IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	No. 3:16-CR-35
v.	)	
	)	
THOMAS ALLAN SCARBROUGH,	)	(JORDAN / SHIRLEY)
	)	
Defendant.	)	

REPORT AND RECOMMENDATION

All pretrial motions in this case have been referred to the undersigned pursuant to 28 U.S.C. § 636(b) for disposition or report and recommendation regarding disposition by the District Court as may be appropriate. The charges in this case arise out of a search of the Defendant's home in Rockwood, Tennessee, pursuant to a search warrant. The affidavit supporting the search of the Defendant's residence relies heavily upon information gleaned through the execution of a prior search warrant in the Eastern District of Virginia ("the Virginia warrant"). The Virginia warrant authorized the Federal Bureau of Investigation (FBI) to employ a Network Investigative Technique (NIT) on computers accessing Playpen, a hidden website on the "dark internet," dedicated to the sharing and discussion of child pornography. The NIT attached computer code to Playpen users when they logged onto the website, and that code directed the user's computer to send the user's internet protocol (IP) address and other identifying information to a government computer. The Defendant accessed Playpen using his computer located in the Eastern District of Tennessee during the time that the NIT was active. Through use of the NIT, the FBI learned the Defendant's IP address and, ultimately, obtained a search warrant from the undersigned for the search of his residence.

On April 21, 2016, the Defendant filed a Motion to Suppress [Doc. 14], asking the Court to suppress all evidence seized in the search of his home because the probable cause supporting the search warrant for his residence was based upon the illegal Virginia warrant. The Government responded [Doc. 19] in opposition on May 23, 2016. The Defendant filed a reply [Doc. 20] on June 6, 2016, and the Government filed a Notice of Supplemental Authority in Support of Response to Defendant's Motion to Suppress [Doc. 21] on the following day.

The parties appeared for a hearing on the motion on June 15, 2016. Assistant United States Attorney Matthew T. Morris appeared on behalf of the Government. Attorney Gregory P. Isaacs represented the Defendant, who was also present. The parties presented argument on the issues. The day after the hearing and at the Court's request, the parties provided copies of unpublished case law analyzing the Virginia warrant in question in this case. The Court took the parties' filings, arguments, and the case law under advisement on June 16, 2016. On July 22, 2016, the Government provided additional case law to the Court and defense counsel. The Court has also considered this recent case.

The Court finds that the deployment of the NIT pursuant to the Virginia warrant to the Defendant's computer in the Eastern District of Tennessee violated the Fourth Amendment and Federal Rule of Criminal Procedure 41(b) because the issuing magistrate judge from the Eastern District of Virginia lacked authority to authorize a search of the Defendant's computer, which was located outside the Eastern District of Virginia. However, the Court also finds that the evidence seized pursuant to both the Virginia search warrant and the search of the Defendant's residence should not be excluded because the executing law enforcement officers acted in good faith.

I. POSITIONS OF THE PARTIES

The Defendant is charged [Doc. 3] with one count of distribution of child pornography on October 12, 2015, and one count of possession of child pornography on October 20, 2015. A search warrant for the Defendant's residence was issued on October 15, 2015, and executed on October 20, 2015.

The Defendant asks the Court to suppress all evidence gained in the October 20, 2015 search of his residence. He contends that probable cause for the search of his residence was based on information gathered pursuant to the execution of an invalid search warrant issued in the Eastern District of Virginia. He argues that the Virginia warrant was issued in violation of Federal Rule of Criminal Procedure 41(b) because the magistrate judge in the Eastern District of Virginia did not have jurisdiction to issue a search warrant to employ the NIT to search his computer outside of her district. He argues that he was prejudiced by this violation of Rule 41(b) because without the NIT, law enforcement could not identify him as a user of the Playpen website. He maintains that he was also prejudiced because the FBI acted in deliberate disregard of the jurisdictional requirements of Rule 41(b) by seeking a search warrant in the Eastern District of Virginia. He contends that the instant violation of Rule 41(b) is a substantive violation and, as such, is not subject to the good faith exception to the exclusionary rule. However, he maintains that, even if the Court were to examine the actions of the executing officers in light of the good faith exception, it must find that such exception does not apply in this case because the officers seeking the Virginia warrant deliberately disregarded Rule 41(b) by asking to search outside the Eastern District of Virginia.[1]

[1] In his motion [Doc. 14] and supporting memorandum, the Defendant also argues that the execution of the Virginia warrant violates his rights to privacy, free speech, and freedom of association under the First Amendment. The Government responds [Doc. 19, p.9 n.2] briefly

The Government responds that no Fourth Amendment violation occurred in the execution of the Virginia warrant because the Defendant does not have a legitimate expectation of privacy in his computer's IP address. It argues that the Virginia warrant does not violate Rule 41(b) because the rule does not directly address the situation that the NIT is designed to investigate. However, it asserts that even if the Virginia warrant is deemed to violate the technical aspects of Rule 41(b), it does not violate the spirit of the rule because the officers sought a search warrant from a magistrate judge in the only district with any physical tie to the deployment of the NIT. Finally, the Government argues that the Defendant was not prejudiced by the non-constitutional violation of Rule 41(b) and that the good faith exception overrides technical violations of Rule 41(b), including when a judge issues a warrant outside of his or her authority.

---

that the Defendant does not explain how the Virginia warrant impinged upon his First Amendment rights or what "protected speech" was implicated by the Virginia warrant. The Court also finds the Defendant's First Amendment claim to be general and ill-defined.

