UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 16-cr-20551

v.

Honorable Thomas L. Ludington

JASON JOHN KAHLER,

Defendant.

_____/

OPINION AND ORDER DENYING MOTION TO SUPPRESS

On February 20, 2015, a federal magistrate judge in the Eastern District of Virginia signed a warrant authorizing a FBI hacking operation designed to infiltrate a suspected child pornography website, named "Playpen."[1] After breaching the website's security, the FBI recoded the website to request certain information from every computer that accessed the website. Because of that coding, accessing computers sent identifying information to the FBI. Using the data gathered, the FBI obtained a warrant from a magistrate judge for the Eastern District of Michigan to search Defendant Jason John Kahler's home and computer, located in Saginaw, Michigan. The items seized in that search served as the basis for the August 10, 2016, indictment which charges Kahler with possessing prepubescent child pornography. ECF No. 1. On December 21, 2016, Kahler filed a motion to suppress the fruits of the original warrant which authorized the hacking operation. ECF No. 21. On February 9, 2017, the parties submitted a stipulation to waive oral argument on the motion. ECF No. 29. Because the material facts are

[1] The website is no longer active and the details of the hack have been reported on by the media. Accordingly, directly identifying the website poses minimal threat to ongoing investigations.

largely undisputed, the motion to suppress will be decided based on the arguments made in the briefing. For the reasons that follow, the motion to suppress will be denied.

I.

A.

The following information is primarily drawn from the affidavits in support of the two applications for a search warrant. The "target website" which the FBI hacked was operated on the so-called "dark web." The dark web is accessed by using certain software (Tor routing software) which routes communications through a series of computers and thus masks the user's IP address. The Tor software prevents websites from learning the user's physical location and prevents individuals attempting to monitor the user's internet usage from determining which sites have been visited. When, as was the case for Playpen, a website can be accessed only by users which are using Tor Software, it is considered part of the dark web. Further, the dark web is not indexed like the traditional internet. Accordingly, a Tor user could not simply use a search engine to discover and access Playpen.[2] Rather, Playpen could be accessed only by someone who had obtained its web address from another source, like a user familiar with the site or an online posting.

According to the FBI's affidavit, Playpen "was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children." FBI Aff. at 12, ECF No. 21, Ex. A. Playpen became active in approximately August 2014. As of March 4, 2015, 117,773 posts had been made by 214, 898 total members on Playpen. Between September 2014 and February 19, 2015, the front page of Playpen included an image of two scantily clothed girls. Both girls were posed

[2] As discussed below, Kahler disputes this point, but has not sufficiently corroborated this assertion to justify holding a hearing. Even if this assertion in the warrant were not true, the motion to suppress the warrant would still be denied.

salaciously and appeared to be prepubescent. The image also included the website's title and the following text: "No cross-board reposts, .7z preferred, encrypt filenames, include preview." Gov. Resp., ECF No. 27, Ex. 1. According to the FBI Agent who prepared the affidavit: "Based on my training and experience, I know that: 'no cross-board reposts' refers to a prohibition against material that is posted on other websites from being 're-posted' to [Playpen]; and '.7z' refers to a preferred method of compressing large files or sets of files for distribution." FBI Aff. at 13.

On February 19, 2015, the image on the front page was changed. The new image depicted one girl with no visible breast development. The girl was pictured wearing a short dress which exposed her upper thighs and thigh-high fishnet stockings. She was posed in a chair in a sexually suggestive manner. The new image also included instructions which forbade cross-posts, indicated a preference for .7z, and directed users to encrypt the file names and include a preview.

Only registered users were allowed to enter Playpen. The front page included a hyperlink to the registration page. On that account registration page, users were directed to enter an "email address," but the page expressly instructed users to enter a fake email address. Users were also instructed that "'for your security you should not post information here that can be used to identify you.'" *Id.* The registration page included further instructions regarding best practices for hiding the user's identity.

According to the affidavit, Playpen included (among others) the following forums and subforums: "(a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat." *Id.* at 14. The FBI affiant indicated that, based on his training and experience, he knew "that 'jailbait' refers to underage but post-pubescent minors; [and] the abbreviation 'HC' means hardcore (i.e., depictions of penetrative sexually explicit conduct)." *Id.* Playpen included a forum

where members could exchange usernames for a Tor-based instant messaging service which the FBI agent knew to be commonly used by individuals "engaged in the online sexual exploitation of children." *Id.* Playpen included text-only sections where, according to the FBI affidavit, members discussed methods and tactics for the perpetuation of child sexual abuse. The website also included a private message function which users used to correspond more discretely. At least one post on the website revealed that private messages were being sent to discuss sexual abuse of children perpetrated by the users themselves.

