UNITED STATES OF AMERICA,
v.
GERALD ANDREW DARBY.

2016 WL 3189703
United States District Court, E.D. Virginia.

Signed June 3, 2016

OPINION AND ORDER

ROBERT G. DOUMAR, UNITED STATES DISTRICT JUDGE

***1** This matter comes before the Court on Two Motions to Suppress filed by Gerald Andrew Darby ("Defendant"). ECF Nos. 15, 18. For reasons set forth below, the Court **DENIES** Defendant's First Motion to Suppress, ECF No. 15, and **DENIES** Defendant's Second Motion to Suppress, ECF No. 18.

I. BACKGROUND

The instant prosecution is the result of an FBI investigation into a website that facilitated the distribution of child pornography. The government seized control of this website and for a brief period of time operated it from a government facility in the Eastern District of Virginia. Both Motions to Suppress seek to exclude all evidence obtained as the result of a search warrant that allowed the government to use the website to remotely search the computers of individuals who logged into the website.

The following summary is provided as way of background. There is not yet any evidentiary record in this case, but the basic details of the investigation are not in dispute. Most of the information summarized here has been drawn from the warrant application, Appl. for a Search Warrant ("Warrant Appl."), ECF No. 16-1, specifically the affidavit in support of the warrant sworn to by FBI Special Agent Douglas Macfarlane. Aff. in Supp. of Appl. for Search Warrant ("Aff., Warrant Appl.,"), ECF No. 16-1 at 6. Additional details undisputed by the parties in their briefing are included mainly to fill out the narrative. For instance, neither the warrant nor warrant application identify the website and both refer to it simply as "TARGET WEBSITE." See Aff., Warrant Appl., ¶ 4. As explained in the affidavit in support of the warrant, at the time the warrant application was submitted the website was still active. Id. ¶ 2 n.1. The government was concerned that disclosure of the name of the website in the application would alert potential users of the site to the government's investigation and thus undermine it. Id. At present, the government has since ceased operation of the website, and the name of the website has been widely reported.[1] Both parties refer to the website by its name: Playpen.

Playpen operated on the Tor network, which provides more anonymity to its users than the regular Internet.[2] Aff., Warrant Appl., ¶¶ 7–8. The Tor network was developed by the U.S. Naval Research Laboratory and is now accessible to the general public. Id. ¶ 7. Users of the Tor network must download special software that lets them access the network. Id. Typically, when an individual visits a website, the website is able to determine the individual's Internet Protocol ("IP") address. See id. ¶ 8. An individual's IP address is associated with a particular Internet Service Provider ("ISP") and particular ISP customer. Id. ¶ 35. Because internet access is typically purchased for a single location, an IP address may be used by law enforcement to determine the home or business address of an internet user. See id. When a user accesses the Tor network, communications from that user are routed through a system of network computers that are run by volunteers around the world. Id. ¶ 8. When a user connects to a website, the only IP address that the website "sees" is the IP address of the last computer through which the user's communications were routed. Id. This final relay is called an exit node. Id. Because there is no practical way to trace a user's communications from the exit node back to the user's computer, users of the Tor network are effectively anonymous to the websites they visit. Id.

***2** The Tor network also provides anonymity to the individuals who run websites or forums on it. Id. ¶ 9. Websites may be set up on the Tor network as "hidden services." Id. A hidden service may only be accessed through the Tor network. Id. A hidden service functions much like a regular website except that its IP address is hidden. Id. The IP address is replaced with a Tor-based address which consists of a series of alphanumeric

characters followed by ".onion." Id. There is no way to look up the IP address of the computer hosting a hidden service. Id.

A user of the Tor network cannot simply perform a search to find a hidden service that may interest the user. Id. ¶ 10. In order to access a hidden service a user must know the Tor-based address of the hidden service. Id. As a result, a user cannot simply stumble onto a hidden service. Id. The user may obtain the address from postings on the Internet or by communications with other users of the Tor network. Id. One hidden service may also link to another. See id. Playpen was a hidden service contained on the Tor network, and it had been linked to by another hidden service that was dedicated to child pornography. Id.

Of importance to the First Motion to Suppress is the homepage of the Playpen site. See Def.'s First Mot. to Suppress ("First Mot."), ECF No. 15 at 2–3. In the warrant application, the homepage is said to contain "images of prepubescent females partially clothed and whose legs are spread." Aff., Warrant Appl., ¶ 12. The censored version of the exact images has been attached to the briefing. ECF No. 16-2. There appears to have just been two photographs on the home page. The images show two young girls in the attire and pose described. Id. The images of these children appear at the top of the homepage and flank a large image of the site's name, Playpen. Id. Although these images were at an earlier point on the homepage, the parties agree that at the time the warrant was signed, on February 20, 2015 at 11:45 am, a different image confronted users to the site. First Mot. at 9; Gov't's Resp. to Def.'s First Mot. to Suppress ("Gov't's Resp. to First Mot."), ECF No. 16 at 14. A censored version of this image has also been included in the briefing. ECF No. 16-3. It shows 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. Id. Her image is to the left of the site name. Id.

