UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,	*	
	*	
v.	*	
	*	
RICHARD ALLAIN,	*	Criminal No. 15-cr-10251
	*	
Defendant.	*	
	*	

MEMORANDUM AND ORDER

September 29, 2016

BURROUGHS, D.J.

I. Introduction

On September 3, 2015, a grand jury returned a three-count indictment against Defendant Richard Allain ("Allain"). The indictment charged Allain with one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), and two counts of receipt of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and (b)(1). Currently pending are Allain's Motion to Suppress [ECF No. 60] and Motion to Dismiss Count II of the Indictment [ECF No. 62]. Both of the pending motions relate to the FBI's 2015 investigation into "Playpen," a website that facilitated the distribution of child pornography.

In early 2015, after a foreign law enforcement agency informed the FBI that it suspected a United States-based IP address was being used to run Playpen, the FBI seized a copy of the server hosting the site. Rather than immediately shut down Playpen, the FBI continued to operate it for two weeks, in order to identify users of the site. Because Playpen operated on the "Tor" network—a network designed to maintain a user's anonymity—the FBI could not easily identify Playpen users, even after it had seized control of the website. To advance its investigation, the

FBI obtained a search warrant (the "NIT Warrant") authorizing it to deploy a "Network Investigative Technique" ("NIT") onto any computers used to log into Playpen. By installing the NIT onto Playpen users' computers, the FBI could identify the IP addresses, and eventually the individuals, that logged into the site. The NIT Warrant has already been subject to significant judicial scrutiny across the country. A majority of courts have found that the magistrate judge who issued the NIT Warrant lacked authority to do so, yet declined to suppress evidence. See, e.g., United States v. Ammons, No. 3:16-CR-00011-TBR-DW, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016); United States v. Henderson, No. 15-CR-00565-WHO-1, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). A minority of courts have suppressed evidence based on a finding that the warrant was void and the good-faith exception to the exclusionary rule did not apply. See, e.g., United States v. Levin, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016); United States v. Croghan, No. 1:15-CR-48, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016).[1]

[1] Additionally, two judges in the Eastern District of Virginia have found, in three separate cases, that the magistrate judge had the authority to issue the warrant within her own district. Because it is clear that the magistrate judge had the authority to issue a warrant or authorize a tracking device in her own district, those cases are factually distinct and therefore not relevant to the analysis in this case. See United States v. Darby, No. 2:16CR36, 2016 WL 3189703, at *12 (E.D. Va. June 3, 2016) (Doumar, J.) (finding that the NIT was a tracking device, which Fed. R. Crim. Pro. 41(b)(4) permits a magistrate to authorize to be installed within her district); United States v. Eure, No. 2:16CR43, 2016 WL 4059663, at *8 (E.D. Va. July 28, 2016) (Doumar, J.) (same); United States v. Matish, No. 4:16CR16, 2016 WL 3545776, at *17-18 (E.D. Va. June 23, 2016) (Morgan, J.) (same).

On or about February 27, 2015, after Allain logged into Playpen, the NIT was installed onto his computer, located in Framingham, Massachusetts. The information gathered by the FBI from Allain's computer forms the basis of Count 2 of the Indictment. [ECF No. 17].[2]

On April 27, 2016, Allain filed his Motion to Suppress, in which he moves for an order suppressing all evidence obtained by the government using the NIT Warrant. [ECF No. 60]. Allain raises five independent grounds for suppressing the evidence. He contends that the NIT Warrant was: (1) not supported by probable cause; (2) issued only after the FBI intentionally and recklessly misled the issuing court; (3) an impermissible general warrant; (4) contingent on a "triggering event" that did not occur; and (5) void ab initio, since the issuing magistrate judge did not have authority to issue it. In his Motion to Dismiss Count II of the Indictment, also filed on April 27, 2016, Allain claims that by continuing to operate Playpen during its investigation, and therefore briefly facilitating the distribution of child pornography, the government engaged in outrageous misconduct that warrants dismissal of the resulting charge. [ECF No. 62]. The government filed separate oppositions to the two motions on June 17, 2016 [ECF Nos. 69, 70], and the Court heard oral argument on July 18, 2016. [ECF No. 76]. After oral argument, the government filed three addendums to its response to Defendant's Motion to Suppress [ECF Nos. 74, 77, 79], the second of which the Defendant has moved to strike. [ECF No. 78]. In addition, the Defendant filed a supplemental memorandum in support of his Motion to Dismiss [ECF No. 82], and a supplemental memorandum in support of his Motion to Suppress [ECF No. 83].

For the reasons stated herein, both motions are hereby DENIED.

[2] Allain's computer was seized by the Framingham Police Department on June 9, 2015 as the result of a state court search warrant issued in connection with a separate investigation of Allain. Forensic analysis identified child pornography on the computer, which is the basis of the possession of child pornography charge in Count 1 of the Indictment.