B.

In December 2014, a foreign law enforcement agency informed the FBI that it suspected the target website's originating IP address was based in the United States. After further investigation, the FBI located the server hosting the target website, in North Carolina, and the residence of the website's administrator, located in Florida. The FBI seized the server, transported it to a government facility in Virginia, and assumed administrative control of Playpen. Rather than closing the website, the FBI chose to briefly operate Playpen in order to identify users of the website. Despite the FBI's control over Playpen, the Tor software through which members accessed the site prevented the FBI from obtaining identifying information from the users.

To overcome the anonymity granted by the Tor software, the FBI sought a warrant authorizing a "Network Investigative Technique" ("NIT"). That technique works as follows: Typically, users view a webpage by communicating with the website. The user's computer requests access to a certain webpage, and the website then sends content to the user's computer. The user's computer receives that information and uses it to display the webpage. The NIT augments the instructions sent by the webpage and causes the user's computer to transmit

identifying information from that computer, including the computer's IP address, operating system, operating system username, and network adapter address.

A United States Magistrate Judge for the Eastern District of Virginia approved the FBI's search and seizure warrant, thus authorizing use of the NIT. After the FBI implemented the NIT, Defendant Kahler's computer made two postings on the target website on two different days. Based on the information the NIT revealed, the FBI sought and obtained a warrant to search Kahler's residence and computer. Pornographic images of minors were seized during the search. After that search, Kahler was charged with possessing prepubescent child pornography. This motion to suppress followed.

II.

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

Generally speaking, the requirement that searches be reasonable means law enforcement officials must obtain a judicially approved warrant beforehand. *Riley v. California*, 134 S. Ct. 2473, 2482 (2014). To satisfy the warrant requirement, a detached, neutral judge must find that there is probable cause that evidence of a crime will be found. *United States v. Leon*, 468 U.S. 897, 913–15 (1984). "[G]reat deference" is given to a magistrate's determination that probable cause exists. *Id.* at 914. And there is a "presumption of validity with respect to the affidavit supporting the search warrant." *Franks v. Delaware*, 438 U.S. 154, 171 (1978). However, if a defendant shows that the warrant affidavit included deliberate falsehoods or otherwise demonstrates a

reckless disregard for the truth and the finding of probable cause was dependent on those falsehoods, the defendant is entitled to a hearing. *Id.*

Even if the defendant shows that the Fourth Amendment was violated, "suppression is not an automatic consequence." *Herring v. United States*, 555 U.S. 135, 137 (2009). The key inquiry is whether "the culpability of the police" and the need "to deter wrongful police conduct" justifies suppression. *Id.* Because the purpose of exclusion is deterrence, exclusion is not an individual right, even when the defendant's Fourth Amendment rights have been violated. *Id.* at 141. Exclusion is a last resort, not a "first impulse." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). Even if exclusion would provide some marginal deterrence, that benefit must outweigh the costs of exclusion. *Pennsylvania Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 369 (1998). Generally speaking, "the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring*, 555 U.S. at 144. If law enforcement's reliance on the warrant's lawfulness was objectively reasonable, exclusion is inappropriate. *Id.* at 142–43; *Leon*, 468 U.S. at 922.

III.

Kahler argues that the warrant approved by the Magistrate Judge for the Eastern District of Virginia exceeded the court's territorial jurisdiction of the court, as provided in Federal Rule of Criminal Procedure 41(b). Kahler further argues that the warrant violated the Fourth Amendment's particularity requirement. Third, Kahler argues that the FBI agent who wrote the affidavit supporting the warrant purposely included materially misleading or incorrect information. Finally, Kahler argues that suppression is the appropriate remedy.

A.