Even if the Court were to find that the Playpen website contained some content that enjoyed First Amendment protection, rather than being exclusively a repository for illegal content, the NIT in no way prevented the Defendant from logging on to Playpen, accessing any of the forums (including the ones the Defendant claims are innocuous), or interacting with any other Playpen user while on the website. The Defendant's First Amendment claim is analogous to an argument that the government's investigation and prosecution of a drug dealer wrongfully chills the dealer's ability to speak to and associate with his drug customers regarding matters ancillary to their drug transactions. The First Amendment does not protect speech that is "an integral part of conduct in violation of a valid criminal statute." Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 498 (1949); see also City of Dallas v. Stanglin, 490 U.S. 19, 25 (1989) (holding that "[w]hile it is possible to find some kernel of expression in almost every activity a person undertakes . . . such a kernel is not sufficient to bring the activity within the protection of the First Amendment"). The Court finds that the Defendant's vague First Amendment claim is untenable.

II. SUMMARY OF THE SUPPORTING AFFIDAVITS

On February 20, 2015, United States Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia issued a search warrant [Doc. 19-1] authorizing the search of computers logging onto (by entering a username and password) a certain website, which has since been identified as the Playpen website,[2] through the use of a network investigative technique (NIT). The warrant authorized law enforcement to seize from any such computer the computer's IP address and other identifying information.[3] Probable cause for the issuance of the Virginia warrant is based upon the affidavit of Special FBI Agent Douglas Macfarlane. The Court briefly summarizes the affidavit's description of the Playpen website, the events leading to the deployment of the NIT, and how the NIT operates.

According to Agent Macfarlane, the Playpen website "is dedicated to the advertisement and distribution of child pornography, the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders use to abuse children, as well as methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes[.]" [Doc. 19-1, ¶6] Playpen operates on "The Onion Router" or "Tor" network, which hides the IP address of the user's computer by bouncing communications

[2] The affidavits of both Agent Macfarlane and Agent Norris refer to this website simply as the target website or "Website A," in order to preserve the secrecy of the FBI's investigation. The FBI has now stopped operation of the website, and its name has been released in news articles and, case law, as well as in the Government's response and oral argument.

[3] The Virginia warrant permitted law enforcement to seize the following seven categories of information from any computer logging onto the Playpen website: (1) the computer's IP address and the date and time the NIT determines that IP address, (2) a unique identifier generated by the NIT in order to distinguish data from that computer, (3) the type of operating system on the computer, (4) information on whether the NIT had already been delivered to that computer, (5) the computer's host name, (6) the computer's operating system username, and (7) the computer's media access control. The undersigned finds that these categories of information are designed to assist law enforcement in identifying the computer accessing Playpen and do not relay any "content" from the computer to law enforcement.

among a network of relay computers around the world. When a Tor user logs onto a website, the IP address of the last computer in the relay string (also known as the "exit node"), rather than the user's actual IP address, appears in the website's IP log. Agent Macfarlane states that "[t]here is no practical way to trace the user's actual IP [address] back through that Tor exit node IP [address]." [Doc. 19-1, ¶8] Hidden websites such as Playpen can only be accessed by a Tor user who knows the site's web address and cannot be located through a search. Playpen's address must be learned directly from other users of the website or from other internet postings describing the content available on Playpen and posting its address.

According to Agent Macfarlane's affidavit, when a user accesses Playpen, the opening screen contains images of prepubescent females who are partially clothed with their legs spread apart.[4] Before the user can enter Playpen, the user must register. When the user chooses the registration link, the user receives a message warning the user not to post or enter any real identifying information. Once logged in, the user arrives at an index of the forums available on Playpen. Agent Macfarlane relates that a few forums are devoted to general information on Playpen, with regard to how to post on the site, etc. The remaining forums contained numerous images, videos, and discussions of child pornography and child erotica. Playpen also contains a private messaging feature, which is used to disseminate child pornography; file and image

[4] Other cases analyzing the Virginia search warrant have pointed out that the picture on the opening page changed around the time the search warrant was obtained to a picture of "a young girl with her legs crossed, reclined on a chair, wearing stockings that stop at her upper thigh and a short dress or top that exposes the portion of her upper thigh not covered by the stockings." United States v. Darby, 2:16cr36, Doc. 31, p.4 (E.D. Va. June 3, 2016) [Doc. 21-1, p.4]; United States v. Matish, No. 4:16cr16, 2016 WL 3545776, *4 (E.D. Va June 21, 2016). The instant Defendant does not raise this change to the opening page as an issue in this case. The courts that have grappled with this issue have nevertheless found that the alternative opening page still alerts persons logging in to Playpen that the website contains child pornography. Darby, 2:16cr36, Doc. 31, p.4; Matish, 2016 WL 3545776, *12 (finding no Franks hearing warranted); United States v. Michaud, No. 3:15-cr-05351, 2016 WL 337263, *1 (W.D. Wash. Jan. 28, 2016).

hosting features, which allow users to upload links to videos and images of child pornography and to make them available to other Playpen users; and a chat feature.

Agent Macfarlane's affidavit relates that in December 2014, the FBI obtained a copy of the Playpen website from a server in North Carolina and identified a Florida resident as the administrator of Playpen. The FBI assumed administrative control of Playpen and maintained the copy of Playpen on a computer server at a government facility in the Eastern District of Virginia. The affidavit proposes that law enforcement operate Playpen from the Virginia computer server for thirty days in order to identify administrators and users who log into Playpen with a username and password. The affidavit relates that when a user accesses Playpen, the user's computer downloads content and displays it. The NIT adds instructions to the downloaded content, which direct the computer to send certain identifying information to a government-controlled computer. The affidavit states that the information relayed pursuant to the NIT will aid in identifying the user's computer, its location, and the user him or herself. The affidavit requests that notice of deployment of the NIT on a computer be delayed for thirty days after the user logs onto Playpen.

On October 15, 2016, the undersigned issued a search warrant [Doc. 14-2] for the search of the Defendant's residence in Rockwood, Tennessee. Probable cause for the residential warrant was supplied by the affidavit [Doc. 14-3] of Special FBI Agent Kristina L. Norris. In addition to a description of the Tor network, the Playpen website, and the Virginia warrant, the affidavit relates that during the time that law enforcement maintained Playpen and deployed the NIT, a user with the username "teddybear555" registered an account on Playpen on February 26, 2015, and logged onto Playpen on at least three days for a total of twenty hours on the website. While logged in, teddybear555 visited 806 posts and accessed images of child pornography on

Playpen. Using teddybear555's IP address, obtained via the NIT, law enforcement sent an administrative subpoena to Comcast, which allowed them to identify the Defendant as the account holder assigned to that IP address and to discover his Rockwood, Tennessee address.