The government claims that the images must have changed shortly before the warrant was signed. Gov't's Resp. to First Mot. at 14. In the affidavit in support of the warrant, Special Agent Macfarlane recounts that FBI agents reviewed the Playpen website from September 16, 2014 to February 3, 2015. Aff., Warrant Appl., ¶ 11. The screenshot of the home page that was included in the government's brief and contains the images of the two young girls was taken on February 3, 2015. ECF No. 16-2. The date is visible in the lower right corner of the screen. Id. The affidavit further states that sometime between February 3, 2015 and February 18, 2015, the Tor address of the site was changed. Warrant Appl. ¶ 11 n.1. Special Agent Macfarlane states in his affidavit that after the address change he "accessed the TARGET WEBSITE in an undercover capacity at its new URL, and determined that its content had not changed." Id. In its briefing the government asserts that this statement confirms that the homepage of Playpen was as described in the warrant application on February 18, 2015, two days before the warrant was sworn and signed. Gov't's Resp. to First Mot. at 14–15.

***3** The homepage also provided users with instructions on how to join and then log into the site. Aff., Warrant Appl., ¶ 12. Users had to register with the site before going any further into the site. Id. Users were instructed to enter a phony email address and to create a login name and password. Id. ¶ 13. The instructions also informed users that staff and owners of the site were unable to determine the true identity of users and that the website could not see the IP addresses of users. Id.

Once registered and logged into the site users had access to numerous sections, forums, and sub-forums where they could upload material and view material uploaded by others. Id. ¶ 14. For instance under the heading "Playpen Chan"[3] are four subcategories: "Jailbait—Boy," "Jailbait—Girl," "Preteen—Boy," and "Preteen—Girl." Id. Special Agent Macfarlane, based on his training and experience, explains that "jailbait" refers to underage but post-pubescent minors. Id. ¶ 14 n.4. Other forum and sub-forum categories on the site include "Jailbait videos," "Family Playpen—Incest," "Toddlers," and "Bondage." Id. ¶ 14. Not surprisingly, a review of the contents of these forums revealed that the majority of content was child pornography. Id. ¶ 18. The warrant application has several specific examples of the reprehensible material contained on the site. Id. ¶¶ 18, 23–25. Additionally, there was a section of the site that allowed members of the site to exchange usernames on a Tor-based instant messaging service known to law enforcement to be "used by subjects engaged in the online sexual exploitation of children." Id. ¶ 15.

In December of 2014, a foreign law enforcement agency informed the FBI that it suspected that a United States-based IP address was the IP address of Playpen. Id. ¶ 28. In January 2015, after obtaining a search warrant, the FBI seized the IP address and copied the contents of the website. Id. ¶ 28. On February 19, 2015 the FBI arrested the individual suspected of administering Playpen. Id. ¶

30.

The FBI desired to continue to operate Playpen for a limited time so as to identify individuals who logged into the site and who were likely to possess, distribute, or produce child pornography. Id. ¶ 30. The FBI would operate the site from a location in the Eastern District of Virginia. Id. ¶ 33. As mentioned above, normally a website administrator is able to determine the IP addresses of those individuals that visit the site. However, on the Tor network the website administrator is only able to determine the IP address of the exit node, which it not the IP-address of the visitor to the website. To determine the IP addresses of individuals who logged into Playpen, the FBI sought a warrant from a magistrate judge in the Eastern District of Virginia, Alexandria division, that would allow it to deploy a Network Investigative Technique ("NIT"). Id. ¶ 31.

According to the FBI in its warrant application, when an individual visits a website the website sends "content" to the individual. Id. ¶ 33. This content is downloaded by the individual's computer and used to display the webpage on the computer. Id. A NIT "augments" the content with additional instructions. Id. The NIT deployed in the instant case instructed the computers of those individuals who logged into Playpen to send to a computer "controlled by or known to the government" certain information. Id. The information that the NIT would instruct the computers to send is described in an attachment to the warrant application. Attach. B, Warrant Appl., ECF No. 16-1 at 5. The NIT extracted from any "activating computer"—a computer that logged into Playpen using a username and password—(1) the IP address of the computer and the date and time this information is determined, (2) a unique identifier that distinguishes the data from this activating computer from that of others, (3) the type of operating system used by the computer, (4) information about whether the NIT has already been sent to the computer, (5) the computer's Host Name, (6) the computer's operating system user name, and (7) the computer's media access control ("MAC") address. Id.

***4** On February 20, 2016 at 11:45 am, Magistrate Judge Theresa Carroll Buchanan of the United States District Court for the Eastern District of Virginia, Alexandria Division, issued the requested warrant. Warrant Appl., ECF No. 16-1 at 39. The warrant permitted the FBI to run Playpen from a location in the Eastern District of Virginia for thirty (30) days and to deploy a NIT from the website. Id. at 37–39. The NIT would instruct any computer that logged into Playpen with a username and password to send the just described information. Id. at 37–38.

According to the briefing of the defendant, Gerald Andrew Darby ("Defendant"), on or about February 27, 2015, the NIT on the Playpen website sent instructions to Defendant's computer.[4] First Mot. at 10. The FBI identified Defendant's IP address and issued an administrative subpoena to his ISP, Verizon. Id. at 10–11. Verizon provided Defendant's name, subscriber information, and address to the government. Id. On January 4, 2016, a warrant to search Defendant's home was issued by Magistrate Judge Robert J. Krask. Id. at 11. FBI agents searched Defendant's home on January 7, 2016 and seized computers, hard drives, cell phones, tablets, video game systems, and other property. Id. According to the government, Defendant was present during the search and agreed to be interviewed. Gov't's Resp. to First Mot. at 7. During this interview Defendant admitted to downloading sexually explicit images of minors for the past three to four years. Id. The government also relates that forensic analysis found that Defendant possessed 1,608 images and 298 videos of child pornography. Id.