II. The Warrant and Relevant Factual Background

a. Playpen

On February 20, 2015, FBI Special Agent Douglas Macfarlane filed an application for a search warrant in the Eastern District of Virginia. [ECF No. 61-2 (the "Warrant Application")].[3] The subject of that warrant was "Playpen," a website "dedicated to the advertisement and distribution of child pornography" and "the discussion of matters pertinent to child sexual abuse." Playpen operated on the Tor network. Typically, visitors to a public website can be identified by their IP address, but on the Tor network, IP addresses are masked, thus enabling users to access websites anonymously. To access the Tor network, a user must install Tor software either by downloading an add-on to their web browser or by downloading the free "Tor browser bundle." Id. ¶ 7.

Further, Playpen operated as a "hidden service" within the Tor network. Id. ¶ 6. Hidden websites within Tor operate the same as other public websites except that the IP address for the web server is hidden and replaced with a Tor-based web address, which is a series of sixteen algorithm-generated characters followed by the suffix ".onion." Thus, at the time the Warrant Application was submitted, the web address for Playpen was upf45jv3bziuctml.onion. Id. As described in the Warrant Application, "[a] user can only reach these 'hidden services' if the user is using the Tor client and operating the Tor network." Id. ¶ 9. "Even after connecting to the Tor network . . . a user must know the web address of the website in order to access the site." Id. ¶ 10. Because Playpen was a hidden website on the Tor network, users had to take many

[3] The following information concerning Playpen is largely taken from Special Agent Macfarlane's affidavit in support of the application. These facts to do not seem to be disputed, unless otherwise noted herein.

affirmative steps to locate the site, making it "extremely unlikely that any user could simply stumble upon [Playpen] without understanding its purpose and content." Id. ¶ 10.

Even after locating Playpen, its content was only accessible to users who registered a username and then logged into the site. Upon arriving at the Playpen homepage, a user was prompted to either register an account or login using a pre-existing username and password. In order to register an account, users were required to accept Playpen's registration terms, which stated, among other things, that "the forum operators do NOT want you to enter a real [e-mail] address," "[users] should not post information [in their profile] that can be used to identify you," "it is impossible for the staff or the owners of this forum to confirm the true identity of users," "[t]his website is not able to see your IP," and "[f]or your own security when browsing . . . we also recomend [sic] that you turn off javascript and disable sending of the 'referer' header." Id. ¶ 13.

Once logged into Playpen, users had complete access to all of Playpen's sections, forums, and sub-forums, where they could upload material and view material uploaded by others. The Warrant Application included a listing of the sections, forums, and sub-forums on Playpen, along with the corresponding number of topics and posts in each, which Special Agent Macfarlane observed upon accessing the site. Based on his review of Playpen's different forums, Special Agent Macfarlane concluded that the "the majority contained discussions, as well as numerous images that appeared to depict child pornography ('CP') and child erotica of prepubescent females, males, and toddlers." Id. ¶ 18. The FBI's review of Playpen revealed links to numerous depictions of what appeared to be child pornography. This included:

> • An image of a prepubescent or early pubescent female being orally penetrated by the penis of a naked male. [ECF No.61-2 ¶ 18].

> • A video of a prepubescent female, naked from the waist down, being anally penetrated by the penis of a naked adult male. Id. ¶ 18.
>
> • Images focused on the nude genitals of a prepubescent female. Id. ¶ 23.
>
> • A video of an adult male masturbating and ejaculating into the mouth of a nude prepubescent female. Id. ¶ 24.
>
> • An image of two prepubescent females lying on a bed with their genitals exposed. Id. ¶ 25.
>
> • An image of four females, including at least two prepubescent females, performing oral sex on one another. Id. ¶ 25.

In addition, according to the Warrant Application, Playpen contained certain features, such as private messaging and image hosting, that facilitated the distribution of child pornography. Id. ¶¶ 22-25.

b. The NIT Warrant

In the Warrant Application, Special Agent Macfarlane stated that there was "probable cause to believe there exists evidence, fruits, and instrumentalities of criminal activity related to the sexual exploitation of children on computers that access [Playpen], in violation of 18 U. S.C. §§ 2251 and 2252A," and that the search authorized by the NIT Warrant would help the FBI to identify the computers used to log into Playpen, the locations of the computers, and the users of the computers. [ECF No. 61-2 ¶ 48].

The NIT Warrant authorized the FBI to deploy the NIT onto any "activating" computer, defined as the computer "of any user or administrator who logs into [Playpen] by entering a username and password." Id., Att. A. When deployed, the NIT would cause the user's computer to send the following information back to a government-controlled computer in the Eastern District of Virginia:

> 1) the 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 to distinguish data from that of other computers;
>
> 3) the type of operating system running on the computer;
>
> 4) information about whether the NIT has already been delivered to the "activating" computer;
>
> 5) the computer's Host Name;
>
> 6) the computer's active operating system username; and
>
> 7) the computer's media access control ("MAC") address.

Id. at Att. B. The NIT Warrant was issued on February 20, 2015 by Theresa Carroll Buchanan, a United States Magistrate Judge for the Eastern District of Virginia.