III. ANALYSIS

The Fourth Amendment requires that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." U.S. Const. amend. IV. The Defendant asks the Court to suppress evidence seized during the search of his residence because probable cause for the residential search warrant was based upon information seized through an invalid Virginia warrant. He argues that the Virginia warrant is void because the issuing judge lacked authority to issue a search warrant for the search of a computer located outside of her district and that the evidence seized as a result of a void search warrant must be excluded and is not subject to the good faith exception to the exclusionary rule. Additionally, he argues that even if the Court finds no constitutional violation, the evidence must be excluded for a violation of Rule 41(b) because he was prejudiced by the execution of the Virginia warrant which allowed law enforcement to identify him as a user of the Playpen website and, ultimately, to obtain a search warrant for his residence.

The Court first examines whether a violation of either the Fourth Amendment or Rule 41 occurred. Necessary to this analysis is the question of whether the deployment of the NIT is a search implicating the Fourth Amendment. Second, the Court looks at whether the evidence must be excluded as the result of any violation.

A. Fourth Amendment and/or Rule 41 Violation

The Court first explores whether a violation of the Fourth Amendment or of Rule 41(b) of the Federal Rules of Criminal Procedure occurred in this case. The Government argues that no "search" worthy of constitutional or even administrative scrutiny occurred because the Defendant has no legitimate expectation of privacy in his IP address, which is information he readily and necessarily shares with third parties in order to use the Internet. The Defendant argues that a search occurred in this case because he took precautions to keep his IP address hidden while using the Tor network and Playpen.

(1) Reasonable Expectation of Privacy

In order to contest whether a search comports with the Fourth Amendment, the defendant must have "a reasonable expectation of privacy" in the location searched. Rakas v. Illinois, 439 U.S. 128, 143 (1978). Whether an individual has a reasonable expectation of privacy has two aspects: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). "It is well-established that a defendant claiming that a search violated his Fourth Amendment rights has the burden of demonstrating that he had a legitimate expectation of privacy in the place that was searched." United States v. Talley, 275 F.3d 560, 563 (6th Cir. 2001). Whether the defendant enjoys a reasonable expectation of privacy does not turn solely upon the defendant's subjective belief but also depends upon (1) the defendant's interest in and control of the place searched, (2) any measures the defendant took to ensure privacy, and (3) whether society recognizes the defendant's expectation as reasonable. United States v. Padin, 787 F.2d 1071, 1075-76 (6th

Cir.), cert. denied, 479 U.S. 823 (1986). In addition to the reasonable expectation of privacy test, the Supreme Court has recently reaffirmed that the government's intrusion upon the categories enumerated in the Fourth Amendment—"persons, houses, papers, and effects"—may also constitute a search. United States v. Jones, 132 S. Ct. 945, 950-51 (2012) (holding that long-term use of a tracking device without a warrant violates the Fourth Amendment, even though the officers only gleaned information that any third party could observe through physical surveillance).

In the instant case, law enforcement searched the Defendant's computer for his IP address and other identifying information. Three courts considering motions to suppress evidence gained through the application of the instant NIT have questioned whether a search occurred because an individual has no legitimate expectation of privacy in his or her IP address. United States v. Werdene, No. 2:15-cr-00434, Doc. 48, p.2 (E.D. Pa. May 18, 2016) (holding that the "magistrate judge's failure to comply with Rule 41 did not violate Werdene's Fourth Amendment rights because Werdene had no reasonable expectation of privacy in his IP address, and certainly not one society would recognize as reasonable"); United States v. Michaud, No. 3:15-cr-05351, 2016 WL 337263, *7 (W.D. Wash. Jan. 28, 2016); see also United States v. Rivera, No.15-266, Doc. 69, pp.8, 16-17 (E.D. La July 20, 2016) (assuming that use of the NIT is a search but finding that the defendant had no legitimate expectation of privacy in his IP address). The Sixth Circuit has held that "[i]ndividuals generally lose a reasonable expectation of privacy in their information once they reveal it to third parties." Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001). Thus, "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator." Id. This

holding in Guest would seem to dictate a similar result for an IP address, because the Defendant conveyed his IP address to the "entry node" on the Tor, in order to access the Playpen website.

However, in the wake of the Supreme Court's decision in Jones, the Court must also consider the location to be searched, in addition to the nature of the information sought. Although the *information sought*, an IP address, may be information that individuals typically share with third parties in order to use the internet,[5] the *location to be searched*, the Defendant's computer, is one to which Fourth Amendment protections apply. See Riley v. California, 134 S. Ct. 2473, 2492-93 (2014) (holding that accessing the data in a cellular telephone is a search, regardless of the fact that the owner had no expectation of privacy in call records obtained); see also Guest, 255 F.3d at 333 (observing that "[h]ome owners would of course have a reasonable expectation of privacy in their homes and in their belongings—including computers—inside the home; United States v. Levin, No. 15-10271-WGY, 2016 WL 2596010, *5 (D. Mass. May 5, 2016) (amending and superseding Apr. 20, 2016 opinion) (observing that the plain language of the Virginia search warrant states that the locations to be searched are computers accessing the

[5] In her concurring opinion in United States v. Jones, Justice Sotomayor warned:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., Smith[v. Maryland], 442 U.S.[735, 742 (1979)]; United States v. Miller, 425 U.S. 435, 443 . . . (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . . But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Id. at 957 (Sotomayor, J., concurring) (discussing the warrantless monitoring of a tracking device and noting that whether electronic monitoring without physical trespass constitutes a search is a question for another day).

website). The Defendant's computer is one of his "effects" and enjoys the protections of the Fourth Amendment. See United States v. Darby, 2:16cr36, Doc. 31, p.10 (E.D. Va June 3, 2016). Thus, the Court finds that the Defendant can raise a Fourth Amendment challenge to the deployment of the NIT on his computer.