On March 10, 2016 a grand jury returned an indictment charging Defendant with five counts of Receipt of Images of Minors Engaging in Sexually Explicit Conduct in violation of 18 U.S.C. § 2252(a)(2) and three counts of Possession of Images of Minors Engaging in Sexually Explicit Conduct in violation of 18 U.S.C. § 2252(a)(4)(B). ECF No. 1. Defendant filed his First Motion to Suppress on April 13, 2016. ECF No. 15. The government filed its Response in Opposition on April 27, 2016. ECF No. 16. Defendant filed his Second Motion to Suppress on May 3, 2016, and the government responded to this motion of May 9, 2016. ECF Nos. 18, 22. A hearing on both motions was held on May 10, 2016. Hr'g, ECF No. 24.

II. DEFENDANT'S MOTIONS TO SUPPRESS

Both of Defendant's Motions to Suppress challenge the warrant, issued by Magistrate Judge Theresa Buchanan, which authorized the deployment of the NIT through the government's administration of the Playpen website. Because the second warrant, which authorized the search of Defendant's home, was issued on account of information gathered pursuant to the NIT Warrant, Defendant seeks to suppress all evidence obtained during the search of his home.

A. WAS DEPLOYMENT OF THE NIT A FOURTH AMENDMENT SEARCH?

Before reaching the merits of Defendant's motions, it will be useful to address a preliminary question unaddressed by the parties: Was the deployment of the NIT a "search" of Defendant's computer within the meaning of the Fourth Amendment? If the use of the NIT was not a search, the Fourth Amendment was not implicated, no warrant was required, and any violation of Rule 41(b) irrelevant. See Kyllo v. United States, 533 U.S. 27, 31, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (referring to the "antecedent question whether or not a Fourth Amendment 'search' has occurred").

***5** The government in its response to Defendant's First Motion to Suppress never argues that no warrant was required because deployment of the NIT was not a Fourth Amendment search. See Gov't's Resp. to First Mot. at 15–38. In failing to raise this argument when it would have been appropriate, the government has likely waived it. The government does, in justifying the scope of the warrant, argue that Defendant had no reasonable expectation of privacy in his IP address, even though he was using the Tor network. Id. at 33–34. However, the government never pushes this point to its possible conclusion: that the use of the NIT was not a Fourth Amendment search because Defendant had no expectation of privacy in the information obtained by the NIT. Similarly, the government, in a recent filing, has drawn the Court's attention to a recent case from the Eastern District of Pennsylvania, United States v. Werdene, No. 2:15–cr–434–GJP, ECF No. 33, —— F.Supp.3d ——, 2016 WL 3002376 (E.D.Pa. May 18, 2016). In Werdene, the district court discussed whether the alleged Rule 41(b) violation was constitutional or procedural, a distinction that will be explained below. Id. at 14–20. In determining that the violation was not constitutional, the district court held that users of the Tor network have no reasonable expectation of privacy in their IP addresses. Id. However, the district court did not—perhaps because not urged to by the government—hold that because Tor users had no reasonable expectation of privacy in their IP address, no warrant was necessary to deploy the NIT and therefore any violation of rule 41(b) irrelevant. See id.

It will be instructive to explore fully whether the deployment of the NIT was a Fourth Amendment search. In deciding this question the Court will have to analyze just how a NIT works. Doing so will elucidate the privacy concerns raised by the NIT and clarify what is and is not at stake in this case. The discussion will also aid the analysis below concerning a possible violation of Rule 41(b).

A Fourth Amendment search occurs when "the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." Smith v. Maryland, 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) (collecting cases). The classic analysis of this rule comes from Justice Harlan, who explained that there are two components to a reasonable expectation of privacy: "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, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring). In more recent years the Supreme Court has recognized, or reiterated, that a search may also occur when the government trespasses upon the areas—"persons, houses, papers, and effects"—enumerated in the Fourth Amendment. United States v. Jones, —— U.S. ——, 132 S.Ct. 945, 950, 181 L.Ed.2d 911 (2012).

The government contends that Defendant had no reasonable expectation of privacy in his IP address even though he was using the Tor network, which is designed to shield the IP addresses of its users. The government does not address whether Defendant had a reasonable expectation of privacy in the other information gathered by the NIT, such as the type of operating system on Defendant's computer and his computer's Host name. But this piecemeal analysis of what this NIT was authorized to extract from Defendant's computer misses the mark. The NIT surreptitiously placed code on Defendant's personal computer that then extracted from the computer certain information. See Aff., Warrant Appl., ¶ 33. In placing code on Defendant's computer, the NIT gave the government access to the complete contents of Defendant's computer. The relevant inquiry is whether Defendant has a reasonable expectation of privacy in the contents of his personal computer, which was located in his home.

Several Courts of Appeals, including the Fourth Circuit, have held that individuals generally have a reasonable expectation of privacy in the contents of their home computers. Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir.2001); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir.2004); Guest v. Leis, 255 F.3d 325, 333 (6th Cir.2001). Individuals' subjective expectation of privacy

in their computers is apparent from the mass of personal and financial information often contained on computers. This widespread practice is also evidence that society is prepared accept this subjective expectation of privacy. To be sure, personal computers are vulnerable to hacking when connected to the internet, just as homes are vulnerable to break-ins. This criminality is not enough to defeat an individual's reasonable expectation of privacy. The prohibition against hacking is itself proof of society's acceptance of the privacy expectations of personal computer users. See 18 U.S.C. § 1030(a)(2)(C).