Between the time the Warrant Application was drafted and the NIT Warrant was issued, the appearance of Playpen's homepage changed. The homepage was the only page visible on the Playpen site until a user entered log-on credentials. Due to the change, the description of Playpen's homepage in the Warrant Application differed from the homepage that would have been seen by Allain when he accessed the website prior to the NIT deploying. According to the Warrant Application, "On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, 'No cross-board reposts, . 7z preferred, encrypt filenames, include preview, Peace out.'" [ECF No. 61-2 ¶ 12]. At the time the NIT Warrant was executed, however, and therefore at the time Allain logged into Playpen, the homepage contained a single image, not two. The image, to the right of the site name "PlayPen," depicted a prepubescent girl, wearing a short dress and black stockings, reclined on a chair with her legs crossed and posed in a sexually suggestive manner. [ECF No. 61-12]. To the right of the site name was text stating, "No Cross-Board Posts; 7z Preferred; Encrypt File-Names; Include Preview." Id.

c. The Search

Following the issuance of the NIT Warrant, on or about February 27, 2015, FBI agents sent the NIT to a computer connected to someone with the Playpen username "littlepinks." [ECF No. 61 at 14]. On March 4, 2015, the FBI used some of the data that the NIT collected from the computer affiliated with "littlepinks" to prepare an administrative subpoena for Verizon, intended to reveal the identity of "littlepinks." Verizon responded with Allain's subscriber information, name and address. Id. at 15.

III. Motion to Suppress

a. The NIT Warrant Was Supported by Probable Cause

The Fourth Amendment to the United States constitution provides 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. Pursuant to the Fourth Amendment, before executing a search, law enforcement must generally obtain a search warrant supported by probable cause.

"A warrant application must demonstrate probable cause to believe that (1) a crime has been committed—the 'commission' element, and (2) enumerated evidence of the offense will be found at the place searched." United States v. Dixon, 787 F.3d 55, 58–59 (1st Cir. 2015), cert. denied, 136 S. Ct. 280 (2015) (quoting United States v. Feliz, 182 F.3d 82, 86 (1st Cir.1999)). "Probable cause does not require certainty or an unusually high degree of assurance. All that is needed is a 'reasonable likelihood' that incriminating evidence will turn up during a proposed search." United States v. Clark, 685 F.3d 72, 76 (1st Cir. 2012) (citation omitted). In other

words, the facts presented in the warrant application "need only 'warrant a [person] of reasonable caution' to believe that evidence of a crime will be found." Dixon, 787 F.3d at 59; see also United States v. Rivera, 825 F.3d 59, 63–64 (1st Cir. 2016) ("[P]robable cause does not demand certainty, or proof beyond a reasonable doubt, or even proof by a preponderance of the evidence—it demands only 'a fair probability that contraband or evidence of a crime will be found in a particular place.'").

"The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before [him or her] . . . 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, 238–39 (1983). The magistrate judge determines whether the "totality of the circumstances" stated in the affidavit demonstrate probable cause to execute a search. Id.

When reviewing a magistrate judge's probable cause determination, the "district court should pay great respect to the issuing magistrate's determination of probable cause." United States v. Tanguay, 787 F.3d 44, 49 (1st Cir. 2015). A court should reverse a magistrate judge "only if [there is] no substantial basis for concluding that probable cause existed." Dixon, 787 F.3d at 58-59 (citation omitted).

The NIT Warrant authorized the NIT to be deployed to any computer used to log into Playpen. Because logging into Playpen was not itself a crime, the warrant application needed to establish probable cause to believe that anyone logging into Playpen was doing so for the purpose of viewing or distributing child pornography. See United States v. Wilder, 526 F.3d 1, 6–7 (1st Cir. 2008) (finding probable cause to search defendant's home based on his subscription to child pornography website because "it was a fair inference from his subscription . . . that

downloading and preservation in his home of images of child pornography might very well follow.").

Allain contends that merely logging into Playpen was not sufficient to establish probable cause that a crime had been committed or that evidence of a crime would be found by the NIT. Allain complains that, "[T]he NIT warrant did nothing to distinguish between accidental browsers (or even people looking for legal pornography or more extreme, but still legal, fetish content) and people who . . . had indisputably viewed samples of the child pornography." [ECF No. 61 at 20-21].

Allain claims that "when a computer search is based on a user's mere accessing of a website, there is probable cause for a search only if the site's illegal purpose or content is readily apparent," and that here, the illegal content of Playpen was not readily apparent from its homepage. In support of this argument, he relies primarily on the First Circuit's decision in United States v. Wilder, 526 F.3d 1 (1st Cir. 2008). In Wilder, the First Circuit found probable cause to search the defendant's residence based in part on defendant's subscription to a pay-for-membership website called "Lust Gallery." The First Circuit found that "[t]he entrance page of the [Lust Gallery] website, as described, was plainly designed and written to attract persons interested in viewing child pornography." 526 F.3d at 6. As a result, "it was a fair inference from [defendant's] subscription to the Lust Gallery website . . . that downloading and preservation in his home of child pornography might very well follow." Id. The First Circuit noted that the preview page for the website showed naked female children identified as being under fourteen years old. Id. at 3. Furthermore, the preview page stated that "everyone understands there are reasons not to reveal everything right here." Id. Based on the appearance of the website, which "vividly indicated that child pornography was a featured product," as well as the fact that the

defendant had previously been convicted for possession of child pornography, the First Circuit found that there was probable cause to believe that child pornography had been accessed and might be found at his home. Id. at 6-7.