(2) The Fourth Amendment

After finding that a search implicating the Fourth Amendment occurred in this case, the Court next turns to the question of whether the Virginia magistrate judge's issuance of the search warrant to deploy the NIT violates the Fourth Amendment. As set out above, the Fourth Amendment requires law enforcement to have a search warrant, based 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. "Finding these words to be 'precise and clear,' Stanford v. Texas, 379 U.S. 476, 481, . . . (1965), [the Supreme] Court has interpreted them to require only three things[:]" (1) that the warrant be based upon probable cause, (2) that it be sufficiently particular, and (3) that it be issued by a neutral and detached magistrate. Dalia v. United States, 441 U.S. 238, 255 (1979). The Court finds the first of these three requirements was certainly met. The Virginia search warrant was supported by probable cause provided in the sworn affidavit of Agent Macfarlane. See United States v. Epich, No. 15-cr-163, 2016 WL 953269, *2 (E.D. Wis. Mar. 14, 2016) (holding that sufficient probable cause existed to issue Virginia warrant). Moreover, the Defendant does not allege that the Virginia search warrant was not supported by probable cause.

Second, the Court examines whether the Virginia warrant meets the Fourth Amendment's requirement of particularity. The Defendant summarily argues that it does not because the

deployment of the NIT for simply logging into Playpen, rather than for accessing the child pornography forums therein, renders the Virginia warrant too broad to satisfy the Fourth Amendment.

A warrant satisfies the particularity requirement of the Fourth Amendment "if the description is such that the officer with a search warrant can, with reasonable effort, ascertain and identify the place intended." Steele v. United States, 267 U.S. 498, 503 (1925). Here, the Virginia warrant states the location to be searched (through incorporating Attachment A) is "the activating computers," which are defined as "those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password," and the information to be seized (through incorporating Attachment B) is the IP address and other identifying information of the activating computer. [Doc. 19-1, pp.2-4] The undersigned agrees with every court to address the particularity of the Virginia warrant, that an individual logging on to Playpen did so knowing that the website was a repository for child pornography. Darby, 2:16cr36, Doc. 31, at pp.17 (determining that the Virginia warrant is not a "general warrant" and is sufficiently particular); United States v. Matish, No. 4:16cr16, 2016 WL 3545776, *14 (E.D. Va June 21, 2016); Epich, No. 15-cr-163, 2016 WL 953269, at *2; Michaud, 2016 WL 337263, at *5; see also Levin, 2016 WL 2596010, at *8, 15 (declining to reach the particularity issue but observing that other courts have found the Virginia warrant to be sufficiently particular and that "NITs, while raising serious concerns, are legitimate law enforcement tools"). The fact that the Virginia warrant authorized the deployment of the NIT on any number of computers "does not negate particularity because it would be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor network." Michaud, 2016 WL 337263, at *5. Additionally, the fact that a large number of persons could have been snared by the NIT warrant speaks to the nature of the

website, i.e., that it "facilitated rampant criminality[.]" Darby, 2:16cr36, Doc. 31, at pp.17. Thus, the Court finds that the Virginia warrant was sufficiently particular to direct deployment of the NIT to those computers which individuals used in the commission of a crime, that of knowingly accessing child pornography with intent to view it. See 18 U.S.C. § 2252(a)(4)(B).

Third, although the Fourth Amendment does not expressly state who has authority to issue search warrants, the Supreme Court has held that the probable cause finding required by the Fourth Amendment must be made by a neutral and detached magistrate. See Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972); United States v. Pennington, 328 F.3d 215, 217-18 (6th Cir. 2003). The Sixth Circuit has held that integral to being a neutral and detached magistrate capable of making the probable cause determination is the requirement that the individual have the legal authority to issue search warrants. United States v. Scott, 260 F.3d 512, 515 (6th Cir. 2001), abrogated on other gnds by United States v. Masters, 614 F.3d 236 (6th Cir. 2010). In Masters, the appellate court examined the validity of a search warrant issued by a judge in Franklin County, Tennessee, for a residence in Coffee County, Tennessee. Id. at 238-39. The court held that even though state law, rather than federal law, limited a judge's authority to issue search warrants to property in his or her own county, the violation of this state law also violated the Fourth Amendment because the law went to the judge's authority to issue warrants. Id. at 239. Thus, the Master court deemed the search warrant to be "'void *ab initio*,'" because it was signed by one without the legal authority to issue search warrants. Id. (quoting Scott, 260 F.3d at 515).

Similarly, the District of Massachusetts has determined that the same Virginia warrant at issue here was void from the time of its issuance and violated the Fourth Amendment because the magistrate judge from the Eastern District of Virginia lacked authority to issue a search

warrant for computers outside of her district. Levin, 2016 WL 2596010, at *12 (observing that a search warrant that is void from the outset is tantamount to a warrantless search). The undersigned also finds that the Virginia warrant violates the Fourth Amendment because, as explained in full in the next section, it was issued by a judge without the legal authority to do so.

