the judge "wholly abandoned his judicial role"; (3) the affidavit on which the warrant was based was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) the warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923, 104 S.Ct. 3405 (internal citations omitted).

Defendant does not allege that any of these circumstances indicating bad faith are present here, and indeed none are supported by the record. None of the information in Special Agent Mcfarlane's affidavit was false. The magistrate judge in the Eastern District of Virginia did not wholly abandon her judicial role; the divergent results of the various motions to suppress resulting from the NIT warrant are themselves evidence that the magistrate judge did not make a determination completely outside the realm of reason. This court has already found that the NIT warrant was supported by probable cause. And the court has also determined that the warrant additionally complied with the particularity requirements of the Fourth Amendment, making it facially valid.

[26] "A magistrate judge's mistaken belief that she had jurisdiction, absent any indicia of reckless conduct by the agents, does not warrant suppression." *Werdene*, 188 F.Supp.3d at 453; *see Leon*, 468 U.S. at 916, 104 S.Ct. 3405 ("[T]he exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates."). Exclusion of the evidence seized pursuant to the NIT warrant would serve little deterrent purpose where the mistaken conduct of the magistrate judge, not the officers, invalidated the warrant. Accordingly, the court finds that suppression is an inappropriate remedy for the Fourth Amendment and/or Rule 41 violation(s) that occurred here.

III. Conclusion

The court **FINDS** that Mr. Taylor had a reasonable expectation of privacy in the contents of his computer, such that the FBI's actions in deploying the NIT constituted a search under the Fourth Amendment, mandating a warrant. The court **FINDS** that the executing officers did not exceed the scope of the warrant and that the NIT warrant was supported by probable cause and was sufficiently particular; additionally, the court **FINDS** that the

12. The court acknowledges that, contrary to this court, the court in *Werdene* concluded that no constitutional violation occurred in the issuance of the NIT warrant, but as an alternative ruling found good faith. *See Werdene*, 188 F.Supp.3d at 446, 448, 451. This court finds the *Werdene* court's reasoning on the issue of good faith persuasive.

Northern District of Alabama warrant was constitutionally issued and executed. However, the court **FINDS** that the NIT warrant was not authorized under 28 U.S.C. § 636(a) of the Federal Magistrates Act or, in the alternative, Federal Rule of Criminal Procedure 41(b).

The court **FINDS** that the statutory and Rule violations resulted in the NIT warrant being void *ab initio*, making the search of Mr. Taylor's computer unreasonable under the Fourth Amendment; further, the Rule 41(b) violation prejudiced Mr. Taylor. But the court **FINDS** that the good faith exception to the exclusionary rule applies to prevent suppression of the evidence seized pursuant to the NIT warrant, including the evidence seized pursuant to the secondary residential warrant issued in the Northern District of Alabama.

Accordingly, the court **WILL DENY** Defendant's Motion to Suppress. The court will enter a separate order consistent with this Opinion.

DONE and **ORDERED** this 24th day of April, 2017.

GREATER BIRMINGHAM MINISTRIES, et al., Plaintiffs,

v.

John MERRILL, in his official capacity as the Alabama Secretary of State, Defendant.

2:15–cv–02193–LSC

United States District Court, N.D. Alabama, Southern Division.

Signed 04/06/2017

Background: Registered voters and organizations concerned with voting rights of minorities brought § 1983 action against the state, governor, and state's attorney general, alleging that state law requiring voters to show a photo identification to an election official prior to voting violated state's Voter Rights Act as well as the Fourteenth and Fifteenth Amendments. Defendants moved to dismiss.

Holdings: The District Court, L. Scott Coogler, J., held that:

(1) individual voters had standing to sue;

(2) organizations had standing in their own right to sue;

(3) allegations were sufficient to state claim that photo identification law violated state's Voting Rights Act;

(4) allegations were sufficient to state claim that "positively identify" exception form photo identification law violated Voting Rights Act; and

(5) allegations were sufficient to state claim that photo identification law violated the Fourteenth and Fifteenth Amendments.

Motion denied.

1. Federal Civil Procedure ⚿103.2, 103.3

To establish standing under Article III of the Constitution, a plaintiff must allege: (1) that it has suffered an actual or imminent injury in fact, (2) that there is a causal connection between that injury and the conduct complained of, and (3) that the injury is likely to be redressed by a favorable decision. U.S. Const. art. 3, § 2, cl. 1.

2. Federal Civil Procedure ⚿103.5

At the pleading stage, general factual allegations of injury resulting from defendant's conduct may suffice to establish standing.

3. Injunction ⚿1505

Registered voters alleged injury-in-fact sufficient for standing to seek injunc-

2016 WL 4212079
Only the Westlaw citation is currently available.
United States District Court,
M.D. Florida,
Orlando Division.

United States of America
v.
Ryan Anthony Adams.

CASE NO: 6:16-cr-11-Orl-40GJK
|
Signed 08/10/2016

ORDER

PAUL G. BYRON, United States District Judge

***1** This cause comes before the Court on Defendant Ryan Adams' Motion to Suppress Evidence (Doc. 36), filed June 1, 2016, the Government's Response in Opposition (Doc. 46), filed July 1, 2016, and Defendant's Supplemental Briefing to His Motion to Suppress (Doc. 44), filed June 24, 2016. After reviewing the parties' submissions and following an evidentiary hearing held on July 11, 2016 (Doc. 49), the Defendant's Motion to Suppress is denied.

I. BACKGROUND

Defendant is charged with receipt and possession of child pornography, in violation of Title 18, United States Code, Section 2252A(a)(2)(A) and (a)(5)(B). (Doc. 1). The charges arise from the Government's investigation into a website known as "Playpen," which is a global online forum dedicated to the advertisement and distribution of child pornography. (Doc. 36-1, Ex. 3). Defendant and other users visit Playpen via the anonymous Tor network. (*Id.* ¶ 7). The Tor network is constructed to mask the user's IP address (which may be used to identify the user's physical address) by relaying the user's communication among multiple servers located worldwide. (*Id.* ¶ 8). Hence, a server receiving a query from a Tor network displays the IP address of the last node in the Tor network and thereby conceals the user's IP address. (*Id.* ¶¶ 8, 23, 24). The Tor network prevents law enforcement from tracing the communication back through the network to the actual user Defendant in the instant case. (*Id.* ¶ 24). For the same reason, law enforcement cannot subpoena Internet Service Providers ("ISP") to locate the user's physical address. (*Id.*).

On or about February 20, 2015, the computer server hosting Playpen was seized from a web-hosting facility in North Carolina. (Doc. 36-1, Ex. 1, ¶ 12). The website was moved to Virginia and the FBI subsequently operated the server to monitor electronic communications of users of the website. (*Id.*). The United States District Court for the Eastern District of Virginia authorized a search warrant allowing law enforcement officers to deploy a Network Investigative Technique ("NIT") on the Playpen server. (*Id.* ¶ 25). When a user accessed Playpen via the Tor network, the NIT was transmitted back to the user's computer, identified the IP address, and transmitted this information, along with the type of operating system running on the computer, the computer's MAC address, the computer's Host Name, and other data back to a server controlled by law enforcement. (*Id.*; Doc. 36-1, Ex. 3, ¶ 34). Using information generated via the NIT, on March 1, 2015, law enforcement identified Defendant as an individual using the name "Gouki" who had been accessing the Playpen database to retrieve images constituting child pornography. (Doc. 36-1, Ex. 1, ¶¶ 29 31).

1 The affidavit at Doc. 36 1, Ex. 1, ¶¶ 29 30 incorrectly reports the date as February 19, 2015. This mistake was clarified during the evidentiary hearing held on July 11, 2016.

On September 11, 2015, law enforcement officers went to Defendant's residence in Florida. (*Id.* ¶ 32). The officers identified themselves to Defendant as FBI Agents, advised Defendant of the nature of the investigation, and requested permission to speak with Defendant. (*Id.*). The agents informed Defendant that he was not required to speak with them. (*Id.*). Defendant consented to be interviewed by the FBI Agents, and he admitted to using the screen name "Gouki" to access, download, and view child pornography. (*Id.*). Specifically, Defendant confessed to using his laptop to access websites containing child pornography, including Playpen. (*Id.*). Defendant admitted to downloading at least twenty movie files containing child pornography and having at one time over 100 files of child pornography. (*Id.*). Defendant provided a detailed description of the types of images he downloaded from various websites, the number of years he has been engaged in this illegal conduct, and that he has used

Yahoo! Messenger to chat and share child pornography with others. (*Id.*).

***2** At the conclusion of the non-custodial interview, Defendant voluntarily gave the agents his laptop computer, three CDs, a USB external memory 1.8 Hard Drive, and a 10 Mega External Hard Drive which he stated contained child pornography. (*Id.* ¶ 33). After the agents departed Defendant's residence, Defendant approached the agents who were seated in their vehicle and stated that he would call them if he found other devices containing child pornography. (*Id.*). Later that same day, at approximately 4:30 p.m., Defendant called the agents and informed them that he had another flash drive that he wanted to give to the agents. (*Id.*). The following day, at 10:00 a.m., agents met Defendant in a public location at which time Defendant voluntarily provided agents a PNY 16GB Black Blue USB drive, a Micro SD HC 4G, and a Lexar SD Card 128MB which Defendant said were used to store child pornography. (*Id.* ¶ 34). On September 25, 2015, fourteen days after Defendant confessed to the agents and thirteen days after Defendant gave agents additional data storage devices, FBI Special Agent Raymundo applied for, and was issued, a warrant to search the HP Laptop and all of the electronic data storage devices obtained from Defendant. (*Id.* at p. 29).

II. SUMMARY OF THE PARTIES' ARGUMENTS

Defendant contends that the magistrate judge for the Eastern District of Virginia who authorized the Government's search of his computer through the deployment of a NIT acted in violation of Federal Rule of Criminal Procedure 41(b) and 28 U.S.C. § 636(a). (Doc. 36, p. 5). Defendant submits that the violation of Rule 41(b) cannot be characterized as a "mere technical violation" of the rule, such as a violation of a procedural requirement arising under Rule 41(b); therefore, Defendant argues that the Government may not rely upon the good-faith exception to avoid suppression of evidence. (*Id.* at p. 13). That is, it is Defendant's position that the NIT search warrant issued by the magistrate judge in Alexandria, Virginia, violated clearly established jurisdictional limits established in Rule 41(b) by allowing agents to search Defendant's computer in Florida to locate the IP address associated with that device. (*Id.* at p. 6). Defendant concludes that the NIT warrant was "no warrant at all" and the search of Defendant's computer violated the Fourth Amendment to the United States Constitution. (*Id.*).

In response, the Government submits that the affidavit in support of the Government's application for the NIT warrant (Doc. 36-1, Ex. 3) establishes probable cause to search Defendant's computer. (Doc. 46, p. 7). This point is not contested by Defendant in the instant Motion to Suppress. The Government also correctly reports that Defendant does not challenge the NIT warrant on the basis that it lacks particularity or that the magistrate judge was not neutral and detached. (*Id.* at p. 14). After dispensing with these preliminary matters, the Government argues that Rule 41(b) is "a flexible rule that is broad enough to authorize the issuance of the warrant in this case." (*Id.* at p. 15). Assuming Rule 41(b) was violated, the Government submits suppression of the evidence is not warranted, because:

> (1) the defendant suffered no prejudice and the agents did not act with deliberate disregard of Rule 41(b); (2) the agents acted in good faith reliance on the warrant; and (3) the defendant's admissions that his electronic devices contained child pornography and the voluntary relinquishment of those devices to the agents attenuated the connection between the NIT warrant and the child pornography seized from the devices.

(*Id.*).

III. SUMMARY OF THE COURT'S ANALYSIS

To the extent Rule 41(b) was violated when the magistrate judge in the Eastern District of Virginia issued the NIT warrant on February 20, 2015 (Doc. 36-1, Ex. 3, Attachment A), any illegality arising from the violation of the rule is sufficiently attenuated from Defendant's voluntary confession, Defendant's act of voluntarily surrendering various electronic devices to the agents, and the act of applying for and receiving a search warrant prior to inspecting the subject electronic devices.

The NIT warrant was obtained on February 20, 2015, and Defendant's computer was searched via the NIT on March 1, 2015. Agents did not approach Defendant until

six months later on September 11, 2015, at which time they identified themselves and said they were investigating Defendant for possessing child pornography. Defendant was advised that he was not required to speak with law enforcement. Armed with this knowledge, Defendant consented to a non-custodial interview and subsequently provided a detailed confession to possessing child pornography. Defendant voluntarily gave his laptop and electronic data storage devices to the agents and called the agents later that same day to advise he was in possession of additional storage devices containing child pornography. The agents collected those devices from Defendant the following day after meeting Defendant at a mutually agreed upon public location. The agents then applied for and received a warrant to search the laptop and storage devices, giving rise to the instant criminal charges. The Court finds that any illegality arising from a violation of Rule 41(b) six months earlier was sufficiently attenuated by intervening circumstances, rendering suppression inappropriate.

***3** While the Court does not need to address the nature of the Rule 41(b) violation or whether the good faith exception applies in reaching a resolution of Defendant's motion, the Court will do so to ensure the record is clear for appellate review.

IV. DISCUSSION OF ALLEGED FOURTH AMENDMENT VIOLATION

Under the Fourth Amendment to the United States Constitution, every person has the right "to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. The Supreme Court has generally interpreted this to mean that a search must be based on probable cause and must be executed pursuant to a warrant. *Katz v. United States*, 389 U.S. 347, 357 (1967). The Fourth Amendment provides that "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459 (2011). Evidence obtained in violation of the Fourth Amendment may be suppressed pursuant to the exclusionary rule only when suppression is warranted to deter violations of the Fourth Amendment. *See Davis v. United States*, 564 U.S. 229, 238 (2011).

"[T]he application of the Fourth Amendment depends on whether the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (internal quotation marks omitted). A person claiming a violation of the Fourth Amendment must demonstrate that he has a subjective expectation of privacy and that society is prepared to recognize that expectation as objectively reasonable. *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).