Rule 41(b) provides guidelines for determining the proper venue for a warrant application.[3] At the time of the warrant, there were five alternative bases for venue to issue a warrant, only three of which had any possible relevance to this warrant:

> (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> . . .
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both;

Id. at Rule 41(b)(1), (2), and (4).[4]

The FBI's hack of Playpen has resulted in at least dozens of prosecutions across the county. The warrant authorizing the NIT has been challenged repeatedly, with courts adopting essentially one of three outcomes. Most federal courts to review the NIT warrant have concluded that it was likely not properly issued pursuant to Rule 41, but that suppression was inappropriate

---

[3] The Federal Magistrates Act gives magistrate judges "all powers and duties conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts." 28 U.S.C. § 636(a)(1).

[4] After the FBI's seizure of the target website occurred, Rule 41(b) was amended to expressly address situations like the one the FBI faced here. Rule 41(b)(6) reads as follows:

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

Id.

because of the circumstances of the investigation and warrant request.[5] A substantial minority of courts to rule on the NIT warrant have concluded that the warrant was properly issued pursuant to Rule 41.[6] A small number of courts have suppressed the warrant.[7]

The legal issues presented by this motion to suppress are difficult to resolve precisely because the technology deployed by child pornography criminals to obscure their behavior and the law enforcement investigative tactics developed to enforce the law were not contemplated when Rule 41 was drafted. The rule, focused on the geographic location of physical documents and objects, was not crafted for a world with Tor-routing software, technologically sophisticated websites designed to shield the distribution of child-pornography from law enforcement, and the

[5] *See United States v. Kneitel*, No. 16 -cr-23-MSS-JSS (M.D. Fl. Jan. 3, 2017); *United States v. Tran*, No. 16-cr-10010, 2016 WL 7468005 (D. Mass. Dec. 28, 2016); *United States v. Dzwonczyk*, No. 15-cr-3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016); *United States v. Vortman*, No. 16-cr-210, 2016 WL 7324987 (N.D. Cal. Dec.16, 2016); *United States v. Hammond*, No. 16-cr-102, 2016 WL 7157762 (N.D. Cal. Dec. 8, 2016); *United States v. Duncan*, No. 15-cr-414, 2016 WL 7131475 (D. Or. Dec. 6, 2016); *United States v. Owens*, No. 16-cr-38-JPS, 2016 WL 7053195 (E.D. Wisc. Dec. 5, 2016); *United States v. Tippens, et. al.*, No. 16-cr-5110 (W.D. Wa. Nov. 30, 2016); *United States v. Stepus*, No. 15-cr-30028, 2016 WL 6518427 (D. Mass. Oct. 28, 2016); *United States v. Libbey-Tipton*, No. 16-cr-236 (N.D. Ohio Oct. 19, 2016); *United States v. Scarbrough*, No. 16-cr-35, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016); *United States v. Allain*, No. 15-cr-10251, 2016 WL 5660452 (D. Mass. Sept. 29, 2016); *United States v. Anzalone*, No. 15-cr-10347, 2016 WL 5339723 (D. Mass. Sept. 22, 2016); *United States v. Broy*, No. 16-cr-10030, 2016 WL 5172853 (C.D. Il. Sept. 21, 2016); *United States v. Ammons*, No. 3:16-cr-00011, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016); *United States v. Knowles*, No. 15-cr-875, 2016 WL 6952109 (D. S.C. Sept. 14, 2016); *United States v. Torres*, No. 16-cr-285, 2016 WL 4821223 (W.D. Tx. Sep. 9, 2016); *United States v. Henderson*, No. 15-cr-565, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *United States v. Adams*, No. 16-cr-011, 2016 WL 4212079 (M.D. Fl. Aug. 10, 2016); *United States v. Acevedo-Lemus*, No. 15-cr-00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Rivera*, No. 2:15-cr-266- CJB-KWR (E.D. La. Jul. 20, 2016); *United States v. Werdene*, No. 15-cr-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *United States v. Michaud*, No. 3:14-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

[6] *See United States v. McLamb*, No. 16-cr-092, 2016 WL 6963046 (E.D. Va. Nov. 28, 2016); *United States v. Lough*, No. 16-cr-18, 2016 WL 6834003 (N.D. W.Va. Nov. 18, 2016); *United States v. Kienast*, No. 16-CR-103, 2016 WL 6683481 (E.D. Wisc. Nov. 14, 2016); *United States v. Mascetti*, No. 16-cr-308 (M.D.N.C. Oct. 24, 2016); *United States v. Johnson*, No. 15-cr-00340, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016); *United States v. Smith*, No. 15-cr- 00467 (S.D. Tx. Sept. 28, 2016); *United States v. Jean*, No. 15-cr-50087, 2016 WL 4771096 (W.D. Ark. Sep. 13, 2016); *United States v. Eure*, No. 2:16-cr-43, 2016 WL 4059663 (E.D. Va. Jul. 28, 2016); *United States v. Matish*, No. 4:16-cr-16, 2016 WL 3545776 (E.D. Va. June 23, 2016); *United States v. Darby*, No. 2:16-cr-36, 2016 WL 3189703 (E.D. Va. June 3, 2016); *United States v. Epich*, No.15-cr-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016).