(3) Federal Rule of Criminal Procedure 41(b)

The primary issue raised by the Defendant—whether the magistrate judge from the Eastern District of Virginia had the authority to issue a search warrant to search a computer in the Eastern District of Tennessee—relates to compliance with Federal Rule of Criminal Procedure 41. Congress has authorized federal magistrate judges to issue search warrants in compliance with Rule 41 of the Federal Rules of Criminal Procedure. See 28 U.S.C. § 636(a)(1). Rule 41(b) provides five circumstances in which a magistrate judge has authority to issue a search warrant: (1) To search for and seize a person or property located in the district; (2) to search and seize property located outside the district, if the property was located in the district when the warrant was issued; (3) to seize persons or property in any district related to the investigation of terrorism occurring in the judge's district; (4) to install a tracking device within the district to track a person or property within or outside of the district; or (5) to seize property located in a United States territory or on the premises of a diplomatic or consular mission in a foreign state or at the residence of its personnel for a crime occurring in the judge's district. The Defendant argues that none of these jurisdictional provisions apply and, thus, the magistrate judge from the Eastern District of Virginia lacked authority to issue the Virginia warrant for the search of his computer located in the Eastern District of Tennessee. The Government maintains that while the Virginia warrant may technically violate the letter of Rule 41(b), it conforms to the

spirit of the rule because the Eastern District of Virginia, the district in which the Playpen server was located, was the only district with direct ties to the investigation.

To date, the majority of courts to analyze the instant Virginia warrant have found that it violates Rule 41(b). United States v. Rivera, No.15-266, Doc. 69, pp. 14-15 (E.D. La July 20, 2016); United States v. Werdene, No. 2:15-cr-00434, Doc. 48, pp.13-14 (E.D. Pa. May 18, 2016); United States v. Arterbury, No. 15-cr-182, (N.D. Okla. Apr. 25, 2016); United States v. Levin, No. 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016) (amending and superseding Apr. 20, 2016 opinion); United States v. Stamper, No. 1:15-cr-109, Doc. 48, p.21 (S.D. Ohio Feb. 19, 2016); United States v. Michaud, No. 3:15-cr-05351, 2016 WL 337263, *6 (W.D. Wash. Jan. 28, 2016) (holding that even applying Rule 41(b) flexibly, the Virginia warrant technically violated the rule). But see United States v. Darby, No. 2:16cr36, Doc.31, pp.22-23 (E.D. Va June 3, 2016) (finding NIT is "exactly analogous" to the tracking device in Rule 41(b)(4)); United States v. Matish, No. 4:16cr16, 2016 WL 3545776, *17-18 (E.D. Va June 21, 2016) (holding that Rule 41(b)(4) authorized the magistrate judge to issue the search warrant because the NIT resembles a tracking device); United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, *2 (E.D. Wis. Mar. 14, 2016) (observing without further analysis that magistrate judge found no violation of Rule 41(b) and adopting report and recommendation); see also United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, (D. Neb. Aug. 5, 2016) (finding that a different NIT, deployed from Omaha, Nebraska, where government was hosting an intercepted child pornography website, was analogous to a tracking device under Rule 41(b)(4)).

The undersigned agrees with the majority of courts to analyze the Virginia search warrant that it violates Rule 41(b) because the magistrate judge in the Eastern District of Virginia lacked authority to issue a search warrant to search property located outside of her district. The

Defendant's computer was never located in the Eastern District of Virginia. See Fed. R. Crim. P. 41(b)(1) & (2). Moreover, the FBI was not investigating a crime of terrorism in the Eastern District of Virginia, nor was it attempting to seize property located in a United States territory or foreign state. See Fed. R. Crim. P. 41(b)(3) & (5). The Government argues that Rule 41(b)(4) is persuasive because the NIT is analogous to a tracking device, which was installed on the Defendant's computer when his electronic transmission "touched down" in the Eastern District of Virginia, where Playpen was hosted. However, as observed by the Western District of Washington, applying Rule 41(b)(4) to the Virginia warrant "stretches the rule too far[:]"

> If the "installation" [of the NIT] occurred on the government-controlled computer [hosting Playpen], located in the Eastern District of Virginia, applying the tracking device exception breaks down, because [the defendant] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on [the defendant's] computer, applying the tracking device exception again fails, because [the defendant's] computer was never physically located within the Eastern District of Virginia.

Michaud, 2016 WL 337263, at *6; see also Werdene, No. 2:15-cr-00434, Doc. 48, pp.13 (holding that Rule 41(b)(4) does not apply because the defendant's computer was located outside the Eastern District of Virginia). Moreover, the Eastern District of Louisiana has observed that the NIT did "much more" than simply track the defendant's computer's location. Rivera, No. 15-266, Doc. 69, p.15. The undersigned also finds the analogy to a tracking device to fall short.

The Government maintains that the FBI followed the spirit of Rule 41(b) by obtaining a search warrant in the only district with any physical tie to the case. It contends that the Eastern District of Virginia was the only location that the FBI could have obtained a search warrant because the Playpen website was hosted on a government server there. However, as pointed out by the district judge in Levin, the argument that the magistrate judge in the jurisdiction with the

closest connection to the search should be able to issue the search warrant adds words to Rule 41(b). 2016 WL 2596010, at *6. When the language of a statute is clear, "it would be improper to conclude that what Congress omitted from the statute is nevertheless within its scope." University of Texas Sw. Med. Ctr v. Nassar, 133 S. Ct. 2517, 2528 (2013). The same is true for a rule of criminal procedure. Moreover, law enforcement is not without recourse in situations in which the location of the computer is unknown. First, an amendment to Rule 41(b) to permit magistrate judges to issue warrants to search property outside of their districts in circumstances similar to the instant case is presently under consideration. Levin, 2016 WL 2596010, at *8 n. 13 & *14. Second, Rule 41(b) does not limit the authority of district judges to issue search warrants for the search of property outside of their district. Id. at *14.

The undersigned finds that the Virginia search warrant violates both Rule 41(b) and the Fourth Amendment. This, however, is not the end of the inquiry. The Court next turns to the question of whether the Defendant's IP address and other identifying information, gained through the execution of the Virginia warrant, must be suppressed.