Computer users lack a legitimate expectation of privacy in information regarding the to and from addresses for emails, the IP addresses of websites visited, the total traffic volume of the user, and other addressing and routing information conveyed for the purpose of transmitting Internet communications to or from a user. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008), *rev'd on other grounds sub. nom*, *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), *cert. denied*, 555 U.S. 908 (2008); *see also United States v. Christie*, 624 F.3d 558, 573 74 (3d Cir. 2010) (finding no reasonable expectation of privacy in IP address or subscriber information because such information is voluntarily conveyed to third parties), *cert. denied*, 526 U.S. 1236 (2011). At least one court has further held that using Tor does not involve a reasonable expectation of privacy in the IP address. *United States v. Werdene*, No. 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016). The *Werdene* Court found that "a necessary aspect of the Tor network is the initial transmission of a user's IP address to a third party." *Id.* "[I]n order for a prospective user to use the Tor network[,] they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations." *Id.* (quoting *United States v. Farrell*, No. 15-cr-029, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016)).

***4** Applying these principles, the Court finds Defendant does not have a reasonable expectation of privacy in the IP address associated with the computer he used to access Playpen. Defendant called Mr. Richard Connor, a computer forensic expert witness, at the evidentiary hearing on his motion to suppress. Mr. Connor explained that an individual using the Tor network exposes his IP address to the "entry node" in the Tor system that is, the first server to receive the search query from Defendant. After the IP address is exposed to the entry node, the address is unknown to the relay nodes the

servers responsible for bouncing the search query among other various servers until it reaches Playpen. Mr. Connor further explained that each relay node has its own IP address and with each relay additional IP addresses are used, thereby masking Defendant's IP address. While law enforcement can see the IP address of the last Tor server to transmit the search query to Playpen, that server (the exit node) has no way to identify Defendant's IP address. However, this does not alter the fact that Defendant must first disclose his IP address upon entering the Tor system. Defendant's expectation of privacy in his IP address is lost once he discloses the IP address to the first server in the Tor system. It is for this precise reason that the Government is not required to obtain a search warrant to subpoena an Internet Service Provider the physical address connected with a visible IP address. *See Forrester*, 512 F.3d at 510.

However, Defendant pointedly argued during the evidentiary hearing that Defendant's IP address was obtained via the NIT by searching Defendant's computer, which is a correct assertion. The Government, in connection with its application for a warrant to the NIT, attests that the NIT operates by attaching once a user logs onto the Playpen website with a username and password. (Doc. 36-1, Ex. 3, ¶ 32). Once a user's computer downloads the content from Playpen or more accurately once the exit node in the Tor network downloads the content the NIT causes the user's computer to transmit information to a computer controlled by the Government. (*Id.* ¶ 33). Stated differently, the NIT travels to the user's computer and identifies the IP address along with the type of operating system running on the computer, information about whether the NIT was previously delivered to avoid duplication of data, the Host Name assigned to the device connected to the network, and the MAC address for the computer. [2] (*Id.* ¶ 34).

2 The MAC is a unique number assigned to the computer by the manufacturer. (Doc. 36 1, Ex. 3, ¶ 34).

When the Court considers the issue of Defendant's reasonable expectation of privacy, the question becomes whether the IP address should be the focus of this analysis or whether Defendant's expectation of privacy in his computer is the proper subject of this analysis. There is little doubt that had law enforcement officers obtained Defendant's IP address from a non-Tor-based server and issued a subpoena to the ISP to determine Defendant's physical address, a motion to suppress the information obtained from the ISP would be without merit. [3] However, Defendant's IP address was discovered only after property residing within Defendant's home his computer was searched by the NIT. The courts which have thus far grappled with the extent to which a person has a reasonable expectation of privacy in an IP address have analyzed the issue in the context of a subpoena to an ISP to identify the person assigned the IP address. To the extent the *Werdene* Court has concluded that an individual waives his or her expectation of privacy in his or her computer by connecting to the Tor network, this Court disagrees with that conclusion as having improperly conflated the expectation of privacy associated with an IP address with the expectation of privacy one has in the computer searched by the NIT.

3 Non Tor based websites have IP address logs that law enforcement can use in conjunction with publicly available databases to determine the ISP that owns the targeted IP address. (*Id.* ¶ 29). A subpoena is issued to the ISP and the identity of the user assigned to the IP address at a particular time is determined. (*Id.*).

The NIT searches the user's computer to discover the IP address associated with that device. Therefore, one's expectation of privacy in that device is the proper focus of the analysis, not one's expectation of privacy in the IP address residing in that device. For example, a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage. *See United States v. Lanford*, 838 F.2d 1351, 1353 (5th Cir. 1988). Remove the stolen car from the garage, and no expectation of privacy in the vehicle exists. An IP address located in the "open" is akin to a stolen car parked on the street. However, the agents were required to deploy the NIT to search the contents of Defendant's laptop, and Defendant enjoyed a reasonable expectation of privacy in that device. The Court therefore turns to whether the NIT warrant was properly issued and whether the agents may rely in good faith upon that warrant.

V. DISCUSSION OF RULE 41(b)

***5** The Federal Magistrates Act, 28 U.S.C. § 636(a), provides that "[e]ach 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...(1) all powers and duties conferred or imposed...by law or by the Rules of Criminal Procedure." Federal Rule of Criminal Procedure 41(b) confers upon the magistrate judge the authority to issue search warrants in five distinct circumstances:

> (1) a magistrate judge with authority in the district or if none is reasonable 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 purpose; 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.

The Government asserts that the NIT warrant comported with Rule 41(b) presumably subsection (b)(1) because the Playpen server was located in the Eastern District of Virginia, the NIT was placed on the server in that district, and only users who logged onto the server in that district downloaded the NIT. (Doc. 46, p. 15). However, this argument misses the point that Rule 41(b) addresses the location of the property to be searched and places limitations upon the magistrate judge's authority to authorize searches of that property. While the NIT was installed in the Eastern District of Virginia, the search of Defendant's computer occurred in Florida. Recognizing this dilemma, the Government argues for a liberal or broad interpretation of Rule 41. (*Id.*). The Government cites *United States v. New York Telephone Co.*, 434 U.S. 159, 169 & n.16 (1977), wherein the Supreme Court upheld a search warrant for a pen register to collect dialed telephone number information even though Rule 41 at the time did not specifically include electronic intrusions in the definition of property. The Government also cites a more recent case where the Ninth Circuit Court of Appeals upheld a warrant allowing video surveillance, despite Rule 41's silence on this type of warrant. *See United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (en banc). However, neither of these opinions authorize a magistrate judge to authorize a search of property outside his or her district pursuant to Rule 41(b)(1). This Court recognizes that some flexibility in the type of search is appropriate, but the Court is unwilling to expand the authority of the magistrate judge beyond the geographic limitations clearly established by Rule 41(b).

***6** The Government next turns to Rule 41(b)(4) in an attempt to analogize the NIT to a "tracking device." (Doc. 46, p. 17). Rule 41(b)(4) allows the magistrate judge "to issue a warrant to install within the district a tracking device." Because a tracking device monitors the movement of a person or object, the person or object must be located within the district at the time the tracking device is installed. *See* Fed. R. Crim. P. 41(a)(2)(E); 18 U.S.C. § 3117(b). The Government offers a tempting interpretation of this rule by comparing the placement of the NIT onto the government-controlled Playpen server to the concealment of a tracking device in a container holding contraband which is then tracked outside of the district where the warrant was issued.[4] (Doc. 46,

p. 18). However, by the Government's admission, once installed on the Playpen server, the NIT does nothing until the user logs onto the government-controlled server in that district and downloads the NIT. (Doc. 46, p. 15). The warrant authorizes the installation of the NIT onto the government-controlled Playpen server and not onto Defendant's computer, which is located outside of the Eastern District of Virginia. Moreover, the NIT does not track; it searches. As discussed above, the NIT is designed to search the user's computer for certain information, including the IP address, and to transmit that data back to a server controlled by law enforcement. *See United States v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan 28, 2016); *United States v. Levin*, No. 15-cr-10271-WGY, 2016 WL 1589824, at *6 (D. Mass. May 5, 2016); *United States v. Arterbury*, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *21 (N.D. Okla. Apr 25, 2016). The Government relies upon *United States v. Matish*, No. 4:16cr16, 2016 WL 3545776, at *17 (E.D. Va. June 23, 2016), and *United States v. Darby*, No. 2:16cr36, 2016 WL 3189703, at *12 (E.D. Va. June 3, 2016), which hold that a magistrate judge has authority under Rule 41(b)(4) to issue a warrant to deploy a NIT as a "tracking device," because anyone logging in to Playpen makes a "virtual trip" to Virginia. The Court does not find this analysis persuasive for the reasons given. Accordingly, Rule 41(b)(4) is inapplicable.

4 *See United States v. Knotts*, 460 U.S. 276, 285 (1983) (upholding against a Fourth Amendment challenge the use of a tracking device placed in a container of chloroform which was thereafter tracked).

To the extent that the Government argues 28 U.S.C. § 636(a) only limits where a magistrate judge may possess powers conferred by the Federal Magistrates Act and by the Federal Rules of Criminal Procedure and does not, therefore, restrict the geographic locale where a search warrant may be executed (Doc. 46, p. 21), the Court rejects this argument as a basis for finding the NIT warrant proper under Rule 41(b)(1) and (b)(4). That is, Rule 41(b)(1), (2), and (4) all require the property to be located within the district where the magistrate judge is sitting. Only Rule 41(b)(3) and (5) authorize a magistrate judge to issue a warrant to search property not located within the district where the magistrate judge sits. Therefore, the two subsections of Rule 41(b) relied upon by the Government clearly render a warrant authorizing a search outside of the issuing magistrate judge's district ineffective. The Government does not rely upon any other subsection of Rule 41(b), and the Court finds the remaining subsections inapplicable. Having found that the magistrate judge in the Eastern District of Virginia violated Rule 41(b) by issuing the NIT warrant and thereby allowing a search of property located outside of her district, the Court turns to whether the Defendant's confessions and the physical evidence obtained on September 11 and 12, 2015 should be suppressed.

Defendant contends that, for purposes of the Fourth Amendment, a search warrant issued in violation of Rule 41(b) is "no warrant at all." *United States v. Krueger*, 809 F.3d 1109, 1126 (10th Cir. 2015) (Gorsuch, J., concurring). For this reason, Defendant submits that the violation of Rule 41(b) renders the Government's search of his laptop a warrantless search in violation of the Fourth Amendment. (*Id.*). Defendant contends that the instant NIT warrant was void *ab initio* because of the magistrate judge's lack of jurisdiction to authorize the search in the first instance. *See Levin*, 2016 WL 2596010, at *10 13 (holding that the good faith exception to suppression is unavailable where warrant is void *ab initio*). This Court declines to follow the cases holding that a violation of Rule 41(b) renders the warrant void *ab initio.* The Court finds that the magistrate judge in the Eastern District of Virginia had the authority to issue search warrants that is, the inherent power to do so. The Court views a Rule 41(b) violation to be a technical or procedural violation, similar to a violation of Rule 41(a), (c), (d), or (e), which Defendant concedes are technical violations. [5] (Doc. 36, p. 13).

5 If the lack of probable cause supporting the search warrant under Rule 41(d) is a technical violation, then issuing a warrant supported by probable cause but erroneously authorizing the search of property outside the issuing court's district is also a technical violation. After all, the Fourth Amendment requires a showing of probable cause prior to the issuance of a warrant.

***7** The Government accurately asserts that the Fourth Amendment does not impose a venue requirement for applying for a search warrant. (Doc. 46, p. 26). The Fourth Amendment imposes three requirements: (1) a search warrant must be issued by a neutral magistrate; (2) it must be based on a showing of probable cause, and (3) it must satisfy the particularity requirement. *Dalia v. United States*, 441 U.S. 238, 255 (1979). Defendant does not contend that any of these considerations were not met

in the application for, and issuance of, the NIT warrant in this case.

In the absence of a constitutional violation, such as the case at bar, "Rule 41 requires suppression of evidence only where (1) there was '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) there is evidence of intentional and deliberate disregard of a provision in the Rule." *United States v. Loyd*, 721 F.2d 331, 333 (11th Cir. 1983) (per curium) (quoting *United States v. Sefanson*, 648 F.2d 1231, 1235 (9th Cir. 1981)). Even assuming prejudice has been established by Defendant, the good faith exception applies in this case as discussed below.

The Supreme Court in *United States v. Leon*, 468 U.S. 897, 923 (1984) identified four situations in which the good faith exception does not apply: (1) when "the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth," (2) when "the issuing magistrate wholly abandoned his judicial role," (3) when the affidavit supporting the application for a warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," and (4) when "a warrant may be so facially deficient i.e., in failing to particularize the place to be searched or the things to be seized that the executing officers cannot reasonably presume it to be valid." Defendant submits that the NIT warrant recklessly described the search would take place in the Eastern District of Virginia and that no objectively reasonable FBI agent with nineteen years of experience would believe the NIT warrant was valid due to the limitations imposed by Rule 41(b). (Doc. 36, pp. 13 14). Defendant's argument appears to focus on the fourth category identified by the Supreme Court in *Leon*: facial deficiencies in the search warrant.

The Government counters that suppression is a "last resort," not the "first impulse," and any benefit to suppressing evidence must outweigh the substantial social costs that result when "guilty and possibly dangerous defendants go free." *Herring v. United States*, 555 U.S. 135, 140 41 (2009). In *United States v. Berkos*, the Seventh Circuit observed that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause and with advance judicial approval." 543 F.3d at 396 (quoting *United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008)). The Court in *Berkos* further remarked that the remedy of allowing a defendant to go free based on a violation of Rule 41's requirements would be "wildly out of proportion to the wrong." [6] *Id.* (quoting *Cazares-Olivas*, 515 F.3d at 730). In addition, "[t]he exclusionary rule should be limited to those situations where its remedial objectives are best served; i.e., to deter illegal police conduct, not mistakes by judges and magistrates." *United States v. Burgos-Montes*, 786 F.3d 92, 109 (1st Cir. 2015) (quoting *United States v. Bonner*, 808 F.2d 864, 867 (1st Cir. 1986)), *cert. denied*, 136 S. Ct. 599 (2015).