Allain claims that it was much less clear from Playpen's homepage that Playpen was a site dedicated to child pornography because the name of the site was less suggestive than in Wilder, the home page did not contain naked pictures of children, as in Wilder, and no fee was required to register. As a result, according to Allain, "the warrant made no distinction between, on the one hand, casual or unwitting visitors and accidental browsers and, on the other, the subset of people actively seeking child pornography; instead, both groups were authorized targets of the FBI's searches." [ECF No. 61 at 22].

Although Playpen's homepage was less suggestive than the homepage in Wilder, there was nonetheless probable cause to issue the NIT Warrant. While it was possible that someone could log into Playpen and then not attempt to access child pornography, probable cause does not require certainty, and the Warrant Application and supporting affidavit established a fair probability that anyone who logged into Playpen would view or share child pornography. The appearance of Playpen's homepage was only one of the several factors supporting the magistrate's probable cause determination. Even if the homepage alone would not have established probable cause, the totality of the circumstances were sufficient to demonstrate the requisite level of proof. See Illinois v. Gates, 462 U.S. 213, 238–39 (1983) ("The task of the issuing magistrate is simply to 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.") (emphasis added).[4]

Unlike in Wilder, Playpen operated as a hidden service on the Tor network. The parties dispute how hidden websites on the Tor network can be located, but there is no question that it was difficult to find. Users first had to gain access to the Tor Network, and then somehow locate the site, despite its indecipherable web address. Therefore, the Court credits the affiant's statement in the warrant application that it would be "extremely unlikely that any user could simply stumble upon [Playpen] without understanding its purpose and content." [ECF No. 61-2 ¶ 10]. Playpen was in fact a website devoted to child pornography, and the fact that users found it and then logged into it is indicative of criminal intent. While there may be legitimate reasons to use the Tor network other than masking illicit activity, the clandestine nature of the website and the challenges of finding it on the Tor Network suggests that those who logged into Playpen likely knew the purpose of the website and were entering it to access child pornography.

Playpen's registration terms, which appeared before users setup a username and password, gave further indication of Playpen's illicit purpose. Prospective registrants were told that, "the forum operators do NOT want you to enter a real [e-mail] address," that users "should not post information [in their profile] that can be used to identify you," and that, "[t]his website is not able to see your IP." In addition, Playpen's homepage (as it actually appeared when the warrant was issued and Allain logged in), though not as suggestive as in Wilder, would likely still have alerted users to the general content of the website. The homepage had a picture of a young girl scantily clad, was titled "Playpen," and required a username and password to proceed.

[4] In addition, the search in Wilder authorized a search of the defendant's entire home, while the warrant here only authorized a search of the computers actually used to log into the site.

Considering the totality of the circumstances—the appearance and content of Playpen, the fact that it was a hidden service on the Tor network, and its registration terms—the magistrate judge had a substantial basis for concluding that the search warrant was supported by probable cause to believe that evidence of criminal conduct would be found on computers used to log into Playpen. While it may not have been a certainty that Playpen registrants intended to access child pornography, there was a fair probability that users who took the time to locate Playpen, and then log in, did so intending to access child pornography, thus establishing probable cause that the NIT would uncover relevant evidence of a crime.[5]

b. A Franks Hearing Is Not Required

Next, the Defendant contends that he is entitled to a Franks hearing to address the Warrant Application's mischaracterization of the Playpen homepage. As previously discussed, between the time the Warrant Application was drafted and the warrant was issued and executed, the appearance of the homepage changed. As a result, the description of Playpen's homepage in the Warrant Application differed from the homepage that would have been seen by Allain when he accessed the website prior to the NIT deploying. Allain claims that the "FBI intentionally or recklessly misled the issuing court about how the site appeared, among other false and misleading statements" and that an evidentiary hearing is therefore required. [ECF No. 61 at 2].

[5] Several courts have held that because individuals lack a reasonable expectation of privacy in their IP addresses, the FBI did not need to obtain the NIT Warrant in the first place. See, e.g., United States v. Werdene, No. CR 15-434, 2016 WL 3002376, at *8 (E.D. Pa. May 18, 2016); United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016). The Court disagrees, and finds that the FBI did need to obtain a warrant in order to use the NIT. The FBI's search not only implicated defendant's privacy interest in his IP address, but also in his computer. Although an IP address may be obtained from a third party provider and therefore arguably carries with it a lower expectation of privacy, in this case, the FBI needed to install a program that searched through Allain's computer to get the IP address. Regardless of whether and to what extent Allain had a privacy interest in his IP address, he most certainly had a reasonable expectation of privacy in the contents of his computer.

There is a "presumption of validity with respect to the affidavit supporting the search warrant." Franks v. Delaware, 438 U.S. 154, 171 (1978). The Supreme Court's Franks decision established the limited circumstances in which a defendant is entitled to an evidentiary hearing (now known as a "Franks hearing") regarding the accuracy of a warrant application. A court is required to hold a Franks hearing only when "the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and [that] the allegedly false statement is necessary to the finding of probable cause . . . ." Id. at 155-56. This is a two prong standard: the defendant must demonstrate both a "substantial preliminary showing of intentional reckless falsehood in the affidavit," and also that the contested statement is "crucial to the probable-cause calculation—no evidentiary hearing is required if after ignoring the fought-over comment, enough remains in the affidavit to show probable cause." United States v. Rivera, 825 F.3d 59, 66-67 (1st Cir. 2016).