***6** A recent Supreme Court case supports considering whether Defendant had a reasonable expectation of privacy in the contents of his computer rather than in the specific information the NIT commanded the computer to transmit. In Riley v. California, the Court considered "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." —— U.S. ——, 134 S.Ct. 2473, 2480, 189 L.Ed.2d 430 (2014). The Court held that the police generally may not.[5] Id. at 2485. The Court rejected a suggestion by the United States that police could at the very least access the call records contained in an arrestee's cell phone. Id. at 2492–93. The United States had pointed out that the Court had held in Smith v. Maryland that individuals do not have a reasonable expectation of privacy in the phone numbers they dial. 442 U.S. 735, 745, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). There was no reasonable expectation of privacy because individuals voluntarily convey the numbers they dial to the phone company. Id. at 742–44, 99 S.Ct. 2577. The Court in Riley distinguished Smith by noting that the ultimate holding in Smith was that the government's use of a pen register in that case was not a search under the Fourth Amendment. Riley, 134 S.Ct. at 2492. A pen register is a limited technology that can only record the phone numbers dialed by an individual. Smith, 442 U.S. at 740–41, 99 S.Ct. 2577. By contrast, the Court in Riley said that it was undisputed that accessing the information in an individual's cell phone is a search. 134 S.Ct. at 2492–93. It was irrelevant that the individual might not have a reasonable expectation of privacy in the information actually obtained. See id.

Likewise, if an individual has a reasonable expectation of privacy in the contents of his or her personal computer, as he or she does, and the deployment of the NIT invades that privacy, then the NIT is a search. The NIT in this case caused Defendant's computer to download certain code without the authorization or knowledge of Defendant. The "contents" of a computer are nothing but its code. In placing code on Defendant's computer, the government literally—one writes code—invaded the contents of the computer. Additionally, the code placed on Defendant's computer caused Defendant's computer to transmit certain information without the authority or knowledge of Defendant. In this manner the government seized the contents of Defendant's computer. Just as in Riley, it is irrelevant that Defendant might not have a reasonable expectation of privacy in some of the information searched and seized by the government. The government's deployment of the NIT was a Fourth Amendment search.

B. DEFENDANT'S FIRST MOTION TO SUPPRESS

In his First Motion to Suppress Defendant raises several related grounds for suppressing the fruits of the search executed pursuant to the NIT Warrant. First, he argues that the warrant was not supported by probable cause. First Mot. at 2. Second, he argues the FBI, either intentionally or recklessly, misled the warrant issuing court with its description of Playpen's homepage and demands a Franks hearing on this issue. Id. at 2–3; see Franks v. Delaware, 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978). Third, he argues that the NIT Warrant was an anticipatory warrant and that the triggering event establishing probable cause did not occur. First Mot. at 3.

1. Legal Principles

The Fourth Amendment requires that searches and seizures be reasonable. Riley, 134 S. at 2482 (citing Brigham City v. Stuart, 547 U.S. 398, 403, 126 S.Ct. 1943, 164 L.Ed.2d 650 (2006)). Generally, the reasonableness requirement of the Fourth Amendment requires that law enforcement obtain a judicial warrant before performing a search or seizure. Id. (citing Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995)). An application for a search warrant must provide a basis for a magistrate to find that there is probable cause for a search. See United States v. Gary, 528 F.3d 324, 328 (4th Cir.2008). There is probable cause for a search when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." Ornelas v. United States, 517 U.S. 690, 696, 116 S.Ct. 1657, 134 L.Ed.2d

911 (1996). This standard "is a 'practical, nontechnical conception.' " Illinois v. Gates, 462 U.S. 213, 231, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983) (quoting Brinegar v. United States, 338 U.S. 160, 176, 69 S.Ct. 1302, 93 L.Ed. 1879 (1949)). It depends on the considerations of everyday life which inform the decisions of reasonable and prudent men and women. Id.

***7** Probable cause does not require that there be an "absolute certainty" that evidence of a crime will be found. Gary, 528 F.3d at 327. Rather, it requires that there is a "fair probability" that such evidence will be found. Gates, 462 U.S. at 238, 103 S.Ct. 2317. Because "[r]easonable minds frequently may differ on the question whether a particular affidavit establishes probable cause" the Supreme Court has instructed district courts to accord " 'great deference' to a magistrate's determination" of probable cause. United States v. Leon, 468 U.S. 897, 914, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984) (citing Spinelli v. United States, 393 U.S. 410, 419, 89 S.Ct. 584, 21 L.Ed.2d 637 (1969)). A reviewing court does not perform a *de novo* review of the magistrate's finding of probable cause but only determines whether there was substantial evidence in the record in support of the magistrate's finding. Massachusetts v. Upton, 466 U.S. 727, 728, 104 S.Ct. 2085, 80 L.Ed.2d 721 (1984) (*per curiam*).