6 The Court in *Berkos* remarked that had the government made and preserved this argument below, the Court would have affirmed the district judge's denial of Defendant's motion to suppress. 543 F.3d at 396.

***8** Returning to the question of prejudice arising from the Rule 41(b) violation, the defense does not suggest that law enforcement officers intentionally and deliberately disregarded a provision in the Rule. At most, Defendant submits "the NIT Warrant recklessly described the search would take place in the Eastern District of Virginia." (Doc. 36, pp. 13 14). Therefore, the Court must consider whether prejudice is established under the first prong that the search utilizing a NIT might not have occurred if the rule had been followed.

In seeking the NIT warrant, the FBI attests, in pertinent part, as follows:

> 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 other computers or "nodes," as described herein, other investigative procedures [aside from the NIT] 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.

(Doc. 36-1, Ex. 3, ¶ 31). The application in support of the NIT warrant makes it abundantly clear that law

enforcement had no realistic chance of identifying the IP address associated with Defendant's computer without the NIT. Had the magistrate judge followed Rule 41(b), the search of Defendant's computer would not have occurred. Accordingly, Defendant has clearly proven that he was prejudiced by the violation of Rule 41(b). However, the FBI agents acted upon the NIT warrant with objectively reasonable reliance on the warrant's authority. *See Leon*, 468 U.S. at 992. The Court does not accept Defendant's argument that the special agents should have known the limits of Rule 41(b) vis-à -vis the NIT warrant. The parties in briefing the motion to suppress have expended sixty pages of written argument, and have cited competing case law largely addressing the scope and import of the various subsections of Rule 41(b). Furthermore, Defendant failed to offer evidence that the agents possessed some unique knowledge rendering their reliance upon the NIT warrant objectively reasonable.[7] *See id.* ("In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination...."). Accordingly, the Court finds the good faith exception to suppression is applicable.

7 *See United States v. Zimmerman*, 277 F.3d 426, 436 (3d Cir. 2002) ("The test for whether the good faith exception applies is 'whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.) (quoting *United States v. Loy*, 191 F.3d 360, 367 (3d Cir. 1999)).

Finally, the Court turns to the Government's argument that an alleged violation of Rule 41(b) is sufficiently attenuated from Defendant's subsequent confession and voluntary relinquishment of his laptop and electronic data storage devices. (Doc. 46, p. 37). It is undisputed that six months after agents obtained the IP address associated with Defendant's residence, they went to his home, identified themselves as law enforcement officers, disclosed the purpose of their investigation, cautioned the Defendant that he was not required to submit to an interview, and were nevertheless invited inside by Defendant. Thereafter, Defendant provided a detailed and voluntary statement in which he confessed to accessing and downloading child pornography from the Playpen server as well as other servers. Defendant voluntarily relinquished his laptop and numerous electronic storage medium. As the agents were departing his residence, Defendant went to the agent's vehicle and offered to contact them if he discovered additional devices containing child pornography. Later that same day, Defendant in fact called the agents to advise he had additional devices that he wanted to surrender. The agents met Defendant the following morning in a public location where he turned over additional storage devices. Thirteen days later, the agents applied for and were granted a warrant to search the laptop and storage devices. The warrant was issued by a magistrate judge sitting in the Middle District of Florida, and that search warrant is not challenged, although Defendant seeks the exclusion of his confession, his laptop, and all storage devices as fruit of the poisonous tree.

***9** "Where a 'consent to search' follows allegedly unlawful police conduct, the court *must* determine (1) whether the consent was voluntary; *and* (2) whether the consent, even if voluntary, was the product of the unlawful police conduct. *United States v. Moreno-Ortega,* 522 Fed.Appx. 729, 732 (11th Cir. 2013) (per curiam), *cert. denied sub. nom.*, 134 S. Ct. 704 (2013). The Government bears the burden on both issues. *Id.* Three non-exhaustive factors guide this attenuation analysis under the second prong: (1) the temporal proximity between the unlawful conduct and the consent; (2) the presence of intervening circumstances; and (3) the purpose and flagrancy of the unlawful conduct.

In *Moreno-Ortega*, officers responded to the defendant's residence to execute an outstanding arrest warrant. *Id.* at 731. A woman opened the door and, upon seeing the police, ran down the hallway, prompting officers to enter the home without permission, conduct a protective sweep and detain the occupants. *Id.* When the defendant arrived home, he was arrested and brought into the house. *Id.* Approximately thirty to thirty-five minutes later an interpreter arrived, the defendant was interviewed for approximately eleven minutes, was advised of his rights, and provided verbal and written consent to search. *Id.* Officers discovered contraband during the execution of the consensual search, and the defendant moved to suppress the evidence as the product of the initial illegal entry into the residence. *Id.* at 732. The district judge, and subsequently the Eleventh Circuit Court of Appeals, found the verbal and written consent sufficiently attenuated from the initial illegality, thus rendering suppression inappropriate.

As the Supreme Court observed long ago:

> We need not hold that all evidence is fruit of the poisonous tree simply because it would not have come to light but for the illegal actions of the police. Rather, the more apt question in such a case is whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.

Wong Sun v. United States, 371 U.S. 471, 487 88 (1963) (citation and internal quotation marks omitted). Rather, the Court is obliged to determine whether the consent "was sufficiently an act of free will to purge the primary taint of the unlawful invasion," or, alternatively, whether the causal connection had "become so attenuated as to dissipate the taint." *Id.* at 486 87.

The police officers in *Delancy* arrived at the defendant's residence to execute an arrest warrant and observed through the partially open door the defendant seated on a couch. *Id.* at 1301. Officers observed the defendant hiding an object in the cushions of the couch and entered the house to conduct a protective sweep. *Id.* The defendant's girlfriend spoke with officers for ten to twenty minutes and provided written consent to search the residence. *Id.* at 1310 11. On appeal, the Court noted that although the temporal proximity between the unlawful entry and the consent to search was relatively brief, the written consent to search which included notification of the right to refuse consent constitutes an intervening circumstance that interrupted the causal connection between the illegal act and the consent. *Id.* Turning to the third factor, the Court found the purpose of the entry was to secure the officers' safety, particularly since the defendant was known to possess weapons, and that the conduct was not flagrant. *Id.* at 1312. Accordingly, the motion to suppress was denied. Additionally, the Supreme Court recently held that discovery of a valid, pre-existing arrest warrant attenuated the connection between an unconstitutional investigatory stop and evidence seized incident to the defendant's arrest. *See Utah v. Strieff*, 136 S. Ct. 2056, 2061 63 (2016).

***10** In the instant case, the NIT warrant was obtained on February 20, 2015, and Defendant was searched via the NIT on March 1, 2015. Six months later, on September 11, 2015, officers conducted a consensual, non-custodial interview of Defendant. There is no dispute over whether Defendant consented to speak with the officers or whether he knew he had the right to refuse their request. Similarly, there is no dispute that Defendant provided a voluntary confession to the officers. The passage of twenty-six weeks from the NIT search to the consensual encounter with Defendant weighs heavily in favor of admissibility. Secondly, intervening circumstances exist which support admission of the evidence. Defendant's voluntary confession, his voluntarily relinquishing of his laptop and electronic devices, and his initiative in notifying the officers later in the day that he had located additional storage devices for the officers' inspection all constitute intervening circumstances favoring admissibility. Added to these intervening circumstances, the Court considers that the officers sought and obtained a search warrant prior to inspecting the devices obtained from Defendant. It is also abundantly clear that the officers did not act with any purposeful or flagrant misconduct. To the contrary, the officers went to considerable lengths to ensure Defendant understood his rights, including the right not to cooperate in the investigation, and sought judicial oversight at the appropriate time. For these reasons, the violation of Rule 41(b) is sufficiently attenuated from the events giving rise to Defendant's confession and the procurement of his laptop and electronic storage devices to support admission of that evidence.

VI. CONCLUSION

It is therefore **ORDERED AND ADJUDGED** that Defendant Adams' Motion to Suppress Evidence (Doc. 36) is **DENIED**.

DONE AND ORDERED in Orlando, Florida on August 10, 2016. Copies furnished to:

All Citations

Slip Copy, 2016 WL 4212079

2016 WL 4771096
Only the Westlaw citation is currently available.
United States District Court,
W.D. Arkansas, Fayetteville Division.

United States of America, Plaintiff
v.
Anthony Allen Jean, Defendant.

Case No. 5:15-CR-50087-001
|
Signed September 13, 2016

Attorneys and Law Firms

Denis Dean, United States Attorney's Office, Fort Smith, AR, for Plaintiff.

Jose Manuel Alfaro, Federal Public Defender Western District of Arkansas, Fayetteville, AR, for Defendant.

MEMORANDUM OPINION AND ORDER

TIMOTHY L. BROOKS, UNITED STATES DISTRICT JUDGE

***1** Now pending before the Court is a Motion to Suppress Evidence (Doc. 19) filed under seal by Defendant Anthony Allen Jean. The parties fully briefed the Motion, and on June 28, 2016, the Court held an evidentiary hearing, at which time the Government and Mr. Jean each called a witness to testify. The Court then entertained oral argument before taking the matter under advisement. Now having considered these complex issues thoroughly, the Court finds that Mr. Jean's Motion to Suppress Evidence (Doc. 19) should be **DENIED** for the reasons explained herein.

I. BACKGROUND

Mr. Jean was indicted on December 9, 2015 (Doc. 1), on four counts of knowingly receiving child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1); one count of knowingly possessing a laptop computer containing images of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2); and a forfeiture allegation.

Mr. Jean is accused of downloading child pornography from a website called "Playpen." The Playpen website operated as a "hidden service" on "The Onion Router," which allows users to roam the internet in complete anonymity. In the course of its investigation, the FBI was able circumvent the anonymity feature a feat that Mr. Jean now challenges as a constitutionally impermissible violation of his rights under the Fourth Amendment and the Federal Rules of Criminal Procedure.

The TOR Network, a/k/a the "Dark Web"

A primer of The Onion Router, or "TOR network," for short, is necessary for an understanding of the issues presented. The Onion Router is so named because of its onion-like layers of encryption that operate to obscure users' identities. Anyone may download TOR software for free. The TOR browser masks a user's true Internet Protocol ("IP") address by bouncing user communications around a distributed network of relay computers, called "nodes," which are run by volunteers around the world. When a TOR user accesses a website, the IP address of a TOR "exit node" will appear in the website's IP log, rather than the user's actual IP address. Through these mechanisms, the TOR software prevents the tracing of a user's IP address, thereby concealing the identity of the user at every node or "hop" along the information highway.

[1] This is true with respect to the relay of communications after passing through the first relay node on the distributed network. Technically, however, the user's true IP address is contained on the communication stream to the very first node on the route.

The TOR network was originally designed by the United States Naval Research Laboratory to protect intelligence communications online, and legal uses for the network include whistleblowing activities, investigative journalism, activism, and scholarship dealing with such issues as cyber-spying and censorship. Despite these legal uses, TOR has developed a reputation for hosting illicit criminal activity, as well. For this reason, the TOR network of websites called "hidden services"[2] is commonly

referred to by TOR users and non-users alike as the "dark web." This name is apt for two reasons. First, the TOR browser enables users to cloak their identities in darkness like guests to a dimly lit masquerade ball using masks to conceal their faces. Second, the TOR network is an ideal forum for dark, illegal activities to flourish, precisely because TOR users remain masked, and this allows them to escape easy detection by law enforcement.

[2] TOR hidden services bear the suffix ".onion rather than ".com.

***2** In his testimony at the motion hearing, FBI Special Agent Dan Alfin explained the TOR network and its hidden services this way:

> The Tor network is accessible initially through use of the regular Internet. It runs on top of the regular Internet, and it is made up of hundreds of thousands of computers all around the world.
>
> Tor affords its users two primary uses. The first is the user using the Tor network can use it to connect to a website or other type of Internet service on the regular Internet in an anonymous capability. So a user could use the Tor software or the Tor browser software to connect to a regular Internet website, Google.com, CNN.com, any normal website. In doing so through the Tor network, that website cannot see where you're actually coming from. So if I were to access Google.com from this courtroom using the Tor software, Google would not know that I was here in Arkansas. It may pull an IP address somewhere else in the country or somewhere else in the world. It wouldn't be able to locate me here.
>
> Another use of the Tor network [is] what are referred to as hidden services. So when you run a website or other Internet service within the Tor network, that service is now referred to as a hidden service and so when a website is configured to operate as a hidden service, it can only be accessed through use of the Tor software. It can no longer be accessed on the traditional Internet in the manner that you would normally access Google.com. You need to use special [TOR] software to access the hidden service.
>
> And so the hidden service affords the same [ ] benefits that I described earlier in that a user who accesses a hidden service, his or her IP address and other identifying information is concealed. The owner and operator of the hidden service cannot see it. The additional benefit that Tor provides to operators of hidden services is that the true IP address and location of the hidden service [are] similarly concealed .... [The operators] could be anywhere in the world. And so Tor hidden services are frequently used to host child pornography websites because of these types of security benefits afforded to operators of such websites, and these are the areas where I focus the majority of my investigative work.

(Doc. 38, pp.16-17).

The Playpen Website

In August of 2014, Agent Alfin discovered the existence of the Playpen website which was configured as a "hidden service" on the TOR network and he came to learn that the website's primary purpose was dedicated to the advertisement and distribution of child pornography. Because the website operated in complete anonymity on the TOR network, law enforcement had no readily available means to identify its owner/operator, much less its users. Then, in December of 2014, the FBI received a serendipitous break. The Playpen operator inadvertently misconfigured the website's TOR settings during an update temporarily deactivating its cloaking mechanism for a few days which was enough time for investigators to locate a computer server in North Carolina that was being used to host the Playpen website. This, in turn, led to the arrest of Playpen's owner on February 19, 2015, at his residence in Naples, Florida which further resulted in the FBI gaining access to the owner's administrative account, and with that came the ability to control the Playpen website.