[7] *See United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Arterbury*, No. 15-cr-182-JHP (N.D. Okla. May 17, 2016); *United States v. Workman*, No. 15 -cr-397 (D. Co. Sep. 6, 2016); *United States v. Croghan* (consolidated order), Nos. 15-cr-48;15-cr-51, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016).

resulting need to use complex hacking procedures to discover and identify the perpetrators of online crimes.

Properly stated, the question here is whether the FBI's NIT warrant so exceeded the limits of the magistrate judge's jurisdiction and authority or reasonable behavior by law enforcement as to require suppression to deter similar actions in the future. Although the NIT warrant exceeded the scope of Rule 41(b) as it existed at the time, the FBI's actions in investigating and closing Playpen were reasonable and directed toward securing the judicial review of law enforcement which the Fourth Amendment contemplates. Given the circumstances, suppression is not appropriate.

1.

None of the three bases in Rule 41(b) provided jurisdiction for the magistrate judge to approve the warrant. Rule 41(b)(1) cannot serve as the basis for jurisdiction. Under that provision, a magistrate judge can issue a warrant to seize property "located in the district." Here, the server housing Playpen had been transported to Virginia by the FBI, but the NIT involved the transmission of information from that server to computers located around the country and then back to the server. The relevant information (or "property"[8]) was the information requested by the NIT from the user's computer. The NIT cannot be reasonably construed as seizing information "located in the district" even if the request for the information originated from a server in Virginia.

Likewise, Rule 41(b)(2) is an insufficient basis for jurisdiction. The Government attempts to argue that the NIT was initiated only when a user attempted to access Playpen (and thus electronically "entered" Virginia). For substantially the same reasons Rule 41(b)(1) does not

[8] Rule 41(a)(2)(A) defines "property" to include "tangible objects" and "information."

apply, Rule 41(b)(2) does not. This is not a scenario where the property sought by the warrant was within the Magistrate's jurisdiction at the time of approval but moved before law enforcement could seize the property. Rather, the NIT was necessary because the users accessing Playpen were located in other, unknown districts. Even if Kahler had some contact with the Playpen server located in Virginia, the information sought by the NIT was all located in Michigan. The mere fact that the information from outside the district was brought into the district cannot satisfy Rule 41(b)(2). If that scenario was sufficient, then there would effectively be no jurisdictional limit on warrants for seizure of personal property, because property can typically be moved. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) ("Note that (b)(2) does not authorize a warrant . . . for property outside the district when the warrant is issued, but brought back inside the district before the warrant is executed. . . . If such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found.").

Rule 41(b)(4) comes closest to providing a jurisdictional basis for the warrant. Indeed, courts which have found that the NIT warrant complied with Rule 41 typically rest their analysis on subsection (b)(4). That section allows a magistrate judge to authorize use of a tracking device, if installed within the district, to track property outside the district. A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). There is a reasonable argument that the language of Rule 41(b)(4) should be read to encompass NIT software like the FBI used here. The NIT was "installed" on the Playpen server and then retrieved information from computers which accessed

that server. Further, the NIT does not actually "install" a program on the user's computer (in the sense that nothing was left behind on the computer after the NIT finished), it simply requests and receives information. For several reasons, however, this interpretation of Rule 41(b)(4) goes too far. To begin with, the NIT provided law enforcement with more than just location information. As described above, the NIT requested the computer's IP address, operating system, *operating system username*, and network adapter address. The Government admits that the "network information was not itself location information." Gov't Resp. Br. at 11, ECF No. 27. The receipt of the username associated with the computer's operating system goes beyond simple location data to descriptive data regarding the identity of the user. The NIT is more than just a "tracking device"; it is a surveillance device.