2. Analysis

The warrant allowed the government to place the NIT on the computers of anyone who registered and logged into the site. The legal analysis of each of Defendant's three grounds for suppression ultimately turns on a single issue: Were those individuals who registered and logged into the website aware that the site contained child pornography? If they were, their computers likely contained child pornography and a search of their computers supported by probable cause. Defendant argues that some individuals might have "innocently" logged into the site in the hope of finding legal—though perhaps repugnant—content such as nude photographs of children that do not qualify as pornography or pornography involving teenagers that have reached the age of majority. See First Mot. at 10 (mentioning legal child erotica); 12 (noting that all depictions of naked children are not pornography); 17 (discussing the repugnant but legal content available on the internet). Because not all of those who registered with the website would have been seeking child pornography, Defendant argues that the warrant was not supported by probable cause. As will be explained below, Defendant's other grounds for suppression in his First Motion to Suppress depend upon this central contention.

In arguing that there was no probable cause, Defendant places a great deal of emphasis on the difference between the homepage of Playpen as described in the warrant and as it existed when the warrant was executed. First Mot. at 13. It is undisputed that when the warrant was executed the image on the top of the homepage by the site's name was different than the two images described in the warrant application. The warrant application describes images of two prepubescent girls, on each side of the site name, with their underwear exposed and their legs spread. The homepage when the warrant was executed contained a single image, to the left of the site name, of a possibly older child with her legs crossed. According to Defendant, it was critical for the finding of probable cause that the Playpen homepage "displayed 'partially clothed prepubescent females with their legs spread apart.' " First Mot. at 13 (citing Aff., Warrant Appl., ¶ 12).

At the outset the Court must reject Defendant's contention that the image of the single child was innocuous because she is "fully clothed" and possibly over eighteen. First Mot. at 9. The child is obviously under eighteen and not at all fully dressed. She is wearing a short top or dress and posed provocatively with her upper thigh exposed. ECF No. 16-3. It is unclear whether her dress or top is capable of reaching below the line of her stockings. Nevertheless her outfit is inappropriate for her age and strongly suggestive. To the extent one can or should differentiate among sexualized depictions of children, the images of the two girls that were previously on the homepage are more reprehensible. But that distinction does not subtract from the sexualized nature of the single image of child erotica that appeared on the homepage during the period in which the government operated Playpen. Either version of the homepage supports a finding of probable cause.

***8** From the homepage, users could access a page that let them register for the site. Aff., Warrant Appl., ¶ 13. Users were then prompted with a message that informed them that the site administrators would be unable to identify registered visitors to the site. Id. This promise of anonymity alone did not establish probable cause to search the computers of those who visited the site. However, it does support the magistrate judge's determination that there was probable cause. Those looking for illegal content would be encouraged by this promise while those believing that the site contained legal material may have been warned of the reprehensible

content within.

Furthermore, the homepage and logon process of Playpen are not the only basis for finding that the warrant was supported by probable cause. The warrant application contains detailed information about the illegal content available on the Playpen website. Aff., Warrant Appl., ¶¶ 14–27. Whatever legal content may have been available there, the abundance of child pornography available more than establishes probable cause to search the computers of visitors who knew about the site's contents. The warrant application asserts that, because sites on the Tor network are not searchable with the same ease that sites on the traditional internet are, most visitors to Playpen must have been told of site's online address and knew of the content of the site before registering. Id. ¶ 10. Defendant refutes this and identifies both a search engine and index of sites on the Tor network. First Mot. at 16. Defendant claims that one could find Playpen when searching for sites containing sexually explicit content that was not child pornography. Id. The government counters by noting that the search engine identified by Defendant filters out sites containing child abuse. Gov't's Resp. to First Mot. at 18. Additionally, the warrant application notes that the address for Playpen was listed in a directory contain on another Tor hidden service that was dedicated to child pornography. Aff., Warrant Appl., ¶ 10.

Ultimately, no matter how searchable the Tor network may be, the magistrate judge would have been justified in concluding that those individuals who registered and logged into Playpen had knowledge of its illegal content. The Tor network itself, although it has legitimate uses, is an obvious refuge for those in search of illegal material. At the very least, the Tor network is less searchable than the regular Internet. Defendant fails to explain why someone would go to the trouble of entering the Tor network, locating Playpen, registering for the site, and then logging into the site if they were not looking for illegal content. It is not as if the Internet is not saturated in legal pornography. The magistrate's common sense judgment would justify her finding that an individual would likely only take these steps if he was seeking child pornography and knew he could find it on Playpen.

In sum, the information in the affidavit provided substantial evidence in support of the magistrate's finding that there was probable cause to issue the NIT Warrant. The homepage of the website was suggestive of its content and promised anonymity to registrants. Because the website itself was difficult to find, those who accessed it likely knew of its contents. Although it is not beyond possibility that some of those who logged into Playpen did so without intention of finding child pornography, probable cause requires a fair probability that a search will uncover evidence, not absolute certainty.

Each of Defendant's other grounds for suppression are also without merit, primarily because there was probable cause to issue the NIT Warrant. Defendant asserts that the warrant was overbroad because it authorized searches of every individual that logged into Playpen, potentially "tens of thousands of computers." First Mot. at 23. This argument is curious. As explained above, there was probable cause to search the computers of individuals that logged into Playpen even though some of them might not have been seeking child pornography. The fact that Playpen facilitated rampant criminality does not affect this finding. Defendant compares the NIT Warrant to the general warrants—issued by the English judges against the colonists—that motivated the passage of the Fourth Amendment. See Virginia v. Moore, 553 U.S. 164, 169, 128 S.Ct. 1598, 170 L.Ed.2d 559 (2008) (summarizing the motivations behind the passage of the Fourth Amendment). Comparing this warrant to those outrages trivializes the struggles of the American Revolution and the achievements of the Constitution. 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.