The NIT Warrant

***3** But investigators still had no means to identify and locate the website's users, whom they believed to be downloading and distributing child pornography in violation of federal law.[3] The users' identifying information was purposely unknown to Playpen's owner, and the users' IP addresses remained concealed because the website was only accessible as a hidden service on the TOR network, thus providing total anonymity to the users. So the FBI devised a plan. First, agents

made a copy of the Playpen website and placed it on a government computer server located in the Eastern District of Virginia. Then, after obtaining a search warrant, the FBI re-launched the Playpen website from its own computer server in Virginia, secretly assuming administrative control over the website for a window of approximately 13 days, from February 20, 2015, to March 4, 2015.

[3] *See* Agent Alfin's testimony, *id.* at pp. 36 37.

The FBI submitted the application for the search warrant to Magistrate Judge Theresa Carroll Buchanan in the Eastern District of Virginia. *See* Doc. 19-2. The warrant application was supported by a 31-page affidavit signed by Special Agent Douglas Macfarlane. *See* Doc. 19-2, pp. 2-32. In the affidavit, Agent Macfarlane first explained why there was probable cause to believe that users of the Playpen website were committing criminal acts related to the exploitation of children. Agent Macfarlane's affidavit then requested Judge Buchanan to authorize the FBI to deploy computer code, which it refers to as a "Network Investigative Technique" ("NIT"), from its server in Virginia that would be used to host the Playpen website. When a Playpen user's computer (defined in the affidavit and warrant as an "activating computer") would log into the website using a username and password, the NIT would surreptitiously deploy and "cause" the user's "activating computer" wherever it might be located to report back certain identifying information to the government's computer on the other end of the line. *Id.* at pp. 30-31.

Judge Buchanan made a finding of probable cause and signed the warrant authorizing use of the NIT to search "[t]he activating computers[4] ... of any user or administrator who logs into the [Playpen] WEBSITE by entering a username and password." *Id.* at p. 34. The warrant's authorization was expressly limited to a period of not more than 30 days. *Id.* The items authorized to be "seized" were expressly identified and limited to the following identifying information:

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 would 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;[5]

Attachment B to the warrant, *id.* at p. 35.

[4] The term "activating computer is explained in the warrant application to mean the computer of any Playpen user "wherever located who subsequently logged into the website with a username and password. *See* ¶46(a) of the Warrant Application, *id.* at p. 30.

[5] The MAC address is a unique identifier associated with a particular network adapter, and, in contrast to the IP address, does not change, because it is hardwired into the computer or device itself.

Finding of Probable Cause

Judge Buchanan's finding of probable cause was based on Agent Macfarlane's affidavit in support of the search warrant, which provided, in part:

> ***4** Because the TARGET WEBSITE is a Tor hidden service, it does not reside on the traditional or "open" Internet. A user may only access the TARGET WEBSITE through the Tor network. Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the Site. Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the

> traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. The TARGET WEBSITE is listed in that section. Accessing the TARGET WEBSITE therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon the TARGET WEBSITE without understanding its purpose and content.

Id. at pp. 13-14. Agent Alfin elaborated on this point when he testified at the hearing that it was "incredibly unlikely" that a user would simply stumble upon the Playpen website without knowing the website's illegal purpose. *See* Doc. 38, p. 20.

The FBI's Use of the NIT

Agent Alfin also testified that he had personal knowledge as to how the FBI went about deploying the NIT from the Playpen server onto a user's computer. The NIT was designed to automatically deploy once an activating computer (1) entered the Playpen website via a username and password, and then (2) clicked on a forum link to begin downloading child pornography.[6] (Doc. 38, p. 86). The FBI was able to cause the user's computer to report the identifying information by exploiting a defective window in the TOR broswer, through which it ran what amounts to malware[7] on the user's computer, with the objective being to override the TOR browser's and the user's computer security settings, and then "cause" the user's computer to return discrete, content-neutral items of identifying information back to the FBI. *Id.* at pp. 60-61.[8]

6 Although the warrant authorized deployment of the NIT upon the user accessing the website with his username and password, the "FBI further restricted how it] deployed the technique, and in most instances, the NIT was not deployed until the user actually took the final step to begin the download of child pornography. (Doc. 38, p. 38).

7 Malware means "malicious software. Agent Aflin objects to describing the NIT as malware, because the term has a derogatory connotation, and in fact is used to describe criminal activity when used by a computer hacker for unlawful purposes. Nevertheless, Agent Alfin concedes that when used as a term of art to explain an ethical hacking technique used by law enforcement, the term malware is descriptive of the NIT used here. *See id.* at pp. 39 40. Thus, where descriptively appropriate, the Court has used the term malware interchangeably with the term NIT.

8 Although the Defendant's expert, Dr. Christopher Soghoian, testified that he was philosophically opposed to the FBI's use of such "exploits, *id.* at pp. 107 108, 123 125, the Motion to Suppress does not identify the FBI's use of the exploit as a constitutional infirmity.

Important to the Court's analysis below is Agent Alfin's testimony that the NIT deployed and returned the identifying information while the user's computer was (1) actually online, (2) connected to and actively communicating with the FBI's computer in Virginia, and (3) while the user was in the process of receiving child pornography. As Agent Alfin explained:

> As soon as a user clicks on the post, they begin downloading the material from that post. Additionally they download the NIT instructions to their computer, and while the post is still ... downloading, the NIT does its business and sends the information back to the FBI. This happens very quickly. In the matter at hand, the entire transmission generated by the NIT took place in approximately 0.27 seconds. Again, it happened very quickly because it

> was just transferring a very limited amount of information .... [T]he NIT would be triggered and deploy and likely complete its task before that page even fully loads.

***5** *Id.* at pp. 86-87. The entire objective of the NIT transaction was consummated in the blink of an eye,[9] while the user's computer was still in the process of actively downloading child pornography from the computer hosting the Playpen website in Virginia. *See* Doc. 38, pp. 88-89.

9 Harvard Database of Useful Biological Numbers, http://bionumbers.hms.harvard.edu/bionumber.aspx?&id 100706&ver 1 (last visited July 5, 2016) (noting that the average duration of a single eye blink is between 0.1 and 0.4 seconds).

The FBI monitored and generated reports of all Playpen user activity during the authorized period of surveillance. [0] The reports contained two sets of data. *See id.* at pp. 40-41. The first set related to Playpen website usage and included the date each user registered his account with Playpen, the number of hours that each user was logged into the website during the monitoring period, and the specific posts each user accessed while online. None of this data was gathered using the malware, but was instead observed directly by the FBI through website monitoring.

10 Although the warrant authorized the NIT to be used for no more than 30 days, the FBI's monitoring of the Playpen website and usage of the NIT actually took place during a 13 day period from February 20 through March 4, 2015.

The second set of data was seized by virtue of the malware causing each user's computer to return the identifying information (without the user's knowledge) to the government's computer in Virginia. This second set of data, as authorized by the warrant, included the user's MAC address, hostname, log-on name, and the activating computer's IP address.

Interestingly though, the user's IP address the most critical piece of information in locating the user does not actually reside on the user's computer. IP addresses are assigned by an Internet Service Provider ("ISP") much like one's residential address is assigned by the postal service. The IP address is maintained on the internet modem that connects an internet device to the internet. *See id.* at p. 43. Ordinarily, one's true IP address can be determined with relative ease because it is always attached, like a "return address," to every "envelope" of information exchanged back and forth by computers that are actively communicating with each other over the internet. But this is not so on the TOR network, where a user's true IP address is intentionally masked by the shuffling of information into different envelopes with different return addresses at each node along the route. Here, the FBI's malware circumvented TOR's veil simply by causing the user's computer to return the "envelopes" of seized information to the government's computer via the regular internet which had the clever side effect of causing the user's true "return address" to be written on the envelope. With the user's true IP address in hand, the FBI subpoenaed the internet service provider and in effect turned on the lights to unmask the user's real location.

11 *See* Agent Alfin's testimony, Doc. 38, p. 92. (explaining that the information "was sent back] in clear text over the regular Internet). *See also* Dr. Soghoian's testimony, Doc. 38, p. 148. ("The NIT did not harvest the IP address.... the NIT harvested ... information about the computer; ... It put the information] in a letter, put the letter in an envelope and sent it back.... the contents of the envelope does not include the IP address, and Special Agent Alfin testified that the government, in fact, did not harvest the IP address from Mr. Jean's] computer; they merely looked to see where the NIT response came from and assumed that was the IP address for the defendant.).

The Investigation of Anthony Allen Jean

***6** Agent Alfin testified that the Playpen website was accessed thousands of times during the 13 days it was monitored by the FBI. *Id.* at p. 65. As to the specific investigation of Defendant Anthony Allen Jean, Agent Alfin testified that on March 1, 2015, an individual logged into the Playpen website with the username "regalbegal" and used the website index to select a forum dedicated to "Preteen Videos Girls Hardcore." *Id.* at pp. 44-45. There, regalbegal allegedly opened a post that purported to contain images of prepubescent female children engaged in penetrative sexual activity.

Once regalbegal opened this post, the NIT protocol was triggered, and, unbeknownst to regalbegal, the malware deployed from the Playpen server in Virginia to his computer. According to Agent Alfin, in 0.27 seconds, while regalbegal was still actively connected to (and downloading child pornography from) the Playpen server, the malware caused his computer to transmit the information authorized by the warrant back to the government computer server located in the Eastern District of Virginia. And with that return transmission of data over the regular internet came regalbegal's true IP address.

The Administrative Subpoena

From the IP address alone, and using publically available data, the FBI could determine the region of the country where regalbegal resided, as well as the particular ISP, Cox Communications ("Cox"), associated with his IP address. The FBI then sent an administrative subpoena to Cox, and Cox provided the FBI with the name and residential address affiliated with regalbegal's IP address.

The Residential Search Warrant

Soon after obtaining this subscriber information, law enforcement applied to Magistrate Judge Erin L. Setser of the Western District of Arkansas for a residential search warrant (Doc. 19-1) to be executed at Mr. Jean's residence. [2] The warrant was signed on July 8, 2015, and executed on July 9, 2015. When the FBI first arrived at the residence, they advised Mr. Jean that they had a search warrant, but they did not volunteer that they had located his whereabouts by tracing his IP address. Mr. Jean apparently cooperated with investigating agents and allegedly made incriminating statements both at the time of his arrest and later during an interview on July 17, 2015. His computer equipment was seized at that time, and a later search revealed that the computer contained images of child pornography.

12 Mr. Jean does not separately contest the validity of the administrative subpoena or the residential warrant in his Motion to Suppress.

The Motion to Suppress

After charges were brought some five months later, Mr. Jean was arrested and ordered detained on December 15, 2015. On March 21, 2016, his attorney filed the instant Motion, challenging the validity of the Virginia search warrant and seeking to suppress all physical evidence seized from Mr. Jean's computer and related equipment, as well as any alleged incriminating statements he made to law enforcement as "fruit of the poisonous tree." Mr. Jean maintains that the Virginia search warrant did not authorize use of the NIT to search any activating computer outside the Eastern District of Virginia, and as his computer was located outside that district, the search was not authorized. He also argues that the Virginia warrant was issued in violation of Federal Rule of Criminal Procedure 41(b), which outlines the scope of a magistrate judge's authority to issue search warrants. Lastly, he contends that the search warrant itself was not supported by probable cause. The Government filed a Response to the Motion, and both sides supplied the Court with recent persuasive authority from other district courts that have considered the validity of this very same search warrant. In the following discussion, the Court will analyze whether the Virginia search warrant validly comported with the requirements of the Fourth Amendment; whether the magistrate judge who authorized the warrant did so in violation of Rule 41(b); and, finally, if a violation of Rule 41(b) did occur, whether suppression of the evidence is the appropriate remedy.

II. DISCUSSION

A. Did the NIT Warrant Comply with the Fourth Amendment?

1. Was the NIT Warrant Even Necessary?

***7** Mr. Jean has offered several arguments as to why the Virginia warrant failed to comply with the Fourth Amendment and the Federal Rules, and the Court will reach those arguments in due course. However, it seems prudent at the start of the discussion to consider whether it was even necessary for law enforcement to obtain this search warrant at all. The question is somewhat academic, since the FBI did, in fact, make an application for a search warrant, apparently believing it to be necessary, and did obtain the warrant before utilizing the NIT protocol on the Playpen website. Nevertheless the Court begins by

asking whether an alleged Playpen user like Mr. Jean had any legitimate expectation of privacy in his IP address the sole piece of information that led investigators to his door.

Agent Alfin confirmed on the stand that the FBI was able to locate the residential address of the Playpen user named regalbegal by using *only* his IP address. In fact the only information placed on the administrative subpoena served on Cox was the IP address in question, and the date and time it was collected. The rest of the information reported by the NIT (including regalbegal's MAC address, host name, and operating system) potentially could have been helpful to the FBI if there had been a question as to which of several computers or electronic devices in the residence had been accessing Playpen. [3] But no such question exists in Mr. Jean's case, because once investigators arrived at his home, he immediately confessed to accessing child pornography and pointed out the computer he had used. Even if the Court were to determine that Mr. Jean had a legitimate expectation of privacy in all the other information the FBI actually collected from his computer, the question of whether he had a reasonable expectation of privacy in the IP address which was maintained on his modem and ordinarily accompanied messages sent via the regular internet is uniquely important because it is only the IP address that gives rise to Mr. Jean's "fruit of the poisonous tree" argument in favor of suppressing the evidence.

13 This is because several internet capable devices in a given household may share a common IP address.

The Eight Circuit has explained that, "[a]s a preliminary matter ... in order to find a violation of the Fourth Amendment, there must be a legitimate expectation of privacy in the area searched and the items seized." *United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir.2002) (citing *Smith v. Maryland*, 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)). "If there is no legitimate expectation of privacy, then there can be no Fourth Amendment violation." *Id.* The Eighth Circuit has never explicitly held that a defendant lacks an expectation of privacy in his IP address and username, unless he has installed a file-sharing program on his computer that makes his files accessible to others. *United States v. Stults*, 575 F.3d 834, 842 (8th Cir.2009). In general, however, "[a] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *United States v. Miller*, 425 U.S. 435, 442 44, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976).