B. Exclusion of Evidence

The Defendant argues that the violation of Rule 41(b) is a substantive, rather than procedural or technical violation, which requires the suppression of the evidence gained from the deployment of the NIT on his computer and all evidence flowing therefrom. He maintains that the issuance of the Virginia warrant by a magistrate judge without authority rendered the Virginia warrant void *ab initio*. Accordingly, because the Virginia warrant was void from its inception, the deployment of the NIT on his computer was a warrantless search. Alternatively, the Defendant argues that, even if the Court finds the Rule 41(b) violation is technical, he was

prejudiced by the violation in that the search of his computer would not have occurred in the absence of the violation. Moreover, he contends that the FBI deliberately disregarded the limitations of Rule 41(b) in seeking the issuance of a search warrant in the Eastern District of Virginia to search computers located anywhere in the country. Thus, the Defendant contends that the fruits of the illegal search must be excluded and that the good faith exception to the warrant requirement does not apply.

The Government responds that the Defendant has raised no constitutional violation, that he was not prejudiced by a technical violation of Rule 41, and that, in any event, law enforcement acted in good faith in seeking a search warrant from a judge in the sole district with a connection to the investigation of the website. The Court first examines whether the evidence should be suppressed due to the Fourth Amendment violation and second whether the Rule 41(b) violation requires the suppression of the evidence.

(1) Exclusion for Fourth Amendment Violation

The Defendant argues that the Virginia warrant was void from the time it was issued, because the magistrate judge from the Eastern District of Virginia lacked authority to issue the Virginia warrant. The Defendant contends, as the District of Massachusetts held in Levin, that "a warrant that was void at the outset is akin to no warrant at all[.]" 2016 WL 2596010, at *12. Because his IP address and other identifying information was seized in a warrantless search, the Defendant argues that this information must be suppressed. He argues that the good faith exception to the exclusionary rule does not apply because the Virginia warrant is void.

As discussed above, the undersigned agrees that the Virginia warrant is void because it was issued by a judge without authority. Our appellate court has held that "'when a warrant is

signed by someone who lacks the legal authority necessary to issue search warrants, the warrant is void *ab initio*.'" United States v. Master, 614 F.3d 236, 241 (6th Cir. 2010) (quoting United States v. Scott, 260 F.3d 512, 515 (6th Cir. 2001), abrogated in part by Master). However, the undersigned must part company with the holding in Levin with regard to the application of the exclusionary rule to void warrants. The Sixth Circuit *previously* held, as does the court in Levin, that the good faith exception to the exclusionary rule did not apply to warrants issued by a judge lacking authority. Scott, 260 F.3d at 515. However, in Master, the Sixth Circuit modified its prior holding in Scott, concluding that this position is no longer "viable in light of more recent Supreme Court cases" and changing the approach for the exclusion of evidence. Master, 614 F.3d at 242 (citing Herring v. United States, 555 U.S. 135 (2009) & Hudson v. Michigan, 547 U.S. 586 (2006)).

In Herring, the Supreme Court turned from an analysis of whether law enforcement's actions fell within the narrow "good faith" exception to the exclusionary rule to a broader cost-benefit analysis of whether the exclusion of evidence will deter future Fourth Amendment violations. 555 U.S. at 141; Master, 614 F.3d at 242. Observing that the Supreme Court stressed that the exclusionary rule is designed to "'curb police misconduct rather than judicial misconduct[,]'" the Sixth Circuit reasoned that "[a]rguably, the issuing magistrate's lack of authority has no impact on police misconduct, if the officers mistakenly, but inadvertently, presented the warrant to an incorrect magistrate." Id. (quoting Herring, 555 U.S. at 142). Thus, the Sixth Circuit concluded that suppression of evidence seized pursuant to a void warrant should no longer be automatic:

> The Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violation, "the benefits of deterrence must outweigh the costs." Herring, [555

> U.S. at 141]. In following the Supreme Court's approach with respect to the instant case, the costs of excluding the evidence would appear to outweigh any deterrent effect. This is so, in no small measure, because the Herring Court's emphasis seems weighed more toward preserving evidence for use in obtaining convictions, even if illegally seized, than toward excluding evidence in order to deter police misconduct unless the officers engage in "deliberate, reckless, or grossly negligent conduct." Id. at [144].

Master, 614 F.3d at 243 (remanding to district judge for additional fact finding regarding the officers' conduct). Although the instant Defendant argues that Scott and Levin apply the better rule, the undersigned is bound to follow current Sixth Circuit precedent, i.e. the Master case. See id.

The Court looks to the totality of the circumstances, outlined above, in weighing the benefits of deterrence against the cost to society in excluding the evidence. Here, the "deterrent value" to law enforcement of excluding the evidence is low. First, the Court observes that the FBI agents sought a search warrant in order to deploy the NIT, despite the fact that they were seeking information that the users of the Playpen website had already disclosed to third parties in order to access the website. Case law recognizes a "strong preference for warrants" because "a search warrant 'provides the detached scrutiny of a neutral magistrate, which is a more reliable safeguard against improper searches than the hurried judgment of a law enforcement officer "engaged in the often competitive enterprise of ferreting out crime[.]"'" United States v. Leon, 468 U.S. 897, 913-14 (1984) (quoting United States v. Chadwick, 433 U.S. 1, 9 (1977) (in turn, quoting Johnson v. United States, 333 U.S. 10, 14 (1948))). Additionally, the Court finds that the Virginia warrant was limited in the length of time that the NIT would be deployed and the type of information the NIT could return, which was only identifying information that users of Playpen disclosed to third parties to access the website. Thus, not only did the FBI seek a search

warrant in order to deploy the NIT, it did not seek to search the activating computers for child pornography but, instead, asked to search them only for identifying information.

Second, the Court finds that Agent Macfarlane disclosed all of the facts necessary for the magistrate judge in the Eastern District of Virginia to make a probable cause determination and to determine whether she had the authority to issue the warrant. The FBI fully disclosed to the magistrate judge the nature and content of the website, how the NIT functioned, and that the officers sought to learn the IP address and other identifying information from "activating computers . . . wherever located." The agent disclosed all the relevant information to the magistrate judge, and "[t]here was indeed nothing more [Agent Macfarlane] 'could have or should have done under these circumstances to be sure his search would be legal.'" United States v. McClain, 444 F.3d 556, 566 (6th Cir. 2005) (quoting United States v. Thomas, 757 F.2d 1359, 1368 (2d Cir. 1985) (declining to suppress evidence because the officers acted in good faith in presenting all information to the judge)).