***9** Defendant also requests the Franks hearing based on the change to the Playpen homepage described above. First Mot. at 19–22. In Franks v. Delaware the Supreme Court established two prerequisites that must be satisfied before a defendant is entitled to a hearing on any inaccuracies in an affidavit in support of a warrant application. 438 U.S. at 155–56, 98 S.Ct. 2674. A Franks hearing is required if (1) "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 (2) "the allegedly false statement is necessary to the finding of probable cause" Id. At the hearing if, by a preponderance of evidence, the defendant establishes that the allegedly false statement was made knowingly or with reckless disregard of the truth, and, "with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." Id. at 156, 98 S.Ct. 2674.

Neither of the requirements for a Franks hearing is met in this case. Defendant has failed to make a substantial preliminary showing that the inaccuracies regarding the Playpen homepage were made knowingly or with reckless disregard for the truth. The government took over Playpen on February 19, 2015. Aff., Warrant Appl., ¶ 30. The warrant was signed and executed on February 20, 2015. Warrant Appl. at 39. As discussed in the Background section above, the homepage certainly existed as described in the affidavit on February 3, 2015. The government took a screenshot of the page on that day and has attached it to its briefing. ECF No. 16-2. Additionally, Special Agent Macfarlane accessed the site on February 18, 2015 and found that it had not changed since February 3, 2015. Aff., Warrant Appl., ¶ 3 n.3. Based on the evidence before the Court, the website must have changed between February 18, 2015 and February 19, 2015. There is nothing reckless about relying on a visit to the website on February 18, 2015 when describing the website for a warrant signed and executed on February 20, 2015. Defendant has submitted no evidence that the government knew the site had changed. He merely makes conclusory allegations that the government must have known because they took over the site. First Mot. at 20. This is not enough to entitle Defendant to a Franks hearing.

Additionally, a Franks hearing is not justified because the alleged falsity in the affidavit was not necessary to the finding of probable cause. See United States v. Colkley, 899 F.2d 297, 300 (4th Cir.1990) ("[T]o be material under Franks, an omission must do more than potentially affect the probable cause determination."). As discussed, contrary to the repeated emphasis of Defendant, the images of two prepubescent females described in the warrant application were not necessary to the finding of probable cause. There was an abundance of other evidence before the magistrate judge that supported her finding that there was probable cause to issue the warrant.

Defendant also argues that the warrant was an anticipatory warrant whereby probable cause was established when a user logged into the homepage as described in the warrant application. First Mot. at 25–27. Because the homepage had changed, Defendant argues that this triggering event never occurred. Defendant's argument is again premised on his contention that the images of two prepubescent females were necessary to the finding of probable cause. If probable cause only existed to search the computers of those that registered and logged into Playpen when it contained those images, then the triggering event of the warrant would not have occurred because those images were not on the webpage while the government operated it. However, as discussed, Defendant mischaracterizes the evidence before the magistrate judge in support of her finding of probable cause. Even without those images there was probable cause to search anyone who registered and logged into Playpen. Logging into Playpen was the triggering event, and all the computers searched under the NIT Warrant, including Defendant's, logged into the site.

***10** Because each of the grounds for suppression asserted in Defendant's First Motion to Suppress is without merit, the Court **DENIES** Defendant's First Motion to Suppress. ECF No. 15.

C. DEFENDANT'S SECOND MOTION TO SUPPRESS

In his Second Motion to Suppress Defendant argues that the magistrate judge lacked jurisdiction under the Federal Magistrates Act, which incorporates Federal Rule of Criminal Procedure 41(b), to issue the NIT Warrant. Def.'s Second Mot. to Suppress ("Second Mot.), ECF No. 18 at 2. Because the magistrate judge lacked jurisdiction to issue the warrant, the warrant was issued without lawful authority and void at the outset or *ab initio* in Latin. Id. If the warrant was void, the search of Defendant's computer was performed without a valid warrant in violation of the Fourth Amendment to the Constitution. Because of this alleged constitutional violation Defendant seeks to suppress all fruits of the search performed under the NIT Warrant. In the alternative, Defendant argues that the fruits of the NIT Warrant should be suppressed because he was prejudiced by the alleged violation of Rule 41(b) and because the government's violation of the rule was deliberate. Id.

1. Legal Principles

The Federal Magistrates Act in relevant part provides that

> (a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—
>
> (1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules

> of Criminal Procedure for the United States District Courts;

28 U.S.C. § 636(a). Rule 41(b) of the Federal Rules of Criminal Procedure, which are explicitly incorporated by the Federal Magistrates Act in above text, provides

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> (3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
>
> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
>
> ***11** (A) a United States territory, possession, or commonwealth;
>
> (B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

There are two types of Rule 41 violations: those that involve the constitutional violations and those that do not. United States v. Simons, 206 F.3d 392, 403 (4th Cir.2000). Suppression is warranted for non-constitutional violations of Rule 41 "only when the defendant is prejudiced by the violation or when there is evidence of intentional and deliberate disregard of a provision in the Rule." Id. (internal citations and quotations omitted).