To access the internet at one's residence, an individual must first go through a network that is either connected to the internet or grants access to the internet. An ISP will generally provide this access and assign the resident an IP address. The IP address can change at any time at the ISP's discretion or at the resident's request. The IP address will give clues as to the identity of the ISP, as well as the region or state where the IP address has been assigned. Although the Eighth Circuit has not had the opportunity to rule on the broader issue of whether an internet user who does not use file-sharing software would otherwise enjoy a legitimate expectation of privacy in his IP address, other courts of appeal have clearly decided the issue, and their opinions are instructive.

***8** Before turning to these more recent circuit court opinions, the Court begins its discussion with a Supreme Court opinion issued 40 years ago. The 1976 case of *United States v. Miller* was one in which the Court held that an individual enjoys no legitimate expectation of privacy in bank records showing his various transactions, including his checks and deposit slips. *Id.* The Court reasoned that when one voluntarily conveys such transactional information to third parties for example, to multiple banks one loses any expectation of privacy in those records or transactions. *Id.*

A few years later in 1979, the Court in *Smith v. Maryland* held that an individual has no legitimate expectation of privacy in the list of phone numbers he has dialed from his phone. 442 U.S. at 743 744, 99 S.Ct. 2577. In *Smith*, police had requested that a telephone company install a pen register at its central offices to record all the phone numbers dialed by a particular customer. *Id.* Justice Harry A. Blackmun, writing for the majority in *Smith*, explained that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* Since users know this, he reasoned, they should also understand "that their phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills." *Id.* at 742, 99 S.Ct. 2577.

An IP address does not "belong to" the user in the sense that it is not associated with the user's personal property and cannot be transported to a new location simply by moving the user's personal computer to that new location. For example, if a user were to take his home laptop computer to a local coffee shop to browse the internet, his IP address would not follow him from his home to the coffee shop. Instead, he would use the coffee shop's IP address when browsing online.

The Third Circuit has definitively held that a person has "no reasonable expectation of privacy in his IP address and so cannot establish a Fourth Amendment violation" because IP addresses are routinely conveyed to and from third parties, including ISPs. *United States v. Christie*, 624 F.3d 558, 574 (3d Cir.2010). Similarly, the Ninth Circuit, relying on an analogy to the pen register in *Smith*, has determined that IP addresses are not subject to Fourth Amendment protection because they "are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir.2008) (discussing and comparing to *Smith*, 442 U.S. at 742, 99 S.Ct. 2577). Both of these appellate courts concluded that there is no need to obtain a search warrant to capture an IP address because the IP address itself conveys no substantive information about the user or the contents of the user's online communications just as a pen register, which does not require a warrant to install, only captures "the addressing information associated with phone calls" and not the content of the communications themselves. *See id.* at 509.

The Fourth, Tenth, and Sixth Circuits have long held that subscriber information that is provided to an ISP is not protected by the Fourth Amendment's privacy expectations, since the subscriber voluntarily conveys that information to the system operator and thus assumes the risk that the company might later provide it to law enforcement if served with an administrative subpoena. *See United States v. Bynum*, 604 F.3d 161, 164 (4th Cir.2010); *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir.2008); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir.2001). In general, then, "when an individual reveals private information to another, he assumes the risk that this confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." *United States v. Jacobsen* 466 U.S. 109, 117, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984).

***9** Turning now to the thorny issue of whether any of the above cases and legal principles should apply when an internet user has gone to the trouble of downloading TOR software to mask his IP address from public view, a reasonable question to ask is whether the TOR user's expectation of privacy in his IP address may be stronger, or more legitimate, than that of an internet user who has taken no affirmative steps to conceal his IP address. As explained previously, the TOR software operates on top of the regular internet and in the normal course of using the internet, one's IP address is routinely attached to the back-and-forth transmissions that occur when two computers are actively communicating with each other. This is exactly what happened here when the NIT caused the seized information from Mr. Jean's computer to be transmitted back across the unencrypted regular internet.

TOR's encryption works by substituting components of the IP address of each volunteer node as it hops across the internet, but on its very first hop, the TOR user's true IP address is disclosed to the first node computer in the TOR chain. Thus, the user's true IP address is not a complete secret, and the user must necessarily assume some measure of risk that TOR's encryption technology could be defeated and thereby potentially reveal his true IP address. Taking this reasoning to its logical conclusion, the principles behind the decision in *United States v. Miller* would apply: If a user engaged in illegal activity while using TOR, and law enforcement obtained the user's true IP address, it would follow that the user would have no legitimate expectation of privacy in the IP address, as he "[took] the risk, in revealing his affairs to others," namely, to both his ISP and the owner of the first node computer in the TOR chain "that the information [would] be conveyed by that person to the Government." 425 U.S. at 443, 96 S.Ct. 1619. Indeed, the Supreme Court has repeatedly held "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.*

All of the above authority leads the Court to consider that, if pressed, it could potentially find that the FBI

in the instant case was under no legal obligation to obtain a search warrant to discover the residential IP addresses of Playpen users in the manner that it did, as IP addresses are unlikely to be entitled to the same Fourth Amendment protections as are the substantive contents of users' computers. [4] However, as the reality of the situation is that the FBI *did* obtain a warrant, and there is no definitive authority in this Circuit as of yet regarding the privacy interests either a general user or a TOR user would have in an IP address, the Court will assume that a warrant was necessary in this case, and will analyze below whether the warrant complied with both the Fourth Amendment and the Federal Rules.

14 This would be a very close call though, because unlike some of the cases cited by the Court, the Government here did not actually obtain the information at issue from a third party. Another important distinction has to do with the source of the information which the defendant seeks to have suppressed. For example, if the MAC address (or any other content derived from a search of the computer) was the subject of suppression, the Court would likely find a warrant necessary because such information wasn't obtained or freely available from a third party, but rather it was seized directly from Mr. Jean's computer. The difference here is that Mr. Jean's true IP address is the one piece of information that wasn't harvested from a search of his computer. In fact, the IP address at issue does not even belong to Mr. Jean. The IP address is assigned by the ISP with the intent and understanding that it will be automatically attached to every transmission of data which is directed across the regular internet.

2. Was the Virginia search warrant supported by probable cause?

***10** A court reviewing the validity of a search warrant issued by a magistrate judge must make sure "that the magistrate had a substantial basis for ... [concluding] that probable cause existed." *Illinois v. Gates*, 462 U.S. 213, 238 39, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983) (internal quotation and citation omitted). The question now becomes whether, under the totality of the circumstances, it was reasonable for the magistrate judge to infer that there was a probability or substantial chance of criminal activity being committed by Playpen users, and that deploying the NIT protocol onto the Playpen website in Virginia would reveal evidence of violations of federal law. *See id.* at 230 31, 103 S.Ct. 2317. The Court must bear in mind that "after-the-fact scrutiny by courts of the sufficiency of an affidavit [written in support of a warrant] should not take the form of *de novo* review. A magistrate's 'determination of probable cause should be paid great deference by reviewing courts.' " *Id.* at 236, 103 S.Ct. 2317 (quoting *Spinelli v. United States*, 393 U.S. 410, 419, 89 S.Ct. 584, 21 L.Ed.2d 637 (1969)). Further, "so long as the magistrate had a substantial basis for ... conclud[ing] that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more." *Id.* (internal quotation and citation omitted).

Mr. Jean focuses his probable cause argument on his contention that some of the statements made by Agent Macfarlane in the supporting affidavit were either untrue or potentially misleading. For example, Mr. Jean asserts that innocent TOR users could have unknowingly stumbled upon the Playpen website without understanding that it was dedicated to child pornography. He notes that the homepage of the website did not include enough information or images to allow an unsuspecting user to conclude that child pornography lay within. He contends that accessing the Playpen website did not require as many affirmative steps or as much advance knowledge of the content of the site as Agent Macfarlane's affidavit led the magistrate judge to believe. Finally, he maintains that the name "Playpen" might not have signaled to potential users that the site was devoted to advertising and distributing child pornography, since, according to Mr. Jean, the name "Playpen" is more commonly associated with a men's lifestyle magazine that is a knock-off of *Playboy* magazine, featuring legal, adult pornography. *See* Doc. 19-5 (images from *Playpen* magazine and print advertisements for adult strip clubs that use the name "Playpen").

The Court has considered Mr. Jean's arguments as to probable cause and has reviewed Agent Macfarlane's affidavit carefully. Considering Agent Macfarlane's many years of experience and the level of detail contained in the 31-page affidavit, the Court is well satisfied that the information provided to Judge Buchanan about the contents of the Playpen website, the details of the NIT protocol, and the way that the TOR software and TOR network operated afforded her a substantial basis for determining there was probable cause to believe that Playpen users knew about the contents of the site when they logged in, and did so with the intent to engage

in illegal acts. Agent Macfarlane's affidavit is neither conclusory, nor "bare-bones," but is instead filled with a wealth of information about the reasons why the NIT protocol provided a minimally intrusive method for revealing the locations of Playpen users. The Court is not persuaded, nor does Mr. Jean directly allege, that Agent Macfarlane sought to deceive the magistrate judge in some manner or intentionally placed demonstrably false information in the affidavit. Instead, it appears Mr. Jean simply disagrees with some of the representations made in the affidavit. [5] As the warrant easily meets the totality-of-the-circumstances test for probable cause, it passes constitutional muster on that front.

15 After considering the testimony during the motion hearing of both the Government's expert, Agent Alfin, and Mr. Jean's expert, Dr. Soghoian, the Court is further convinced of the accuracy of the representations in Agent Macfarlane's supporting affidavit. Agent Alfin testified that it would be "incredibly unlikely for any TOR user to accidentally stumble upon the Playpen website without having prior knowledge of its illegal contents. (Doc. 38, p. 20). None of Dr. Soghoian's testimony during the hearing undermined that assertion.

***11** The Government points out that other Courts of Appeal have held that mere membership in a child pornography website even without specific evidence of downloading activity provides sufficient probable cause for a search warrant. *See United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir.2006) (en banc) (citing *United States v. Martin*, 426 F.3d 68, 75 (2d Cir.2005), and *United States v. Froman*, 355 F.3d 882, 890 91 (5th Cir.2004), for the same proposition). This commonsense rule strikes the Court as sound and lends further support to the Court's finding that Judge Buchanan had a substantial basis for concluding that probable cause existed to issue the search warrant and deploy malware to uncover the hidden IP addresses of individuals who logged in as members of the child pornography website known as Playpen.

3. Did the Virginia search warrant meet the particularity requirement of the Fourth Amendment?

The next question the Court must answer is whether the search warrant sufficiently described the place to be searched and items to be seized. According to Mr. Jean, the cover sheet of the Virginia warrant application requested a search warrant as to persons or property "located in the Eastern District of Virginia ...." *See* Doc. 19-2. His argument is that the warrant only authorized a search to take place in the Eastern District Virginia, but the malware actually searched Mr. Jean's computer in the Western District of Arkansas. He further argues that "a fair reading of the warrant and attachment ... authorize[s] searches of 'activating computers' wherever they may be located *in the Eastern District of Virginia*, [and that] there is nothing within the four corners of the warrant that alters its plain language or can reasonably be construed to expand the search authorization to anywhere in the world." (Doc. 19, p. 7 (emphasis added)).

Essentially, Mr. Jean contends that because the data seized from his computer was located outside Virginia, it must be suppressed. Mr. Jean's counsel argues: "To state the obvious, when a warrant authorizes searches in one location, it does not authorize searches in other locations." *Id.* at p. 6. In support of his argument, he cites to various cases in which a warrant was issued to search a particular residential address, but officers searched a different address instead. *See, e.g., Simmons v. City of Paris, Tex.*, 378 F.3d 476 (5th Cir.2004) (warrant for 400 N.W. 14th Street did not justify search of 410 N.W. 14th Street); *Pray v. City of Sandusky*, 49 F.3d 1154 (6th Cir.1995) (warrant for 716 Y2 Erie Street, upper level of a duplex home, did not justify search of 716 Erie Street, lower level of the duplex).

The Government counters that the cases cited to by Mr. Jean are inapposite. The instant case involves an internet-based search, not a search of an apartment building or a duplex. Moreover, the instant search was only triggered after website users voluntarily and remotely accessed a server that was physically located in Virginia. Attachments A and B to the warrant application explain that the NIT protocol and malware would be deployed on "all activating computers" that logged into the website "by entering a username and password." (Doc. 19-2, p. 34). The Government contends that since the server was located in the Eastern District of Virginia, that jurisdiction was the proper place to seek the warrant, as it had the most significant ties to the known location of the server. According to the Government, a reasonable reading of the warrant's scope means the FBI was granted the authority to deploy the NIT protocol from the server in Virginia to the "activating computer" of any user who logged into the server, no matter the user's physical location.

As the entire aim of the NIT protocol was to identify the unknown locations of users who were masking their identities through TOR, the Government maintains it was obvious from the face of the warrant application that the NIT protocol was intended to be deployed to computers in any jurisdiction.

***12** After considering both sides' briefing on this issue, the Court agrees with the Government. The term "activating computer" as used in the exhibits attached to and incorporated into the warrant has a specific meaning and context. The term refers to the computer of any Playpen user who subsequently logged into the website with a username and password. *See* Attachment A to the warrant, Doc. 19-2, p. 34. As stated in the affidavit submitted in support of the warrant request, it is clear that users' "activating computers" are understood to be accessing the website via the internet, and given the anonymity provided by the TOR browser, the users could be located anywhere in the world which created the necessity of the NIT in the first place. Thus, the context for what the FBI was seeking and what the magistrate judge knowingly ordered by using this term in her warrant was authority to search any "activating computer" "wherever located." *Id.* at p. 30.

The Court therefore finds that the warrant application meets the Fourth Amendment's particularity requirement, as "the items to be seized and the places to be searched [were] described with sufficient particularity as to enable the searcher to locate and identify the places and items with reasonable effort and to avoid mistakenly searching the wrong places or seizing the wrong items." *United States v. Gleich*, 397 F.3d 608, 611 (8th Cir.2005).

B. Did the Virginia warrant satisfy Rule 41(b)?

Mr. Jean's next argument is that Judge Buchanan exceeded the authority granted to her by Rule 41(b) of the Federal Rules of Criminal Procedure in issuing the warrant. Rule 41(b) authorizes a magistrate judge to issue a warrant only in certain situations, and that authority is more limited than a district judge's authority. [6] In general, a magistrate judge cannot issue a warrant in her own district to search and seize property located outside the district, unless certain factual situations are present.