Additionally, the entire purpose of the NIT was to interact with a computer and obtain information that was located in another district. Even though the NIT was nominally installed on the Playpen Server, the NIT's "tracking" functionality occurred in other districts. Finally, the purpose of the NIT was to *discover* the location of the users accessing Playpen, not track their movement. The plain language of Rule 41(b)(4) most clearly applies to situations where the property to be tracked has been located (and is within the district), but law enforcement wishes to track its movement. In contrast, the "property" sought here had not been located and the FBI knew that it was not, at least for the most part, within the district. This distinction between discovering the location of an internet user and tracking movement of property illustrates the unsuitability of Rule 41, as it existed at the time of the NIT warrant, for internet investigations. But the unique challenges created by internet investigations do not justify torturing the language of Rule 41(b)(4) to make the warrant lawful *ex post facto*.

2.

The Government argues that, even if the NIT warrant exceeded the scope of Rule 41(b), the magistrate judge possessed inherent power to issue the search warrant. District judges do have inherent power to issue warrants consistent with the Fourth Amendment. *See United States v. Torres*, 751 F.2d 875, 878 (7th Cir. 1984). But there is dispute regarding whether magistrate judges, as opposed to district court judges, possess that inherent authority. *Compare Torres*, 751 F.3d at 878, *with United States v. Levin*, 186 F. Supp. 3d 26, 43 (D. Mass. 2016) (collecting cases). The Court declines to rely on the magistrate judge's purported power to issue warrants to uphold the NIT warrant independent of Rule 41. Although there is some support for the proposition that Rule 41 should be read broadly, *see United States v. N.Y. Tel. Co.*, 434 U.S. 159, 170 (1977), the fact that the NIT warrant exceeded the scope of Rule 41(b) weighs against a finding of inherent authority to issue it. Federal judges, especially federal magistrate judges, preside over courts of limited jurisdiction. Given the uncertainty regarding whether magistrate judges possess inherent authority to issue warrants at all, a broad extension of their geographical authority to issue warrants based on "inherent" power would be unsound. Regardless, because the Court finds (as discussed below) that suppression is an inappropriate remedy, this order does not rest on a finding that the Virginia Magistrate Judge had the inherent authority to issue the warrant.

3.

The Government alternatively argues that, even if the warrant could not have been properly issued under Rule 41(b), the NIT search could have been conducted without a warrant. In making this argument, the Government relies on the consensus among the Federal Courts of Appeal that there is no constitutionally recognizable privacy interest in an IP address. *See e.g.*, *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016). These holdings arise out of the

"third-party doctrine": "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). That doctrine cannot reasonably be applied here. To begin with, the information the NIT obtained from the computers it contacted included more than just locational data. *See* Carpenter, 819 F.3d at 888 (holding that "locational information" contained in cell-site records were not protected under the Fourth Amendment because it was created and maintained by wireless carriers). Rather, the NIT also directly procured information, including the operating system on the computer and operating system username, which had not been voluntarily provided to third parties. More importantly, every person who accessed Playpen had availed themselves of the Tor-routing software. Tor is free software that was originally developed by the United States Government and now is distributed and supported by a volunteer organization. *See* https://www.torproject.org/index.html.en. The entire purpose of the software is to conceal internet users from unwanted online surveillance. Although the individuals accessing Playpen to view child pornography were using the Tor software for heinous purposes, the software could also be used for legitimate purposes. Given the rise of "targeted" online advertisements which use observed information about the user's online habits to individually tailor advertisements, a desire for online anonymity is neither unreasonable nor suspicious.

The Government argues that, despite using a software which exists only to veil the user's IP address from prying eyes, the user has no reasonable privacy interest in his or her IP address. This argument has little to recommend it. If a user who has taken special precautions to hide his IP address does not suffer a Fourth Amendment violation when a law enforcement officer compels his computer to disclose the IP address, the operating system, the operating system username, and other identifying information, then it is difficult to imagine *any* kind of online

activity which is protected by the Fourth Amendment. Internet use pervades modern life. Law enforcement, acting alone, may not coerce the computers of internet users into revealing identifying information without a warrant, at least when the user has taken affirmative steps to ensure that third parties do not have that information. *See generally Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (holding that police may not search a cell phone incident to arrest without obtaining a warrant because cell phone usage "can form a revealing montage of the user's life").

4.