2. Analysis

Defendant's basic argument is simple: nothing in Rule 41(b) allowed the magistrate judge to issue the NIT Warrant. The NIT Warrant allowed the government to utilize the NIT against any computer that logged into the Playpen website. These computers could have been located anywhere in the world. Defendant argues that Rule 41(b) only allows magistrate judges to issue warrants for searches outside of their districts in limited, well-defined circumstances, none of which apply to the facts of the instant case. Second Mot. at 6–11. Of course, Defendant acknowledges that the website was being run from within the Eastern District of Virginia, that the magistrate judge sits in the Eastern District of Virginia, and that Defendant's computer was located in the Eastern District of Virginia when the NIT was deployed. However, according to Defendant, it is irrelevant that magistrate judge could have issued a warrant to search his computer because the warrant was not limited to him or the Eastern District of Virginia. See Second Mot. at 16.

It is understandable why the government sought the warrant in the Eastern District of Virginia. The government planned to run the website from a server located in the district. No district in the country had a stronger connection to the proposed search than this district. Additionally, nothing in Rule 41 categorically forbids magistrates from issuing warrants that authorize searches in other districts—most of its provisions do just that. See Fed. R. Crim. P. 41(b)(2–5). In its briefing the government notes that the Supreme Court has authorized an amendment to Rule 41(b)—to be effective December 1, 2016 absent action from Congress—that explicitly authorizes warrants like the NIT Warrant to be issued by

magistrate judges whose districts have a connection with the criminal activity being investigated.[6] Gov't's Resp. to Def.'s Second Mot. to Suppress ("Gov't's Resp. to Second Mot."), ECF No. 22 at 6; see also ECF No. 22-1, Ex. 1 (a copy of the amendment submitted to congress). The government characterizes this amendment as clarifying the scope of Rule 41(b), and this Court agrees.

***12** In other words, as currently written Rule 41(b) gave the magistrate judge authority to issue the NIT Warrant. Rule 41(b)(4) allows a magistrate judge to issue a warrant for a tracking device to be installed in the magistrate's district. Once installed, the tracking device may continue to operate even if the object tracked moves outside the district. This is exactly analogous to what the NIT Warrant authorized. Users of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government about their location. The magistrate judge did not violate Rule 41(b) in issuing the NIT Warrant.[7]

But even if there were a Rule 41(b) violation, suppression would not be appropriate. Defendant seeks suppression on two related theories. Defendant argues for suppression solely on account of the violation of Rule 41(b) even if it was not of constitutional character. Suppression is warranted for a non-constitutional violation of Rule 41 only if the violation is intentional and deliberate or if the defendant seeking suppression is prejudiced by the violation. Defendant argues that the violation was deliberate because the Department of Justice has been trying to amend Rule 41(b) to allow explicitly this type of warrant. Therefore, Defendant argues, the federal agents knew that the NIT Warrant was not authorized by Rule 41(b). In other words, Defendant seeks to attribute to the FBI agents that sought the warrant the legal expertise of the DOJ lawyers, which is absurd. As discussed above, it was quite logical for the FBI to seek this warrant in the Eastern District of Virginia. Even if this Court is incorrect in holding that there was no violation of Rule 41(b), there is a credible argument that the current rule allowed this warrant. Additionally, it is hard to fathom why the FBI would go through the trouble of seeking a warrant in deliberate violation of Rule 41(b). If they were so inclined to undermine individual rights, they might have forgone seeking the warrant in the first place. But they tried to comply with the Fourth Amendment and the Federal Rules of Criminal Procedure. Any violation of Rule 41(b) was unintentional.

Nor has Defendant been prejudiced by any Rule 41(b) violation. Defendant's computer was in the Eastern District of Virginia when the warrant was executed. Rule 41(b) of course allows magistrate judges to issue warrants authorizing searches of persons and property in their judicial district. Fed. R. Crim. P. 41(b)(1). In more strictly delineating the instances in which magistrate judges may issue warrants for searches outside their district, the Rule protects individuals from being subjected to the powers of distant governmental officials. See United States v. Krueger, 809 F.3d 1109, 1125 (10th Cir.2015) (Gorsuch, J., concurring) ("[O]ur whole legal system is predicated on the notion that good borders make for good government, that dividing government into separate pieces bounded both in their powers and geographic reach is of irreplaceable value when it comes to securing the liberty of the people."). This Defendant was not subject to the power of a distant official, and so was not prejudiced by any violation of Rule 41(b).

***13** As mentioned at the outset of this section, Defendant also seeks suppression on constitutional grounds. He argues that Section 636(a) of the Federal Magistrates Act limits the jurisdiction of magistrates to issue search warrants and that this jurisdiction is defined by Rule 41(b). Because, according to Defendant, the NIT Warrant was issued in violation of Rule 41(b), it was void at its issuance. Therefore, the search of Defendant's computer was allegedly performed without a warrant in violation of the Fourth Amendment to the Constitution.

Of course, not all Fourth Amendment violations require the suppression of the evidence seized as a result.[8] As the Supreme Court has emphasized, "[e]ach time the exclusionary rule is applied it exacts a substantial social cost for the vindication of Fourth Amendment rights." Rakas v. Illinois, 439 U.S. 128, 137, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978). The exclusionary rule should only be applied when its benefits outweigh its costs. Herring v. United States, 555 U.S. 135, 141, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009). In furtherance of this principle, the Supreme Court has established a so-called "good faith" exception to suppression. See id. at 142, 129 S.Ct. 695. "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." Id. (quoting United States v. Leon, 468 U.S. 897, 922, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)).