16 District judges are not limited by Rule 41(b) as magistrate judges are. Instead, district judges may issue warrants to search property located outside their judicial districts when the requirements of the Fourth Amendment are met. "The Fourth Amendment commands that 'no Warrants shall issue, but upon probable cause, supported by Oath or affirmation. *United States v. Fiorito*, 640 F.3d 338, 345 (8th Cir.2011) (quoting U.S. Const. Amend. IV).

Rule 41(b) provides as follows:

> (b) 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 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:
>
> ***13** (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.

The Government argues that the search warrant at issue here met the requirements of subparts (2) and/or (4) above. According to the Government, Judge Buchanan had authority to issue the warrant under subpart (2) because the NIT constituted "property" [7] that was located in the Eastern District at the time the warrant was issued, and that "might move ... outside the district before the warrant is executed." (Doc. 21, pp. 17-18). The Government also contends that the NIT operated like a "tracking device" described in subpart (4), since the NIT "installed" in the Eastern District of Virginia when users logged into the Playpen website, and then revealed the locations of the users outside the district. *Id.* at p. 18. In response to these arguments, Mr. Jean maintains that subpart (2) does not apply because the "property" to be searched was not the NIT located in the Eastern District of Virginia, but the target information on the users' computers outside the district. *See* Doc. 24, p. 2. As for subpart (4), Mr. Jean disagrees that the NIT was "installed" in the Eastern District of Virginia and argues instead that the NIT installed on the users' computers outside the district.

17 Rule 41(a)(2) defines "property to include documents, books, papers, any other tangible objects, and information.

1. Rule 41(b)(2)

The Court has considered the parties' arguments and finds that subpart (2) does not apply, since the "property" that was the target of the warrant was not the NIT itself, but the information collected by the NIT. This information, at least in Mr. Jean's case, was not "located within the [Eastern District of Virginia] when the warrant was issued." Rule 41(b)(2). Therefore, as applied to the facts here, Judge Buchanan had no authority to issue a search warrant under subpart (2) for property that was not within her judicial district when the warrant was issued.

2. Rule 41(b)(4)

Having likewise considered the parties' arguments with respect to subpart (b)(4), the Court finds that the FBI's NIT was an electronic tool or technique designed and executed for the purpose of tracking the movement of information both within and outside the Eastern District of Virginia. For the reasons explained more fully below, Judge Buchanan had the authority to issue such a warrant pursuant to Rule 41(b)(4), and thus the seizure in question was not unlawful.

The *In Re Warrant* Case

In reaching its conclusion, the Court has considered the cases Mr. Jean cites in opposition to the Government's arguments. *In re Warrant to Search a Target Computer at Premises Unknown* is a decision issued in 2013 by Magistrate Judge Stephen William Smith in the Southern District of Texas. 958 F.Supp.2d 753 (S.D.Tex.2013). *In re Warrant* concerned law enforcement's application for a search warrant to surreptitiously install data extraction software on a computer that was allegedly being used by unknown persons at an unknown location to violate federal laws concerning bank fraud, identity theft, and computer security. *Id.* at 755. Law enforcement had obtained an email address they suspected was being used by an individual or individuals engaging in bank fraud and identity theft online. *Id.* at 759. The FBI's plan was to email a malware program to the suspected email address. Once the email was opened and the malware downloaded, the malware would scour the individual's computer for information about the user's web-based activities and his or her physical location, and then send that information back to the FBI. *Id.*

***14** For a variety of fact-specific reasons not present in Mr. Jean's case, the magistrate judge in *In re Warrant* declined to sign the search warrant authorizing the deployment of malware. First, he found that the government had provided nothing more than "conclusory assurance that its search technique will avoid infecting innocent computers or devices." *Id.* This was because the FBI had not been certain about who had access to

the email address in question, and could not give the magistrate judge assurances that an innocent user with access to that same email account could avoid being subjected to the malware search. *Id.* By contrast, with respect to the Virginia warrant in Mr. Jean's case, the malware protocol would only deploy *after* a registered Playpen user affirmatively accessed the Playpen server in Virginia and logged into the website with a username and password. Accordingly, the NIT protocol for the Virginia warrant made it almost impossible for an innocent user to be subjected to the malware search. [8]

18 It appears that in Mr. Jean's particular case, the malware only deployed after the FBI observed the user named "regalbegal committing a crime in the Eastern District of Virginia by opening a file containing child pornography.

The second reason given by Judge Smith in declining the warrant was because the malware in that case was invasive far more so than the malware used in Mr. Jean's case. The malware in the Texas case was designed to take control of the user's computer's camera and generate photographs of the user, and also generate the latitude and longitude coordinates for the computer's physical location. *Id.* at 756. Judge Smith was concerned that "[i]n between snapping photographs, the Government [would] have real time access to the camera's video feed," which would, in turn, "amount[ ] to video surveillance." *Id.* at 759. This fact alone provided sufficient grounds for him to refuse to authorize the warrant, since the malware protocol failed to meet established Fourth Amendment standards for video camera surveillance. *Id.* at 761.

The third reason advanced by the Texas court in refusing to issue the warrant was that the malware would have collected a great deal of content-specific data from the target's computer. The warrant authorized a 30-day period of monitoring the target's internet activity and authorized the collection of "Internet browser history, search terms, e-mail contents and contacts, 'chat', instant messaging logs, photographs, correspondence, and records of applications run, among other things ...." *Id.* at 760. By contrast, the protocol for the Virginia warrant in Mr. Jean's case identified and returned content-neutral information over the course of approximately 0.27 seconds while the user's computer in Arkansas was actively communicating with (and in the act of downloading child pornography from) the Playpen server in Virginia.

Considering the factual circumstances surrounding the Texas warrant, it comes as no surprise that Judge Smith found the warrant to exceed his authority as set forth in Rule 41(b), primarily because the malware's method of deployment in that case was not sufficiently targeted to those individuals likely to be committing crimes, nor was it reasonably limited in time, place, and manner of search.

Opinions Discussing the NIT Warrant at Issue

Setting aside the *In Re Warrant* case, which is too factually distinguishable to be persuasive of the outcome here, Judge Buchanan's warrant has been the subject of extensive motion practice across the United States and, fortunately for this Court, has been the subject of no less than eleven helpful opinions. In six of those opinions, the courts found that the Virginia warrant was issued in at least technical violation of Rule 41(b) or else assumed without deciding that there was a technical violation and, nonetheless, declined to suppress the evidence. *See United States v. Adams*, 2016 WL 4212079, at *6 (M.D.Fla. Aug. 10, 2016) (opining that the tracking exception under subpart (4) did not apply, as "the NIT does not track; it searches"; but declining to suppress the evidence because the Rule 41 violation was only "a technical or procedural violation"); *United States v. Acevedo Lemus*, 2016 WL 4208436, at *7 (C.D.Cal. Aug. 8, 2016) (observing that "there are credible arguments to be made that Rule 41 was never violated at all," but finding that even if the Rule were violated, there was no justification for suppressing the evidence); *United States v. Werdene*, F.Supp.3d , , 2016 WL 3002376, at *11 (E.D.Pa. May 18, 2016) (refusing to apply the tracking exception because, technically, the defendant's computer was never physically present in the Eastern District of Virginia and so could not be outfitted with a tracking device there; but finding "suppression is not the appropriate remedy") (Doc. 27-9, p. 23); *United States v. Epich*, 2016 WL 953269, at *2 (E.D.Wis. Mar. 14, 2016) (Doc. 27-1, p. 23) (adopting report and recommendation of magistrate judge, *see* Doc. 27-1, and declining to decide whether Rule 41(b) had been violated, as "[s]uppression of the evidence is rarely, if ever, the remedy for a violation of Rule 41, even if such a violation has occurred"); *United States v. Stamper*, No. 1:15 CR 00109, 2016 WL 695660 (S.D.Ohio Feb. 19, 2016) (finding without explaining that "the NIT Warrant technically violates Rule 41(b)," but

concluding that "exclusion is not necessary because there has not been a showing of prejudice or an intentional and deliberate disregard of the Rule") (Doc. 27-4, p. 21); *United States v. Michaud*, 2016 WL 337263, at *6 (W.D.Wash. Jan. 28, 2016) (finding that to apply the tracking exception to the NIT protocol "stretches the rule too far" because the defendant's computer was "unlike a car with a tracking device leaving a particular district" and at no point was ever physically present in the Eastern District of Virginia; but conceding that "the arguments to the contrary are not unreasonable and do not strain credulity") (Doc. 27-3, p. 13).

***15** Only two out of the eleven reviewing courts interpreted Rule 41(b)(4) rigidly and found that a violation occurred, and then went so far as to suppress the evidence collected from the search, due to their opinion that Judge Buchanan's apparent lack of jurisdiction rendered the warrant void *ab initio*. *See United States v. Levin*, 2016 WL 2596010, at *6 (D.Mass. May 5, 2016) (suppressing the evidence after finding that Rule 41(b) had been violated, since the FBI's internet transmittal of malware to the defendant's computer was not analogous to "the installation of a tracking device in a container holding contraband ... regardless of where the 'installation' occurred"); *United States v. Arterbury*, No. 15 CR 182 (N.D.Okla. April 25, 2016) (interpreting Rule 41(b)(4) narrowly and suppressing the evidence as a result, after observing that "[t]he NIT did not track Defendant's computer as it moved," and the warrant "was not for the purpose of installing a device that would permit authorities to track the movements of Defendant or his property") (Doc. 27-8, pp. 16-17).

Finally, in three out of the eleven opinions, two district judges both from the Eastern District of Virginia concluded that the warrant was properly issued under Rule 41(b)(4). Judge Robert G. Doumar first considered a motion to suppress the Playpen warrant in *United States v. Darby*, F.Supp.3d , 2016 WL 3189703 (E.D.Va. June 3, 2016) (Doc. 27-11), and he later applied his reasoning from *Darby* to a different defendant making the identical argument in favor of suppression in *United States v. Eure*, 2016 WL 4059663 (E.D.Va. July 28, 2016). In *Darby*, Judge Doumar opined that the warrant authorized something "exactly analogous" to the installation of a traditional tracking device. F.Supp.3d at , 2016 WL 3189703, at *12. He believed that "[u]sers of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government about their location." *Id.*

In like fashion, Judge Henry Coke Morgan, Jr., in *United States v. Matish*, F.Supp.3d , 2016 WL 3545776 (E.D.Va. June 1, 2016) (Doc. 27-10), analogized that "whenever someone entered Playpen, he or she made 'a virtual trip' via the Internet to Virginia, just as a person logging into a foreign website containing child pornography makes 'a virtual trip' overseas." F.Supp.3d at , 2016 WL 3545776, at *18. Continuing the analogy, "the installation [of a tracking device by the FBI] did not occur on the government-controlled computer but on each individual computer that entered the Eastern District of Virginia when its user logged into Playpen via the Tor network. When the computer left Virginia when the user logged out of Playpen [9] the NIT worked to determine its location, just as traditional tracking devices inform law enforcement of a target's location." *Id.*

19 Judge Morgan's explanation of the technology at issue is spoken in the virtual sense. No "individual computer literally entered and left Virginia, simply because the computer's operator logged into and out of the Playpen server. Instead, a Playpen user would remotely visit the server in Virginia and access images located there. While accessing the images, malware would deploy from Virginia to follow the user's signal back to his computer and identify his IP address.

This Court's Ruling

Citing *Levin* and *Arterbury*, Mr. Jean argues that the NIT here was "installed" outside of Virginia, because the NIT was downloaded onto regalbegal's computer in Arkansas. But such an interpretation of the term "install" sacrifices substance in favor of mere form. Internet crime and surveillance defy traditional notions of place. An individual may commit the crime of knowingly receiving child pornography without ever having visited the physical location of the server containing these images. All acts are committed over the virtual highways of the internet. And while advances in technology always seem to outpace the abilities of rules committees to keep up, [20] that doesn't necessarily mean that the newer techniques

used here were outside the bounds of Rule 41(b), as presently defined.

20 It appears the Judiciary Conference's Committee on Rules of Practice and Procedure must have anticipated that courts might have difficulty reconciling the newly evolving technology of electronic surveillance techniques with the current version of the Federal Rules. The Committee therefore updated Rule 41(b) to keep abreast of advances in technology by submitting an amendment to the Supreme Court in October of 2015. The Court approved the amendment on April 28, 2016, and it is scheduled to take effect on December 1, 2016. The amendment explicitly authorizes magistrate judges to issue warrants that employ remote access techniques to search electronic media, when such media is "concealed through technological means exactly the situation in Mr. Jean's case, where Playpen users were using technological means (TOR software) to conceal their IP addresses. Supreme Court of the United States, http://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf (last visited July 8, 2016). In light of this new Rule amendment, the Court agrees with the Central District of California in *Acevedo Lemus* that " i]t would be strange indeed for the Court to suppress the evidence in this case in the face of a strong signal from the Supreme Court that Rule 41 should explicitly permit the issuance of warrants like the NIT Warrant. 2016 WL 4208436, at *8.

***16** It is true that the FBI was not seeking to install a tangible tracking device to some other physical piece of property, but Rule 41(b)(4) is not constrained or limited to traditional tracking techniques. Applying the definitions in Rule 41(a)(2), a "tracking device" is any "electronic or mechanical device which permits the tracking of the movement of a person or object." [2] And subpart (b)(4) authorizes the tracking of "property," which is specifically defined to include the tracking of mere intangible "information." *See* Rule 41(a)(2)(A). Although the term "device" is not more specifically defined in the Rule, it is a word commonly used to describe "a tool or *technique* used to do a task." *Device*, American Heritage Dictionary, http://www.yourdictionary.com/device#americanheritage (last visited September 12, 2016).

21 Rule 41(a)(2)(E) cross references this definition from 18 U.S.C. § 3117(b).

Here, the government was essentially seeking authority to conduct a sting operation, whereby it would re-launch the Playpen website from its own server in Virginia, after which the FBI would then monitor the flow of electronic information as Playpen users accessed the website for allegedly unlawful purposes. Upon entering this "watering hole," [22] a user while still immersed would become infected with the malware as it was deployed to the user's computer incident to the process of downloading child pornography.