The Defendant argues that the FBI intentionally or deliberately disregarded Rule 41(b) in seeking the Virginia warrant, because it was clear that the NIT did not fall within the plain language of the rule. However, as the Government points out, the FBI sought the search warrant in the district with the only "physical" connection to these ongoing crimes, which was the Eastern District of Virginia where the Playpen website was hosted on a government server. The Court finds that it was not clear to a law enforcement officer that the magistrate judge in the Eastern District of Virginia lacked authority, particularly when that magistrate judge found that she had authority to issue the warrant. Of the nine cases to address whether the magistrate judge from the Eastern District of Virginia had the authority to issue the instant NIT warrant, one-third of the judges have concluded that no Rule 41(b) violation occurred. Darby, No. 2:16cr36, Doc.

31, pp.22-23; Matish, 2016 WL 3545776, at *17-18; Epich, 2016 WL 953269, at *2. Thus, reasonable minds—even reasonable legal minds—differ as to whether the Virginia magistrate judge had authority under Rule 41(b) to issue the NIT warrant. When the error rendering the search warrant invalid rests with the judge's determination, rather than the law enforcement officer's conduct, the exclusionary rule loses its deterrent value. Davis v. United States, 564 U.S. 229, 238 (2011); see also Leon, 468 U.S. at 917 (providing that "exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates").

Turning to the other side of the balancing test, the Court finds that the cost to society of excluding the evidence gained through the execution of the Virginia warrant is high. "Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment." Davis, 564 U.S. at 237 (internal citations omitted). Under the present circumstances surrounding the deployment of the NIT, individuals accessing the Playpen website were victimizing the most vulnerable members of society, children, and were using the anonymizing technology of the Tor to evade detection. As observed by the Eastern District of Pennsylvania in Werdene, "[t]he 'cost' of suppression . . . would be letting a 'guilty and possibly dangerous defendant [] go free—something that "offends basic concepts of the criminal justice system."'" No. 2:15-cr-434, Doc. 33, p. 33 (quoting Herring, 555 U.S. at 171 (in turn quoting United States v. Leon, 468 U.S. 897, 908 (1984)). Here, the Court finds that the balance weighs against the application of the exclusionary rule.

(2) Exclusion based on Rule 41(b) Violation

Alternatively, the Defendant argues that the evidence gained through the deployment of the NIT on his computer must be suppressed because he was prejudiced by the Rule 41(b) violation in this case. "'[V]iolations of Rule 41 alone should not lead to exclusion unless (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. Searp, 586 F.2d 1117, 1125 (6th Cir. 1978) (quoting United States v. Burke, 517 F.2d 377, 386-87 (2d Cir.1975)), cert. denied, 440 U.S. 921 (1979); see also Frisby v. United States, 79 F.3d 29, 32 (6th Cir. 1996) (holding that "ministerial" violations of Rule 41, such as the failure to leave a copy of the warrant and a receipt for the property seized, do not require application of the exclusionary rule unless the defendant can show prejudice resulting from the violation). In the instant case, the Defendant argues that he suffered prejudice because the search of his computer never would have occurred if the Virginia magistrate judge had declined to issue the NIT warrant. He argues that Agent Macfarlane's affidavit relates that the use of the Tor browser makes it virtually impossible to identify the IP address of individuals logging onto the Playpen website without using the NIT. The Government argues that like an unlisted telephone number, the Defendant's IP address was difficult, but not impossible, for law enforcement to trace in the absence of the NIT.

Based upon the record before the Court, which is limited to those facts contained in Agent Macfarlane's affidavit, the Court finds the Defendant suffered prejudice from the Rule 41(b) violation. Agent Macfarlane relates that "[w]hen a user on the Tor network accesses a website, for example, the IP address of the Tor 'exit node,' rather than the user's actual IP address, shows up in the website's IP log. . . . . There is no practical way to trace the user's

actual IP back through that Tor exit node IP." [Doc. 19-1, ¶8] He also relates that the website's log of user activity will contain the IP addresses of the exit nodes and that, "[g]enerally, those IP addresses cannot be used to locate and identify the administrators and users of the" website. [Doc. 19-1, ¶29] Agent Macfarlane states that use of a NIT "is necessary in order to locate and apprehend" individuals using the Playpen website. [Doc. 19-1, ¶30] Based upon these statements in Agent Macfarlane's affidavit, the Court finds that the identification of the Defendant's IP address likely would not have occurred without the deployment of the NIT. Thus, the Court finds that the Defendant was prejudiced by the Rule 41(b) violation in this case because, in the absence of the issuance of the Virginia warrant, the identification of the Defendant as a Playpen user and the subsequent search of the Defendant's home and computer pursuant to the separate search warrant issued in this district would not have occurred.

However, even though the Defendant was prejudiced by the Rule 41(b) violation in this case, the application of the exclusionary rule is not automatic. Instead, the Court applies the balancing test set forth by the Supreme Court in Herring and applied by the Sixth Circuit in Master. Herring, 555 U.S. at 141; Master, 614 F.3d at 242. As discussed above in relation to the Fourth Amendment violation, the Court has applied the Herring/Master balancing test to the instant case and finds that the FBI agents seeking and executing the Virginia warrant acted in good faith. Accordingly, the evidence seized in the execution of the Virginia search warrant should not be suppressed.

(3) The Tennessee Warrant

Finally, the Defendant argues that the evidence seized pursuant to the Tennessee warrant must be suppressed as the fruit of the poisonous tree because the affidavit supporting the

issuance of the Tennessee search warrant was based upon the evidence gained during the execution of the invalid Virginia search warrant. The undersigned has already found that the evidence seized pursuant to the Virginia warrant should not be suppressed based upon the good faith of the executing officers. The Court additionally finds that, based upon the good faith of the officers seeking and executing the Tennessee warrant, the evidence seized in the execution of the Tennessee warrant is not the fruit of the poisonous tree.