Here, the Defendant has not met either requirement. He has not shown that the inaccurate description of the homepage was made knowingly or with reckless disregard for the truth, or that it was material to the probable cause determination. In the Warrant Application, the affiant stated that he last accessed Playpen on February 18, 2015. [ECF No. 61-2 ¶ 11, n.3]. Between the last time he accessed the site and the time the warrant was authorized one day later on February 19, 2015, the homepage was apparently modified. There is no indication that the affiant knew about this change, purposefully provided misleading or false information in the Warrant Application, or intentionally excluded pertinent information from the Warrant Application. It was not reckless for the affiant to submit a warrant application on February 19, based on how the website appeared on February 18. "Allegations of negligence or innocent mistake" are insufficient to

warrant a Franks hearing, Rivera, 825 F.3d at 66 (citation omitted), and the Court finds that Defendant's allegations here are nothing more than that. See United States v. Adams, 305 F.3d 30, 36 n.1 (1st Cir. 2002) ("Mere inaccuracies, even negligent ones, are not enough" to entitle defendant to Franks hearing.).

In addition, as discussed *supra*, probable cause did not depend on the affiant's description of the homepage. Even if the affiant had accurately described the homepage, there would have been probable cause for the search. The actual appearance of the homepage was still suggestive of Playpen's pornographic content, and in any event, the appearance of the homepage was only one of several factors supporting the magistrate judge's determination.[6]

The Defendant identifies a handful of other alleged misrepresentations in the Warrant Application that he claims also entitle him to a Franks hearing. [ECF No. 61 at 26-28]. These include the affiants' claim that "the entirety" of Playpen is "dedicated to child pornography," [ECF No. 61-2 ¶ 27], that websites on Tor cannot be accessed by a Google-type search, Id. ¶ 10, and that Playpen had certain features, such as messaging and image uploading, that were indicative of criminality. Id. ¶¶ 15, 23. Unlike the application's description of the homepage, none of these statements were demonstrably false. The affiant assessed Playpen based on his training and experience. The Court has no reason to believe that the affiant's assessment of the website was intended to mislead the magistrate judge, nor has Defendant made the substantial preliminary showing that any of these statements were knowingly and intentionally false, or

[6] The Court also rejects Defendant's argument that the "Triggering Event" required by the NIT Warrant never occurred. [ECF No. 61 at 32]. The "triggering event" for the NIT warrant was the action of logging into Playpen by entering a username and password. There is no allegation that the NIT was deployed before this triggering event took place.

made with a reckless disregard for the truth. Therefore, these additional statements also do not entitle the Defendant to a Franks hearing;

c. The NIT Warrant Was Not Overbroad

Allain next argues that the NIT Warrant was overbroad, characterizing it as the "Internet age equivalent of a general warrant" that "allow[ed] the FBI to search tens of thousands of computers for which probable cause to search was not established." [ECF No. 61 at 30]. Allain contends that the NIT Warrant gave the FBI too much discretion, applied to too many users, and should have been narrowed to authorize searches of only those site visitors who viewed or downloaded illegal pornography, rather than broadly applying to any visitors that logged into the site. [ECF No. 61 at 28-32].

This argument is largely duplicative of Defendant's probable cause argument. As already discussed, there was adequate support for the magistrate judge's finding that there was probable cause to search any computers that logged into Playpen. It is irrelevant how many computers were covered by the warrant, given that there was probable cause to search each one. Likewise, it is irrelevant that the warrant could have been narrower, given that the warrant as actually issued was sufficiently narrow to limit searches to computers for which there was probable cause to search.[7]

[7] On July 27, 2016, the government submitted an addendum to its opposition to Defendant's Motion to Suppress [ECF No. 77], which claimed to show that the NIT was not put onto Allain's computer until after he downloaded child pornography from Playpen. In other words, though the FBI had authority to deploy the NIT as soon as Allain logged into Playpen, it nonetheless waited to deploy the NIT until Allain had actually accessed child pornography. On that same day, Allain moved to strike the addendum, arguing that it was untimely and referenced underlying information and evidence that had not been previously disclosed. [ECF No. 78]. Because the NIT Warrant authorized the FBI to deploy the NIT whenever a user logged on, the fact that the FBI waited for Allain to download pornography before deploying the NIT is irrelevant to Allain's challenge to the NIT Warrant. Accordingly, the Court will not consider the evidence, and Defendant's Motion to Strike [ECF No. 78] is granted. The Court notes, however, that if the

Furthermore, the warrant described with particularly the locations to be searched and the things to be seized. The particularity requirement of the Fourth Amendment "demands that a valid warrant: (1) . . . supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in the sense that it includes items that should not be seized." United States v. Kuc, 737 F.3d 129, 133 (1st Cir. 2013). "In requiring a particular description of articles to be seized, the Fourth Amendment 'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'" United States v. Fuccillo, 808 F.2d 173, 175 (1st Cir. 1987) (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965)).