Kahler also argues that the NIT warrant did not satisfy the Fourth Amendment's particularity requirement. Because resolution of the issue may impact the analysis of whether suppression is justified, this argument will be briefly addressed. The Fourth Amendment specifies that warrants must particularly describe the place to be searched. This requirement is meant to prevent "'general searches by requiring a neutral judicial officer to cabin the scope of the search to those areas and items for which there exists probable cause that a crime has been committed.'"

United States v. Richards, 659 F.3d 527, 537 (6th Cir. 2011) (quoting *Baranski v. Fifteen Unknown Agents of the Bureau of Alcohol, Tobacco and Firearms*, 452 F.3d 433, 441 (6th Cir. 2006)).

According to Kahler, the warrant application was impermissibly broad because it "failed to explain how the government planned to avoid searching the activities of innocent computer users." Mot. Supp. at 19, ECF No. 21.[9] Given the circumstances, the magistrate judge could have reasonably found that there was probable cause to search the computer of every user who logged

[9] Kahler does not specifically argue that the scope of the warrant or the explanation of how the NIT would work was unconstitutionally vague. Even if he had, the warrant affidavit sufficiently described how the NIT worked for the magistrate judge to make an informed decision about whether the scope of the warrant corresponded to the degree of probable cause that wrongdoing was occurring.

onto Playpen. As discussed above, the dark web is not indexed. Accordingly, a user could not innocently "stumble" across Playpen. Rather, the user would have to download the Tor-routing software. Then, the user needed to obtain Playpen's exact URL from another source, like a webpage which listed child pornography websites. The name of the website, Playpen, is evocative of children playing. The front page of Playpen featured two different images, both of which pictured prepubescent girls wearing sexually provocative clothing and posed suggestively. Given the difficulty of finding the website, the website's name, and the images on the front page, it is difficult to imagine someone accessing the front page without knowledge of the website's content. Further, the NIT was triggered only when a user *logged into* Playpen. As explained above, the registration page involved several statements advising users on how to ensure total anonymity on the site. The registration page also disclaimed responsibility for any content posed on the site. When the entirety of the circumstances are considered, it is questionable whether any user could log into Playpen without providing probable cause for law enforcement to believe they intended to view child pornography. Kahler has not shown a significant enough likelihood of "innocent users" being swept up in the FBI's operation to raise constitutional concerns.

B.

Although Rule 41(b) did not provide express authorization for the warrant, the suppression remedy has no place here. In *United States v. Master*, the Sixth Circuit held that the good faith exception can apply even when a warrant is void *ab initio* because it was issued by a judge who lacked jurisdiction. 614 F.3d 236, 241 (6th Cir. 2010). The *Master* Court explained that "[i]ntentional attempts to avoid adhering to jurisdictional limitations imposed by state law is conduct that can and should be considered and deterred by the judiciary." *Id.* at 243. However, "if the officers mistakenly, but inadvertently, presented the warrant to an incorrect magistrate,"

then suppression is not warranted. As explained above, the key inquiry is whether "the culpability of the police" and the need "to deter wrongful police conduct" justifies suppression. *Herring*, 555 U.S. at 137.

Despite the novelty of the FBI's investigative techniques here, their conduct does not justify suppression. Kahler argues that the FBI should have known that the NIT warrant exceeded the jurisdictional scope allowed by Rule 41(b). That is an arguable point. As discussed above, some federal courts have held that Rule 41(b)(4) does authorize the warrant at issue here. Under the best interpretation of Rule 41(b)(4), the NIT warrant was improperly issued. But the very fact that some federal courts have concluded the opposite indicates that law enforcement could have reasonably believed that the NIT warrant was properly issued. The FBI should not be faulted for failing to correctly predict the outcome of an intricate, disputed question of federal jurisdiction.

Even more importantly, this is not a case where the FBI purposely avoided compliance with the law. The investigation of Playpen was difficult precisely because the FBI had so little information about the location of the users. If the FBI had known where certain users were located but nevertheless chose to seek a warrant in another district, suppression would be appropriate. In that case, the FBI would have purposely skirted the law despite a legal alternative. Kahler's arguments, if accepted, would imply that the FBI should not have conducted the NIT investigation at all because the users were masking their true location. The FBI's decision to adopt novel tactics to bring individuals distributing child pornography behind location-concealing software to justice is not inherently troubling behavior.