22 The Defendant's expert, Dr. Soghoian, described these types of virtual sting operations as "watering holes, because of the propensity of an illicit website to attract users of such contraband. (Doc. 38, p. 118).

Looking to the express language of the warrant application before Judge Buchanan, it was explained that the purpose of the NIT was to secure proof of "the actual location and identity of the [Playpen] users." (Doc. 19-2, p. 24). When a Playpen user accessed the website's content, the NIT electronically "augment[ed]" that content with "additional computer instructions." *Id.* at p. 25. These instructions caused the user's activating computer to electronically transmit certain identifying information to a computer controlled by the government. *Id.* at p. 26. As explained above, the simplicity of the NIT was that it caused this information to be transmitted back to the government over the regular internet thus circumventing TOR's encryption which in turn allowed the government to track the user's true IP address.

After considering the reasoning set forth above by the various district courts to have considered Judge Buchanan's authority to issue the warrant in question, this Court is persuaded that the investigative technique comports with Rule 41(b)(4)'s tracking exception. First, the NIT is an "electronic device" within the meaning of 18 U.S.C. § 3117(b), because it is an investigative tool consisting of computer code transmitted electronically over the internet. Second, the purpose of the NIT was to track the movement of "property" which in this case consisted of intangible "information," something expressly contemplated by the definition in Rule 41(a)(2)(A).

The third requirement is that the device be "install[ed]" within the issuing district. As reflected in many of the opinions addressing Judge Buchanan's warrant, the term "install" is problematic, primarily because in a more

traditional scenario the tracking of tangible property under Rule 41(b)(4) requires the tracking device to be physically attached within the warrant issuing district. But the investigative technique used here was not designed or intended to track a tangible item of physical property. Rather, the NIT was designed to track the flow of intangible property information something expressly contemplated by Rule 41(a)(2)(A). So when one uses an intangible technique to track the flow of information, to what does the term "install" refer, and where does "installation" take place? Mr. Jean argues that the NIT was downloaded onto his computer, and therefore installation occurred in Arkansas. But that statement isn't entirely correct. While it is obviously true that Mr. Jean and his computer were never physically present in Virginia, it is equally accurate that the warrant did not violate Rule 41(b)(4)'s jurisdictional boundaries, because law enforcement did not leave the Eastern District of Virginia to attach the tracking device used here. [23]

23 Nor, to the best of this Court's understanding, was the NIT actually "downloaded to Mr. Jean's computer in the sense that something remained installed on the computer until deleted. Instead, the NIT consisted of computer code deployed to Mr. Jean's computer. The code "ran on Mr. Jean's computer and "instructed it to execute a command, *i.e.*, to return identifying pieces of information over the regular internet. But the only thing downloaded onto Mr. Jean's computer, in the sense of remaining on the computer after the fact, was the child pornography.

***17** The whole point of seeking authority to use a tracking device is because law enforcement does not know where a crime suspect or evidence of his crime may be located. In such instances, Rule 41(b)(4) allows a magistrate judge to authorize law enforcement's use of electronic tracking tools and techniques. When an unknown crime suspect, or unknown evidence of his crime, is located in an unknown district, it would be nonsensical to interpret the Rule as Mr. Jean does to require law enforcement to make application for such a warrant to an unknown magistrate judge in the unknown district. The fact that the NIT was purposely designed to allow the FBI to electronically trace the activating computer by causing it to return location identifying information from outside the Eastern District of Virginia is not only authorized by Rule 41(b)(4), but is the very purpose intended by the exception.

The warrant application alleged that unknown Playpen users would likely access the website server located in Virginia for purposes of engaging in illegal activity. The application sought authority to track the flow of electronic information while these suspected crimes were occurring. It is undisputed that the NIT authorized by the warrant was executed by the FBI from its computer located within the Eastern District of Virginia. It is also undisputed that *but for* Mr. Jean electronically traveling in search of child pornography to the watering hole in Virginia, the NIT could not have been deployed. Thus, on the facts of this case, the only reasonable interpretation of where the information-tracking NIT was "install[ed]" for purposes of Rule 41(b)(4), is the Eastern District of Virginia, where the tracking device in this case a string of computer code was caused to be executed and deployed. The only alternative reading of the Rule would require a finding that magistrate judges do not currently possess authority to issue information-tracking warrants; but such a reading is squarely contradicted by the plain language of Rule 41(a)(2)(A).

Accordingly, for all of these reasons, this Court finds that Rule 41(b)(4) is applicable, that Judge Buchanan possessed the authority to issue the warrant on that basis, and that the resulting seizure of evidence was not unlawful.

C. Suppression of the Evidence Not Justified Regardless

Even if the Court had agreed with Mr. Jean and found that Judge Buchanan issued the warrant in violation of Rule 41(b)(4), this Court would nevertheless find the violation to be technical in nature, which would not, in any event, justify the suppression of evidence.

1. Fundamental vs. Non-Fundamental Violation

The Court's first step in this analysis is to determine whether the violation of Rule 41(b) assuming such occurred was either "fundamental" and rendered the search unconstitutional under traditional Fourth Amendment standards, or "non-fundamental." *United States v. Freeman*, 897 F.2d 346, 350 (8th Cir.1990). A fundamental violation would require automatic suppression of the evidence, whereas a non-fundamental violation, where no constitutional error occurred, would

not trigger automatic suppression. *Id.* A non-fundamental violation would only justify suppression where there was prejudice to the defendant, "in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed," or if the defendant were able to show that law enforcement and/or the magistrate judge demonstrated an "intentional and deliberate disregard of a provision in the Rule." *Id.*

Here, if there was any violation of the Rule at all, it was certainly non-fundamental. The search warrant was constitutionally sufficient in that it was supported by probable cause and satisfied the particularity requirement. *See supra*, Section II.A.2-3. Another indication that the violation was, if anything, non-fundamental, is the fact that the search warrant could have been authorized by an Article III judge, apparently without incident. The crux of Mr. Jean's Motion to Suppress is the Rule 41(b) violation. His counsel admitted when pressed by the Court during the motion hearing that a district court judge could have authorized the FBI's warrant application. Furthermore, at least two district court judges in the Eastern District of Virginia have stated in written opinions that they found the search warrant to be constitutionally valid and compliant with Rule 41(b)(4)'s tracking-device exception. *See Darby*, F.Supp.3d at , 2016 WL 3189703; *Matish*, F.Supp.3d at , 2016 WL 3545776; *Eure*, 2016 WL 4059663.

***18** If a non-fundamental violation of Rule 41(b) occurs, the suppression of evidence is only justified if a defendant can demonstrate that the search might not have occurred if the Rule had been followed. Mr. Jean argues that he has been prejudiced by the search because it led to his arrest and detainment on federal charges. The Government counters that, by Mr. Jean's logic, every defendant could potentially argue he was prejudiced due to a search, even though the underlying search warrant was constitutionally valid. The Court agrees with the Government that a showing of prejudice must require more than the fact that the defendant would have been better off had the search not been conducted at all. The simple fact to which both parties appear to agree is that an Article III judge in the Eastern District of Virginia could have authorized this particular search warrant. For these reasons, Mr. Jean has not convinced the Court that the extreme remedy of suppression is required due to a showing of prejudice.

Turning to the second possible argument Mr. Jean could make in favor of suppression under the *Freeman* test, he must show that law enforcement and/or the magistrate judge evinced an "intentional and deliberate disregard of a provision in the Rule." 897 F.2d at 350. Initially, the Court notes that Mr. Jean has made no attempt to characterize as improper the magistrate judge's motivations in signing the warrant application. Instead, he suggests that the FBI should have known better than to submit this search warrant to the magistrate judge when she so obviously lacked jurisdiction under Rule 41(b) to authorize the search. However, at the time the FBI presented the search warrant to the magistrate judge, at least a good-faith basis existed to allow the officers to believe that the warrant satisfied Rule 41(b)(4), as this Court and others have now endorsed that particular reading of the Rule. Moreover, the warrant was not facially insufficient, and there is no persuasive argument that the FBI failed to carry out the NIT protocol as per the description in the warrant application. For these reasons, Mr. Jean has failed to demonstrate to the Court's satisfaction that law enforcement evinced an intentional or deliberate disregard of a provision in the Rule. Therefore, suppression of the evidence would not be supported even if a non-fundamental violation of the Rule had occurred.

2. The Good Faith Exception

The parties' final argument in their briefing contemplates whether the good-faith exception to the Exclusionary Rule, as announced by the Supreme Court in *United States v. Leon*, would save the evidence here from suppression if the warrant were found to be invalid. 468 U.S. 897, 922, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). In light of the Court's previous findings, there is no pressing need to reach this argument at all, as the warrant is, in this Court's view, entirely valid. However, since the parties have so thoroughly briefed this issue, the Court will consider it.

The good-faith exception to the Exclusionary Rule provides that when a search warrant is declared invalid, the evidence obtained as a result of the warrant's execution must not be suppressed if law enforcement's reliance on the warrant was objectively reasonable. In the instant case, Mr. Jean does not suggest that the FBI's search of his computer was not in keeping with the warrant application's written description of how the NIT protocol would function. Neither does Mr. Jean directly allege that

Agent Macfarlane's affidavit in support of the warrant was written in such a way as to mislead the magistrate judge about the contents of the Playpen website or the likelihood that users of the site knew in advance the site's content. Mr. Jean does not even maintain that the affidavit's descriptions of TOR's functionality and the way TOR masked users' IP addresses were untrue. It appears instead that Mr. Jean's argument boils down to his belief that it was not objectively reasonable for the FBI to rely on the validity of the data returned by the malware. He argues that the FBI failed to encrypt the connection between his computer and the FBI server during the deployment of the malware, and this might have caused the data to be compromised in some way.

***19** Mr. Jean's argument fails to persuade the Court that law enforcement's reliance on the warrant was objectively unreasonable, and really goes more to the weight of the evidence than to the suppression of the evidence. There is simply no indication that law enforcement suspected the warrant was lacking in probable cause or sufficient particularity, or that agents believed the magistrate judge might lack the jurisdictional authority to authorize the relatively new technology described in the warrant application. Mr. Jean's speculation that hackers could have corrupted the data in transit, or that the FBI's unencrypted connection might have led to some irregularity, does not go to the ultimate question of whether the good-faith exception from *Leon* should apply. The Court therefore finds that, if somehow the warrant were deemed deficient in some respect, the good-faith exception would save the evidence from suppression.

III. CONCLUSION

For the reasons explained herein, the Court finds that Mr. Jean's Motion to Suppress Evidence (Doc. 19) is **DENIED.**

IT IS SO ORDERED on this 13th day of September, 2016.

All Citations

--- F.Supp.3d ----, 2016 WL 4771096

2016 WL 4549108
Only the Westlaw citation is currently available.
United States District Court,
N.D. California.

Unitied States of America, Plaintiff,
v.
Bryan Gilbert Henderson, Defendant.

Case No. 15-cr-00565-WHO-1
|
Signed 09/01/2016

Attorneys and Law Firms

Helen L. Gilbert, U.S. Attorney's Office, San Francisco, CA, for Plaintiff.

Jonathan Daniel McDougall, San Carlos, CA, for Defendant.

ORDER DENYING MOTION TO SUPPRESS NIT WARRANT

WILLIAM H. ORRICK, United States District Judge

INTRODUCTION

***1** On August 24, 2015, Chief Magistrate Judge Joseph C. Spero of the Northern District of California issued a search warrant for the residence located at 1106 E. 16th Avenue, San Mateo, California on information that Bryan Henderson, or an internet user at that residence, had accessed Playpen, a website used to receive and send child pornography. McDougall Decl. Ex. A. ("San Mateo Warrant") (Dkt. No. 56-2). The San Mateo Warrant was based substantially on evidence obtained in execution of a search warrant issued in the Eastern District of Virginia on February 20, 2015 by Magistrate Judge Theresa Carroll Buchanan. McDougall Decl. Ex. B ("NIT Warrant") (Dkt. No. 56-3). FBI agents executed the San Mateo Warrant, during which they seized multiple computers and cell devices from Henderson's residence and interrogated Henderson for several hours. The FBI arrested Henderson on November 3, 3015 based on evidence obtained in that search, which indicated that Henderson was in possession of child pornography. The United States has indicted Henderson for alleged offenses of 18 U.S.C. § 2252(a)(2) and 18 U.S.C. § 2252(a)(4)(b) for receipt and possession of child pornography. Dkt. No. 26.

On June 16, 2016, Henderson filed a motion to suppress the NIT Warrant and all fruits of the Warrant, including all evidence seized or obtained during the execution of the San Mateo Warrant on September 2, 2015. Motion to Suppress ("Mot.") 1 (Dkt. No. 56). Henderson argues that the NIT Warrant was invalid when issued because it violated Federal Rule of Criminal Procedure 41(b), which outlines the geographic limitations of a magistrate judge's authority to issue a warrant, and violated the Federal Magistrates Act, which incorporates Rule 41.

More than a dozen motions to suppress similar NIT Warrants have been decided in federal courts throughout the country. I agree with the majority of courts that the motion should be denied. I conclude that, although the NIT Warrant was invalid under Rule 41(b), suppression is not appropriate because the violation was technical, not constitutional, Henderson was not prejudiced, the FBI did not act with deliberate disregard for Rule 41, and the NIT Warrant was executed in good faith.

BACKGROUND

Playpen is a website dedicated to sharing child pornography that operated on an anonymous network called "Tor." Mot. 6. The Tor network protects user anonymity by allowing computers to access a large number of intermediary users before accessing the target website. *Id.* This masks the location and identity of the user and prevents publicizing the computer's IP address. *Id.* Tor also allows anonymous web hosting which allows users to host a website on the Tor network while preventing the website's location and its user's locations from being identified. *Id.* at 7.