The NIT Warrant is not a general warrant in that it clearly limited which computers could be searched and what information could be obtained as a result of that search. Attachment A of the warrant authorized deployment of the NIT to the computer server hosting Playpen and then to computers of "any user or administrator who logs into [Playpen] by entering a username and password." Ex. A, Att. A. Attachment B, in turn, imposed detailed limits on what information could be obtained from those computers by the NIT. Id., Att. B. The NIT Warrant therefore satisfied the particularity requirements of the Fourth Amendment. See United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *5 (W.D. Wash. Jan. 28, 2016) ("Both the particularity and breadth of the NIT Warrant support the conclusion that the NIT Warrant did not lack specificity and was not a general warrant."); United States v. Epich, No. 15-CR-163-PP, slip. op. at 19 (E.D. Wis. Mar. 14, 2016) ("[T]he NIT Warrant satisfied the Fourth Amendment's

warrant had not been supported by probable cause, this evidence would have been relevant to the FBI's good faith.

particularity requirement as it specifically described the place to be searched and things to be seized."); United States v. Darby, No. 2:16CR36, 2016 WL 3189703, at *8 (E.D. Va. June 3, 2016) ("The NIT Warrant describes particular places to be searched – computers that have logged into Playpen – for which there was probable cause to search. It is not a general warrant.").

d. Fed. R. Crim. P. 41(b) Does Not Require Suppression

Lastly, Allain argues that because the magistrate judge lacked authority to issue the NIT Warrant under Fed. R. Crim. P. 41(b) ("Rule 41(b)") the warrant was void ab initio and all the evidence seized pursuant to the warrant must be suppressed.

Rule 41(b) sets geographic limits on a magistrate judge's authority to issue a search warrant and generally requires, with some exceptions, that the person or property to be searched must be located within the district at the time the warrant is issued. On its face, the Warrant Application stated that the person or property to be searched was located in the Eastern District of Virginia. [ECF No. 61-2 at 2]. Under Rule 41(b)(1), a magistrate judge clearly has authority to issue a warrant allowing the search and seizure of property located within his or her district. Fed. R. Crim P. 41(b)(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."). Likewise, under Rule 41(b)(2), a magistrate judge may issue a warrant to search and seize property located within his or her district at the time the warrant is issued, but which has moved outside of the district by the time the warrant is executed. Fed. R. Crim. P. 41(b)(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.").

The NIT Warrant Application misidentified the location of the place to be searched when it specified that the place to be searched was within the Eastern District of Virginia, based on the location of the government server that was hosting Playpen. [ECF No. 61-2 at 2]. It stated that the warrant would authorize "the use of a network investigative technique ('NIT') to be deployed on the computer server described below," and then described the server as "the server operating the Tor network child pornography website . . . which will be located at a government facility in the Eastern District of Virginia." Id. at Att. A. While it was technically true that the server would be located in the Eastern District of Virginia, and that the Eastern District of Virginia was the locus of the government's investigation, the actual searches authorized by the NIT Warrant would take place wherever computers used to login to Playpen were located, which could include computers in the Eastern District of Virginia, but would clearly also include computers all over the country, if not the world. The NIT Warrant authorized the FBI to deploy the NIT on any "activating" computer, defined as the computer "of any user or administrator who logs into [Playpen] by entering a username and password." Id. The definition of "activating" computer did not have any geographic limitation. Accordingly, whether a Playpen visitor logged into the site from a computer in the Eastern District of Virginia, the District of Massachusetts, or anywhere else, the NIT Warrant authorized the FBI to deploy the NIT and then search any computer used to log into Playpen.

Because there was no geographic limit on the "activating" computers that could be searched, Rules 41(b)(1) and (2) are inapposite. Some of the "activating" computers could have been located in the Eastern District of Virginia at the time the NIT Warrant was issued and executed, and in theory, some could have been located in the Eastern District of Virginia when the NIT Warrant was issued, but moved outside the district by the time it was executed. Most of

these "activating" computers, however, like the computer in the instant case, were unlikely to have any physical tie to the Eastern District of Virginia, and to be located outside the district at the time the warrant was issued and executed. Accordingly, this Court agrees with several other courts that have already found that Rules 41(b)(1) and (2) did not give the Eastern District of Virginia magistrate judge authority to issue the NIT Warrant. See, e.g., United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *5 (M.D. Fla. Aug. 10, 2016); United States v. Werdene, No. CR 15-434, 2016 WL 3002376, at *7 (E.D. Pa. May 18, 2016).

The government claims that Rule 41(b)(1) and/or (2) properly authorized the warrant, because the NIT was deployed from a server in the Eastern District of Virginia, and the "NIT was only retrieved by registered users of Playpen who logged into the website, located within the Eastern District of Virginia, with a username and password." [ECF No. 69 at 40]. "The NIT," according the government, "constituted property within the District from which the warrant issued." Id. at 40. The NIT, however, was not the property being searched, rather, the NIT was *performing* the search on "activating" computers located around the country.