To be sure, the FBI's best intentions in conducting the NIT cannot substitute for a lawful warrant. But this is not a case where law enforcement opted for illegal investigative methods

over legal methods. Rather, the technical investigative tools available to the FBI have advanced to the point where they, at times, defy categorization by courts. The FBI sought and received approval of the investigative technique by a neutral, detached, magistrate judge. That judge might have lacked jurisdiction under Rule 41(b), but, given the lack of a known geographical nexus for the criminal behavior, the FBI's solution to the technological issues posed by the Tor software was reasonable. Because of the FBI's good faith attempt to comply with existing law, despite its incompatibilities with the investigative realities faced, the fruits of the NIT warrant will not be suppressed.

C.

Kahler separately argues that he is entitled to relief pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). Under *Franks v. Delaware*, a defendant has the right to "challenge the sufficiency of an executed search warrant by attacking the veracity of the affidavit supporting the warrant." *U.S. v. Fowler*, 535 F.3d 408 (6th Cir. 2008). A defendant alleging that an officer made material omissions in his affidavit carries a higher burden than a defendant alleging that an officer made false affirmative statements because of the "potential for endless rounds of Franks hearings due to potentially endless conjecture about investigative leads, fragments of information, or other matter that might, if included, have redounded to defendant's benefit." *Id.* at 415-16 (internal quotations and citations omitted). A defendant is entitled to a *Franks* hearing on the basis of alleged material omissions only if: (1) the defendant makes a substantial preliminary showing that the affiant engaged in deliberate falsehood or reckless disregard for the truth in omitting information from the affidavit; and (2) a finding of probable cause would not be supported by the affidavit if the omitted material were considered to be a part of it. *Id.* at 415.

Kahler does not specifically request a *Franks* hearing, and he has not met his burden of demonstrating entitlement to a hearing regardless. Most of Kahler's arguments here fall far short of making a "substantial preliminary showing" of deliberate falsehoods or even reckless disregard for the truth. The Government's refusal to disclose the details of the code used in the NIT, the locations of the computers that the NIT would target, and other information about the exact procedures used by the NIT do not constitute falsehoods. The FBI's attempt to summarize the technical details of the operation in layman's terms is reasonable. Likewise, the FBI cannot be faulted for not disclosing the locations of the computers the NIT would target, considering the purpose of the NIT was to identify those locations.

Only three of Kahler's arguments that a *Franks* violation occurred merit further discussion. First, Kahler argues that the NIT warrant did not disclose the fact that the image on the front page of Playpen changed on February 19, 2015, just before the affidavit was submitted. However, the differences between the two images were largely irrelevant for purposes of assessing probable cause. Both depicted young girls wearing sexually provocative clothing and posed suggestively. There was probable cause to believe that users who logged into Playpen were seeking child pornography even without considering the front page images, and both images supported that conclusion. Thus, the FBI's failure to indicate that the front page image had recently changed on its affidavit for the warrant was not a material omission.

Kahler also argues that the FBI improperly described Playpen as being dedicated only to child pornography. In fact, Kahler argues, it also included erotic fiction subforums and a chat messaging system. However, the warrant indicated that the chat system was used to relive real-world abuse of children by the Playpen users. Given the content on the remainder of the site, it seems exceedingly likely that the erotic fiction also featured child abuse. Playpen likely included

a small amount of legal (though child-related) content, but Kahler does not dispute that the large majority of the site was devoted to child pornography. There is no basis for a *Franks* hearing on this issue.

Finally, Kahler argues that, contrary to the representations in the warrant, several dark web search engines exist and Playpen could have been accessed by them. Kahler contends that these search engines exist, but does not corroborate his assertion that Playpen was specifically accessible through such a search engine. Even assuming that to be the case, however, accessing Playpen still required a number of affirmative steps—including downloading the Tor software, viewing the homepage, and registering an account—which are indicative of a person seeking child pornography. Even taking Kahler's largely unproven assertions as true, they were not material to the probable cause finding. Kahler has not demonstrated entitlement to a *Franks* hearing.

IV.

Accordingly, it is **ORDERED** that Defendant Kahler's motion to suppress, ECF No. 21, is **DENIED.**

Dated: February 14, 2017

s/Thomas L. Ludington
THOMAS L. LUDINGTON
United States District Judge

PROOF OF SERVICE

The undersigned certifies that a copy of the foregoing order was served upon each attorney or party of record herein by electronic means or first class U.S. mail on February 14, 2017.

s/Michael A. Sian
MICHAEL A. SIAN, Case Manager