1 There is no evidentiary record in this case. However, the parties do not dispute the facts relevant to this motion.

In 2014, the FBI began an investigation into Playpen. *Id.* In December 2014, the FBI determined that Playpen was hosted on servers located in Lenoir, North Carolina. *Id.*

On February 20, 2015, the FBI executed a warrant and seized the Playpen servers which were then relocated to an FBI facility in Newington, Virginia. *Id.* The same day, the FBI obtained a search warrant authorizing use of a "Network Investigative Technique" ("NIT") that would allow the FBI to search computers accessing the Playpen site for identifying information. NIT Warrant.

***2** The NIT worked by augmenting information exchanged between a user's computer and the Playpen server. A user can only access the site by first entering the Tor network, locating the hidden website hosted on the network, and then entering a username and password. Once a computer completed these steps and accessed the Playpen site (located on servers in Virginia), the NIT would be sent to the activating computer (at the computer's unknown location) and would instruct the activating computer to send identifying information, including the IP address of the computer, back to the Playpen servers in Virginia. *Id.*

Using the NIT, the FBI obtained the IP address associated with Playpen user "askjeff." San Mateo Warrant at 11-12. After conducting an additional investigation, the FBI determined that this IP address likely belonged to Bryan Henderson, located in San Mateo, California. *Id.* The FBI then obtained a search warrant from Judge Spero to search Henderson's San Mateo residence and to seize electronic and computer devices believed to contain evidence that Henderson received and possessed child pornography. *Id.* The FBI executed the San Mateo Warrant and arrested Henderson after it found evidence of child pornography on his electronic devices.

Henderson moves to suppress the NIT Warrant and all fruits of the NIT Warrant, including all evidence seized and obtained on September 2, 2015. He argues that the NIT Warrant was invalid at the time it was issued because it violated Federal Rule 41 and 28 U.S.C. § 636(a) the Federal Magistrates Act which limit the jurisdictional reach of a magistrate judge. Mot. 10. Henderson contends that a magistrate judge's authority is limited to the district in which he or she sits except under specific circumstances, none of which apply to the facts here, and that the NIT Warrant exceeded this limitation because it permitted government agents to conduct a search of computers outside the Eastern District of Virginia. I heard oral argument on August 18, 2016 and granted Henderson leave to submit supplemental briefing on August 26, 2016, which I have now reviewed.

LEGAL STANDARD

Henderson argues that the NIT Warrant is invalid under the Federal Magistrates Act and Rule 41(b) of the Federal Rules of Criminal Procedure. The Federal Magistrates Act, Section 636(a) provides that a magistrate judge shall have within her district and "elsewhere as authorized by law ... all powers and duties conferred or imposed upon the United States commissioners by law or by the Rules of Criminal Procedures for the United States District Courts." 28 U.S.C. § 636(a). Henderson contends that the NIT Warrant violated Section 636(a) by failing to meet the requirements of Rule 41(b). Mot. 14. Therefore, analysis of Henderson's arguments under both sections is identical.

Federal Rule 41(b) outlines the geographical areas over which a magistrate judge has authority to issue warrants:

> (b) 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 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;
>
> ***3** (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 the United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

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

Rule 41 violations fall into two categories: fundamental errors and mere technical errors. *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992). A fundamental error is one resulting in a constitutional violation, requiring suppression. *Id.* A technical error requires suppression only if: (1) the defendant is prejudiced by the error, or (2) there is evidence of deliberate disregard for Rule 41. *Id.*

DISCUSSION

I. WHETHER THE NIT WARRANT VIOLATES RULE 41

Henderson contends that the NIT Warrant was not permissible under any of the five sections of 41(b) because it was issued by a magistrate judge in the Eastern District of Virginia and, through the use of the NIT, permitted searches of Playpen users' computers wherever they were located. Many computers, including Henderson's, were not within the Eastern District of Virginia.

The government argues that the NIT Warrant is valid under Rule 41(b)(1), (2), and (4) because the Playpen servers were located in the Eastern District of Virginia and Playpen users had to virtually reach into the district to access the Playpen site, at which time the NIT was sent and installed on their computers. Opposition ("Oppo.") 15 (Dkt. No. 54). The United States adds that the provisions of Rule 41 are to be read broadly and flexibly where a particular type of search does not fall explicitly under the language of the rule. *Id.* at 14.

I agree with Henderson that the NIT Warrant is not permissible under Rule 41(b)(1) and (2). These sections allow a magistrate judge to issue a warrant to search property located in the district or located in the district at the time the warrant is issued. Neither of these applies as the NIT search occurred outside the district at the location of Henderson's computer in San Mateo, California, which was never located within the Eastern District of Virginia.

There is a stronger argument that the NIT Warrant is permissible under Rule 41(b)(4), which authorizes a magistrate judge "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." Fed. R. Crim. P. 41(b)(4). Two courts have found that the NIT Warrant was permissible under (b)(4), noting that this section is "exactly analogous to what the NIT Warrant authorized" because it allowed the FBI to install a tracking device on the computers of Playpen users which "digitally touched down in the Eastern District of Virginia when they logged into the site." *United States v. Darby*, No. 16-cr-36, 2016 WL 3189703 (E.D. Va. Jun. 3, 2016); *United States v. Matish*, No. 16-cr-16, 2016 WL 3545776 (E.D. Va. Jun. 23, 2016). However, a majority of courts have found that the NIT Warrant does not fit under 41(b)(4) because the users did not have "control" over the government controlled servers at the time they accessed the Playpen site and because the NIT was installed on the activating computers located outside the district. *See e.g.*, *United States v. Michaud*, No. 15-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016); *United States v. Werdene*, No. 15-cr-434, 2016 WL 3002376 (E.D. Penn. May 18, 2016).

***4** This is a close question but I am inclined to agree with the majority of courts that have decided this question. The NIT search does not meet the requirements of 41(b)(4) because, even though it was analogous to a tracking device in some ways, it nevertheless falls outside the meaning of

a "tracking device" as contemplated by the rule. Further, the NIT was installed outside of the district, at the location of the activating computers, not within the district as required by Rule 41(b)(4).

Rule 41 has traditionally been read flexibly. *See United States v. New York Telephone Co.*, 434 U.S. 159, 169 (1977) ("Rule 41 is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause."); *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (concluding that Rule 41(b) authorizes a district court to issue warrants for silent video surveillance although the practice is not specifically covered by statute). However, "[e]ven a flexible application of the Rule [ ] is insufficient to allow the Court to read into it powers possessed by the magistrate that are clearly not contemplated and do not fit into any of the five subsections." *Werdene*, 2016 WL 3002376. The NIT Warrant was invalid under Rule 41(b) because the NIT search was not permissible under any of the five subsections of the Rule.

II. SUPPRESSION IS INAPPROPRIATE

While the NIT search violated Rule 41, suppression is not appropriate because the violation was technical, not constitutional, it did not prejudice Henderson, and the Warrant was executed in good faith.

A Rule 41 violation may be constitutional or technical. *Negrete-Gonzales*, 966 F.2d at 1283. While a constitutional violation must be suppressed, a technical violation should only be suppressed if the search prejudiced the defendant or there is evidence that the government acted with deliberate disregard for Rule 41. *Id.*

A. The NIT Warrant Complies with the Fourth Amendment

The NIT Warrant's violation of Rule 41 is technical because the Warrant complies with the Fourth Amendment requirements of probable cause and particularity. The Fourth Amendment reads in part, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The NIT Warrant was supported by substantial probable cause and evidence that the Playpen website was used to host and exchange child pornography. The courts that have analyzed the NIT Warrant have all found that it was supported by probable cause. *See, e.g.*, *Darby*, 2016 WL 3189703, at *8; *Michaud*, 2016 WL 337263, at *8.

Further, the NIT Warrant meets the Fourth Amendment's particularity requirements. *See United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009) ("Particularity means the warrant must make clear...exactly what it is that he or she is authorized to search for and seize."); *United States v. Turner*, 770 F.2d 1508, 1510 (9th Cir. 1985) ("The place searched must be "described with sufficient particularity to enable the executing officer to locate and identify the premises with reasonable effort."). The NIT Warrant describes the persons and places to be searched in the Warrant's Attachment A, which provides that the NIT will "obtain[ ] information... from the activating computers," that are "those of any user or administrator who logs onto [Playpen] by entering a username and password." NIT Warrant, Attachment A. This description is sufficiently particular because it is limited only to individuals that log onto the Playpen website using a username and password. Because of the structure of the Tor network, only individuals actively attempting to access the Playpen website, with sufficient knowledge of the website and its contents, are able to access it. The Warrant is sufficiently particular as it specifies that the NIT search applies only to computers of users accessing the website, a group that is necessarily actively attempting to access child pornography. *See e.g.*, *Michaud*, 2016 WL 337263 (holding that the NIT Warrant meets the Fourth Amendment's particularity requirements).

B. The NIT Warrant did not Prejudice Henderson

***5** Given that I have concluded that issuance of the NIT Warrant was a technical violation of Rule 41, suppression is only appropriate if the violation causes prejudice to the defendant or if there is evidence of deliberate disregard for the Rule. *Negrete-Gonzales*, 966 F.2d 1283; *see also United States v. Williamson*, 439 F.3d 1125, 1132 (9th Cir. 2006) ("[W]e have repeatedly held and have been instructed by the Supreme Court that suppression is rarely the proper

remedy for a Rule 41 violation."). Neither circumstance exists here.

To determine whether Henderson has been prejudiced, I must consider whether the evidence obtained could have been obtained through other lawful means. *United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980). I conclude that Henderson was not prejudiced because he did not have a reasonable expectation of privacy in the key evidence obtained through the NIT search, his IP address. *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) ("Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing information."). Although the Tor network hides IP addresses, the "Tor network does not strip users of all anonymity" and to access the network users "must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a specific physical location." *Michaud*, 2016 WL 337263, at *7. The FBI was ultimately able to locate Henderson by tracking his IP address to his internet provider, demonstrating that Henderson voluntarily turned his IP address information over to this third party so that it could provide him with web services. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). As Henderson does not have an expectation of privacy in his IP address, the FBI could have legally discovered Henderson's IP address absent the NIT Warrant.

While difficult to locate, the IP address of a Playpen user is public information and Henderson's IP address could have been accessed absent the NIT Warrant. Further, the FBI could have conducted its supplemental investigation of Henderson, using his IP address, to obtain the information sufficient to support the San Mateo Warrant. Because the FBI could have lawfully obtained the information for the San Mateo Warrant through other means, Henderson was not prejudiced by the NIT Warrant.

C. The FBI Did Not Deliberately Disregard Rule 41

Henderson argues that the FBI acted with deliberate disregard for Rule 41 because it knew, prior to requesting the NIT Warrant, that the Warrant was not valid under Rule 41's geographical limitations. Henderson first points to *In re Warrant to Search a Target Computer at Premises Unknown*, in which a court concluded that a different NIT search was not permissible under Rule 41. 958 F. Supp. 2d 753, 758 (S.D. Tex. 2013). While the *In re Warrant* court did find an NIT search impermissible under Rule 41, a single court's decision analyzing a complicated and "novel request" does not definitively demonstrate that the FBI deliberately disregarded the Rule. Indeed, multiple courts have now found that the NIT Warrant is valid under Rule 41. *See Darby*, 2016 WL 3189703, at *12; *Matish*, 2016 WL 3545776, at*18. The FBI could have reasonably believed the NIT Warrant complied with the Rule.

***6** Next, Henderson argues that the FBI deliberately disregarded Rule 41 because on May 5, 2014, the government proposed an amendment to Rule 41(b) that would specifically authorize the type of search conducted by the NIT Warrant and "would authorize a court to issue a warrant to use remote access to search electronic storage media and seize electronically stored information inside or outside of the district: (1) when a suspect has used technology to conceal the location of the media to be searched." Mot. 18. Henderson argues that because it proposed this amendment, the government was well aware that Rule 41(b), as it stands, does not authorize the type of search conducted by the NIT Warrant. The government responds that while it believes Rule 41 authorized the NIT search, it proposed an amendment to the rule to help clarify the ambiguities demonstrated by the varying analyses of the courts that have ruled on the issue.

While I find that the NIT Warrant violated Rule 41(b), the government's position is plausible and does not demonstrate deliberate disregard for Rule 41. As the cases analyzing the NIT Warrant demonstrate, whether the NIT search is permissible under Rule 41 is a close question and the Rule will undoubtedly benefit from clarification. The government's proposed amendment to the Rule demonstrates that it recognized ambiguities in the Rule, not that it acted with deliberate disregard for the Rule.

Because I conclude that Henderson was not prejudiced by the NIT Warrant and the FBI did not deliberately

disregard Rule 41, suppression of the NIT Warrant is not appropriate.

D. The FBI Acted in Good Faith

In addition, suppression is not appropriate in this case because the government acted in good faith. *United States v. Leon*, 468 U.S. 897, 922 (1984) ("objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion."). A warrant is executed in good faith if the warrant is objectively reasonable. *Negrete-Gonzales*, 966 F.2d at 922. Here, the NIT Warrant was objectively reasonable it was supported by substantial probable cause, was sufficiently particular in describing the people and places to be searched, and was issued by a neutral magistrate judge. The good faith exception applies and suppression is not appropriate.

CONCLUSION

Henderson's motion to suppress is DENIED. Although the NIT Warrant was invalid under Rule 41(b), suppression is not appropriate because the warrant meets the Fourth Amendment requirements of probable cause and particularity, the FBI did not deliberately disregard Rule 41, and the FBI acted in good faith in executing the warrant.

IT IS SO ORDERED.

Dated: September 1, 2016.

All Citations

Slip Copy, 2016 WL 4549108

Encryption Workarounds and the Law

Nathan Judish
Computer Crime and Intellectual Property Section
Criminal Division
United States Department of Justice

I. Encrypted Devices

II. Encrypted Communications Channels

Encrypted Communications Channels

- Use of Network Investigative Techniques (NITs)
- Provider assistance provisions

NITs and Remote Searches

- Useful when target uses Tor or other Internet anonymizing technique
- Is a warrant necessary?

Rule 41(b)(6)

- Rule 41(b)(6):
  - Issued in district where activities related to crime may have occurred
  - Authorizes remote access to electronic storage media
  - Available when location of storage media concealed through technological means

Where to Get More Information

- **CCIPS phone number: 202-514-1026**