Alternatively, the government attempts to argue that the NIT is a tracking device, and that the magistrate judge could issue the NIT Warrant under Rule 41(b)(4). Rule 41(b)(4) 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. Civ. P. 41(b)(4). Some courts have agreed that the NIT was analogous to a tracking device, and that Rule 41(b)(4) therefore permitted the NIT Warrant. These Courts have found that "whenever someone entered Playpen, he or she made, in computer language, 'a virtual trip' via the Internet to Virginia." United States v. Matish, No. 4:16CR16, 2016 WL 3545776, at *18 (E.D. Va. June 23, 2016); see also United States v. Darby,

No. 2:16CR36, 2016 WL 3189703, at *12 (E.D. Va. June 3, 2016) ("Users of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site."). The NIT, according to these courts, tracked the movement of this "virtual trip."

There is a plausible argument that the installation of the NIT falls within Rule 41(b)(4)'s tracking device provision, since the ultimate purpose of the NIT was to identify the location of Playpen users. The Court finds, however, that the NIT is not analogous to the tracking devices allowed under Rule 41(b)(4) because the NIT did not merely track the movement of a person or object. See 18 U.S.C. § 3117(b) (defining "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object."). Rather, once installed on a Playpen user's computer, the NIT searched for and seized data from the computer, including the computer's IP address, host name, and operating system. This type of information is significantly more extensive than that contemplated by Rule 41(b)(4). See Rule 41 Comments ("The amendment is based on the understanding that the device will assist officers only in tracking the movements of a person or property.").

Even if the Court agreed with the tracking device analogy, the NIT Warrant would still not be permitted under Rule 41(b)(4), since the NIT was not installed in the Eastern District of Virginia. Rule 41(b)(4) allows a magistrate judge to "issue a warrant to install *within the district* a tracking device." Fed. R. Civ. P. 41(b)(4) (emphasis added). The NIT was downloaded from the Playpen server (located in the Eastern District of Virginia) and placed onto the "activating" computers (located anywhere in the U.S.). Given that the "activating" computers never entered the Eastern District of Virginia, it stretches the rule too far to say that the installation occurred within the Eastern District of Virginia.

Having found that the NIT Warrant did not comply with Rule 41(b), the Court must next determine the consequence of this noncompliance. In United States v. Levin, after similarly finding that that the NIT Warrant was not authorized under Rule 41(b), Judge Young ordered that the evidence seized pursuant to the NIT Warrant be suppressed. No. CR 15-10271-WGY, 2016 WL 2596010, at *10 (D. Mass. May 5, 2016). He concluded that the NIT Warrant was void ab initio because the magistrate judge lacked jurisdiction to issue the warrant, and therefore any evidence seized pursuant to the void warrant could not be used, regardless of the FBI's good faith. The good faith exception, Judge Young concluded, did not apply because it is intended only for "subsequently invalidated warrants," and not for "a warrant that was void at the time of its issuance." Id. at *10 (emphasis in original).[8] Judge Young held that a "warrant that was void at the outset is akin to no warrant at all" and relied on First Circuit law declining to "recognize[] a good-faith exception in respect to warrantless searches." Id. at *12; United States v. Curzi, 867 F.2d 36, 44 (1st Cir. 1989). See also United States v. Croghan, No. 1:15-CR-48, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016) (substantially agreeing with the reasoning of Levin); United States v. Workman, No. 1:15-CR-00397 (D. Colo. Sept. 6, 2016) (same).

This Court however does not find the evidence seized through the use of the NIT Warrant must be suppressed. Though the NIT Warrant technically violated Rule 41(b), the FBI's conduct was objectively reasonable, and the good faith exception therefore applies. See, e.g., United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10,

[8] The Court declines to conclude that evidence obtained through a warrant that was supported by probable cause, but that ran afoul of a jurisdictional statute, must be suppressed, but that evidence seized pursuant to a warrant later found not to be supported by probable cause, an issue of constitutional dimension, can be preserved by a finding of good faith. In this case, suppressing the fruit of the search would do nothing to deter misconduct on the part of law enforcement, which is the purpose of the exclusionary rule.

2016) (declining to follow cases holding that a violation of Rule 41(b) renders the warrant void *ab initio*); United States v. Werdene, No. CR 15-434, 2016 WL 3002376, at *14 (E.D. Pa. May 18, 2016) (noting that "[t]he good faith exception is not foreclosed in the context of a warrant that is void *ab initio* and the Court must now determine if it applies").

As the Supreme Court articulated in United States v. Leon, evidence seized pursuant to a procedurally defective warrant need not be suppressed, where the warrant was executed in good faith. Leon, 468 U.S. 897, 913 (1984). By good faith, the Supreme Court means where law enforcement acted in "objectively reasonable reliance" on the defective search warrant. Id. at 922; see also Herring v. United States, 555 U.S. 135, 142 (2009) ("When police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted 'in objectively reasonable reliance' on the subsequently invalidated search warrant. We (perhaps confusingly) called this objectively reasonable reliance 'good faith.'") (internal citations omitted). When law enforcement "acting with objective good faith ha[ve] obtained a search warrant from a judge or magistrate and acted within its scope," there is "no . . . illegality and thus nothing to deter." Leon, 468 U.S. at 920-21.