Behind this exception is the recognition that the purpose

of the exclusionary rule is to deter unlawful police conduct. United States v. Gary, 528 F.3d 324, 329–30 (4th Cir.2008) (citing Leon, 468 U.S. at 918, 104 S.Ct. 3405). Accordingly, the Court has instructed district courts to consider whether the conduct of law enforcement was: (1) "sufficiently deliberate [such] that exclusion can meaningfully deter it," and (2) "sufficiently culpable that such deterrence is worth the price paid by the justice system." Id. at 144, 99 S.Ct. 421.

The FBI agents in this case did the right thing. They gathered evidence over an extended period and filed a detailed affidavit with a federal magistrate in support of their search warrant application. They filed the warrant application in the federal district that had the closest connection to the search to be executed. The information gathered by the warrant was limited: primarily the IP addresses of those that accessed Playpen and additional information that would aid in identifying what computer accessed the site and what individual used that computer. Defendant seeks suppression because of an alleged violation of a Federal Rule of Criminal Procedure, a rule that will likely be changed to allow explicitly this type of search. The pending amendment is evidence that the drafters of the Federal Rules do not believe that there is anything unreasonable about a magistrate issuing this type of warrant; the Rules had simply failed to keep up with technological changes. That is, there is nothing unreasonable about the scope of the warrant itself. The FBI should be applauded for its actions in this case.

***14** In short, the officers in charge of this investigation are not at all culpable. Additionally, as discussed above, there is no evidence that any failure by the FBI to understand the intricacies of the jurisdiction of federal magistrates was deliberate. Even if the NIT Warrant was void because not authorized by the Federal Magistrates Act, suppression is not warranted in this case.

In summary, the NIT Warrant did not violate Rule 41(b) and even if it did suppression is not warranted. Accordingly, the Court **DENIES** Defendant's Second Motion to Suppress. ECF No. 18.

III. MOTION TO COMPEL

Defendant has belatedly filed a Motion to Compel last night at 11:49 pm. ECF No. 30. With this Motion, Defendant seeks a copy of the source code of the NIT used to search his computer. Id. Defendant alleges that the source code may show that the NIT did not comply with the conditions of the NIT Warrant and is thus critical to his First and Second Motions to Suppress.[9] Id. at 1–2. However, Defendant does not make this argument in either Motion to Suppress. Accordingly the Court decides the Motions to Suppress now and will consider the Motion to Compel when it is ripe.

IV. CONCLUSION

For reasons set forth above, the Court **DENIES** Defendant's First Motion to Suppress, ECF No. 15, and **DENIES** Defendant's Second Motion to Suppress, ECF No. 18.

The Clerk is **DIRECTED** to forward a copy of this Order to all Counsel of Record.

IT IS SO ORDERED.

All Citations

--- F.Supp.3d ----, 2016 WL 3189703

Footnotes

1 See e.g., Joseph Cox, The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers, Motherboard, Jan. 5, 2016, http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

2 The Tor network is also known as "The Onion Router." Aff., Warrant Appl., ¶ 7. More information about it may be found on its website: www.torproject.org.

3 "Chan" is a common postscript for online bulletin boards where users may post pictures and messages. See Nick Bilton, One on One: Christopher Poole, Founder of 4chan, Bits Blog, New York Times, Mar. 19, 2010, http://bits.blogs.nytimes.com/2010/03/19/one-on-one-christopher-poole-founder-of-4chan/.

4 Defendant identifies his Playpen username as "Broden" while the government identifies the username as "NeoUmbrella." First Mot. at 10; Gov't's Resp. to First Mot. at 16. This apparent disagreement does not affect any of the analysis in this case.

5 In so holding the Court emphasized the extensive amount of personal information typically held on modern cell phones. Id. at 2491. Personal computers of course typically contain a similar mass of personal information.

6 The proposed addition to the rule reads in relevant part "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 ...." Fed. R. Crim. P. 41(b)(6) (proposed amendment).

7 The government also argues that Rule 41(b)(2) allows the NIT Warrant. Gov't's Resp. to Second Mot. at 3–4. However this Rule only allows a magistrate judge to issue a warrant to search "a person or property outside the district if the person or property is located within the district when the warrant is issued." Fed. R. Crim. P. 41(b)(2). At the time the warrant was issued, Defendant's computer was outside the district and not accessing the website.

8 In addition to the good faith exception discussed here, the government makes two additional arguments for why suppression is not warranted. The government argues that even if the NIT Warrant was void, a warrantless search was justified by exigent circumstance. Gov't's Resp. to Second Mot. at 9–11; see Kentucky v. King, 563 U.S. 452, 460, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011). Of course, the government was able to obtain a warrant in this case, somewhat undercutting this argument. The government also argues that Defendant does not have standing to challenge the warrant because the alleged defect in the warrant, that it exceeded the magistrate's jurisdiction, does not apply to him because his computer was in the Eastern District. Gov't's Resp. to Second Mot. at 8–9. This seems to be a novel interpretation of standing law in Fourth Amendment cases. The standing inquiry in Fourth Amendment cases asks if the individual seeking suppression had a reasonable expectation of privacy in the thing searched. See Rakas v. Illinois, 439 U.S. 128, 133–34, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978). Defendant's computer was searched, and he has a reasonable expectation of privacy in his computer.

9 He also claims that the code is necessary for his trial preparation. ECF No. 30 at 2–3.