The "fruit of the poisonous tree doctrine" excludes not only that evidence that was illegally seized, but all evidence gained from the "'exploitation'" of an illegal search or seizure unless that evidence is sufficiently attenuated from the illegal actions as to "'purge[it] of the primary taint.'" Wong Sun v. United States, 371 U.S. 471, 488 (1963) (citing Maguire, Evidence of Guilt, 221 (1959)). In United States v. McCain, the Sixth Circuit analyzed the intersection of the fruit of the poisonous tree doctrine and the good faith exception to the exclusionary rule, in a case in which information related in an affidavit supporting a search warrant was gained through a Fourth Amendment violation, there a warrantless entry into a residence. 444 F.3d 556, 564-66 (2005). The appellate court observed that traditionally,

> [t]he exclusionary rule . . . work[s] to exclude all evidence obtained subsequent to and as a consequence of an illegal search because, as the fruit of a prior illegality, such evidence is tainted unless (1) the government learns of the evidence from an "independent source," Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 . . . (1920); (2) the connection with the unlawful search becomes "so attenuated as to dissipate the taint," Nardone [v. United States], 308 U.S. [338,] 341 . . . [(1939)]; or (3) the evidence "would inevitably have been discovered." Nix v. Williams, 467 U.S. 431, 444 . . . (1984).

Id. at 564. As in McCain, none of these three "exceptions" to the fruit of the poisonous tree doctrine appears to apply in the instant case. See id. The FBI did not learn the identity or home address of Playpen user "teddybear555" through an independent source. The connection

between the Virginia warrant and the Tennessee warrant is not attenuated. In fact, the Tennessee warrant is based primarily upon information related in or gained from the execution of the Virginia warrant. Finally, although the Government argues that the Defendant's IP address, like an unlisted phone number, was discoverable, the record is devoid of any information that the Defendant's IP address and, subsequently, his home address, would have been discovered without the deployment of the NIT.

However, the court in McCain held that the Leon good faith exception could also apply to evidence gained in the execution of a search warrant, which itself was the fruit of a Fourth Amendment violation. Id. at 565. The Sixth Circuit held that the officer seeking the subsequent search warrant acted in good faith when "the facts surrounding the initial Fourth Amendment violation were 'close enough to the line of validity to make the officer's belief in the validity of the warrant objectively reasonable.'" Id. at 566 (quoting United States v. White, 890 F.2d 1413, 1419 (8th Cir. 1989)). Applying this standard to the facts of that case, the court observed that while the initial warrantless search of McCain's home was not justified by exigent circumstances, the officers entering the home were not "objectively unreasonable" in their belief that criminal activity was afoot, nor did they know their actions violated the Fourth Amendment. Id. "More importantly, the officers who sought and executed the search warrants were not the same officers who performed the initial warrantless search, and [their search] warrant affidavit fully disclosed to a neutral and detached magistrate the circumstances surrounding the initial warrantless search." Id.

Likewise, the Court finds that, in the instant case, the FBI was not "objectively unreasonable" in executing the Virginia warrant and deploying the NIT onto the Defendant's computer. As discussed herein, the Virginia warrant was based upon probable cause, was

sufficiently particular, and was issued by a magistrate judge in the only district with a physical tie to the ongoing crimes on the Playpen website. The matter of whether that magistrate judge had authority to issue the warrant remains the subject of legal analysis for judges across the country. More importantly, Agent Norris, who sought and executed the Tennessee warrant, was not involved in seeking the Virginia warrant or deploying the NIT and had no reason to doubt the validity of the Virginia warrant. In her affidavit, Agent Norris fully disclosed to the undersigned the circumstances surrounding the Virginia warrant. Moreover, at the time the undersigned issued the search warrant for the Defendant's residence, no court had determined that the underlying Virginia warrant violated the Fourth Amendment or Rule 41(b). Accordingly, the Court finds that the evidence seized in the execution of the Tennessee warrant should not be suppressed pursuant to the fruit of the poisonous tree doctrine.

IV. CONCLUSION

After carefully considering the parties' filings and arguments and the relevant legal authorities, the Court finds that although the Virginia warrant was issued in violation of the Fourth Amendment and Federal Rule of Criminal Procedure 41(b), the FBI acted in good faith in seeking the Virginia warrant and, thus, the evidence gleaned from the deployment of the NIT on the Defendant's computer, i.e., the Defendant's IP address and other identifying information, should not be suppressed. Additionally, the Court finds that the subsequent search warrant for the Defendant's residence was not tainted by the Fourth Amendment and Rule 41(b) violations in the Virginia warrant and, thus, the evidence seized in the execution of the search warrant for the

Defendant's residence is likewise not subject to suppression. For the reasons set forth herein, it is **RECOMMENDED** that Defendant's Motion to Suppress [Doc. 14] be **DENIED**.[6]

Respectfully submitted,

s/ C. Clifford Shirley, Jr.
United States Magistrate Judge

[6] Any objections to this report and recommendation must be served and filed within fourteen (14) days after service of a copy of this recommended disposition on the objecting party. Fed. R. Crim. P. 59(b)(2) (as amended). Failure to file objections within the time specified waives the right to review by the District Court. Fed. R. Crim. P. 59(b)(2); see United States v. Branch, 537 F.3d 582, 587 (6th. Cir. 2008); see also Thomas v. Arn, 474 U.S. 140, 155 (1985) (providing that failure to file objections in compliance with the required time period waives the right to appeal the District Court's order). The District Court need not provide de novo review where objections to this report and recommendation are frivolous, conclusive, or general. Mira v. Marshall, 806 F.2d 636, 637 (6th Cir. 1986). Only specific objections are reserved for appellate review. Smith v. Detroit Federation of Teachers, 829 F.2d 1370, 1373 (6th Cir. 1987).