In Levin, Judge Young cited several cases in which suppression was ordered because the evidence was seized pursuant to a search warrant issued by an unauthorized judge. These cases involved such clear violations of Rule 41(b) that the law enforcement activity at issue was not objectively reasonable. In United States v. Scott, 260 F.3d 512, 515 (6th Cir. 2001), for instance, the issuing judge was retired and therefore "possessed no legal authority pursuant to which he could issue a[ny] valid warrant."[9] In United States v. Krueger, 809 F.3d 1109, 1116–17 (10th

[9] The Sixth Circuit has also indicated that Scott, decided in 2001, is "no longer clearly consistent with current Supreme Court doctrine." United States v. Master, 614 F.3d 236, 242 (6th Cir.

Cir. 2015), the warrant "clearly violate[d]" Rule 41(b)(1) and constituted "gross negligence," where a federal magistrate judge in the District of Kansas issued a warrant for property already located in Oklahoma.

Here, by contrast, the FBI's reasonable, albeit incorrect, interpretation of Rule 41(b) (an interpretation seemingly endorsed by the prosecutor and the magistrate judge) caused an invalid search warrant to be issued. The FBI's conduct was not "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." United States v. Master, 614 F.3d 236, 243 (6th Cir. 2010) (quoting Herring v. United States, 555 U.S. 135, 144 (2009)). The FBI's investigation into Playpen involved sophisticated and novel technology—used both by the operators and users of Playpen as well as the federal investigators—and the FBI made a reasonable attempt to structure a search warrant that complied with rules that have not evolved as quickly as the technology. The First Circuit has indicated that "[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. Bonner, 808 F.2d 864, 867 (1st Cir. 1986). The remedial objectives of the exclusionary rule do not require the exclusion of the evidence seized using the NIT Warrant. The warrant was supported by probable cause. Though the warrant did not technically comply with Rule 41(b), the FBI's decision to apply for the warrant from a single a magistrate judge in the Eastern District of Virginia was objectively reasonable, particularly given the legal complexities of the situation.[10]

2010); see also United States v. Beals, 698 F.3d 248, 265 (6th Cir. 2012) (recognizing that Master overruled Scott).

[10] The court notes that the fact that the magistrate judge did not properly identify or resolve the issue and that reviewing courts have had differing views of the issue raised by the NIT warrant

IV. Motion to Dismiss

In addition to the Motion to Suppress, Allain has also filed a Motion to Dismiss Count II of the indictment based on the contention that by continuing to operate Playpen during its investigation, and therefore briefly facilitating the distribution of child pornography, the government engaged in outrageous misconduct that warrants dismissal of the resulting charge. As described above, following its seizure of Playpen, the government operated the website for an additional two weeks during which the FBI allowed the distribution of child pornography through Playpen to continue. Allain claims that this decision to keep Playpen in operation, "cannot be reconciled with fundamental expectations of decency and fairness." [ECF No. 62 at 14].

The government responds that its conduct was necessary given the challenges of investigating and prosecuting child pornography. While reasonable people might disagree over the government's decision to allow Playpen to remain in operation unabated, "it did not act outrageously and certainly not in a matter that offends fundamental notions of fairness." [ECF No. 70 at 9].

The outrageous government conduct doctrine "permits dismissal of criminal charges only in those very rare instances when the government's misconduct is so appalling and egregious as to violate due process by 'shocking . . . the universal sense of justice.'" United States v. Luisi, 482 F.3d 43, 59 (1st Cir. 2007) (quoting United States v. Russell, 411 U.S. 423, 432 (1973)). "While the doctrine is often invoked by criminal defendants, it has never yet been successful in this circuit." Id. at 59.

---

further suggest the conclusion that the law enforcement approach was undertaken in good faith and that the extreme remedy of suppression is not warranted.

The Court agrees with Allain that the government's investigation had disturbing consequences: while investigating child pornography, the government facilitated the distribution of child pornography and did so in way that did not allow the pornography it distributed to be retrieved or cabined. Thus, the child pornography distributed by the government might live on and be redistributed in the internet ether for an indeterminate period of time. Furthermore, the Court is concerned by Allain's allegations that traffic to Playpen increased after the government took over operation of the site. Nonetheless, the Court will not dismiss Count II. Given the difficulty of identifying individuals that access child pornography online, the governments' conduct was not so outrageous as to warrant dismissal. As child pornography migrates to the hidden corners of the web, the government will have to continue to make difficult choices about how to investigate and prosecute the related crimes. Reasonable minds will no doubt differ on whether the government made the right choice here, but it is not the rare case in which any misconduct on the part of the government was sufficiently blatant, outrageous, or egregious to warrant the dismissal of the indictment.

V. Conclusion

For the reasons stated herein, Defendant's Motion to Suppress [ECF No. 60] and Motion to Dismiss [ECF No. 62] are DENIED.

So Ordered.

September 29, 2016

/s/ Allison D. Burroughs
ALLISON D. BURROUGHS
U.S. DISTRICT JUDGE