IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Newport News Division

UNITED STATES of AMERICA,

v. **Criminal No. 4:16cr16**

EDWARD JOSEPH MATISH, III,

Defendant.

OPINION AND ORDER

This matter is before the Court on Defendant Edward Matish, III's ("Defendant" or "Matish") First Motion to Suppress ("First Motion"), Doc. 18, Third Motion to Suppress ("Third Motion"), Doc. 34, and Motion to Compel Discovery, Doc. 37. The Court recently rescheduled the trial in this case from June 14, 2016 to October 25, 2016.

The Court issued an Opinion and Order denying Defendant's First and Third Motions to Suppress on June 1, 2016, and the Court *sua sponte* filed this Opinion and Order under seal. Doc. 75. Subsequent to an inquiry by the Court on June 14, 2016, defense counsel asked the Court to continue to keep the Opinion and Order, Doc. 75, under seal. However, the Government now has filed a Motion to Unseal the original Opinion and Order. Doc. 89. The Government notes that the trial date has been rescheduled and that Defendant's declarant, Dr. Soghoian, has published information regarding this case and named Defendant on the Internet. See id. Defendant does not oppose the Government's Motion. Doc. 87. Accordingly, the Court will make public its June 1, 2016 Opinion and Order, which it hereby modifies and restates.

On February 8, 2016, Defendant was named in a four (4) count criminal indictment charging him with access with intent to view child pornography, in violation of 18 U.S.C.

§ 2252A(a)(5) and (b)(2). Doc. 1. The Government filed an eight (8) count superseding indictment on April 6, 2016, charging Defendant with access with intent to view child pornography, in violation of 18 U.S.C. § 2252A(a)(5) and (b)(2) (Counts One through Four), and receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1) (Counts Five through Eight). Doc. 26. Defendant filed his First Motion on March 17, 2016, Doc. 18, and he adopted it after the Government filed the superseding indictment on April 8, 2016, Doc. 30. Defendant filed his Third Motion on May 2, 2016. Doc. 34. Defendant filed the Motion to Compel Discovery on May 6, 2016. Doc. 37.

In the Motions to Suppress, Defendant seeks to suppress "all evidence seized from Mr. Matish's home computer by the FBI on or about February 27, 2015 through the use of a network investigative technique, as well as all fruits of that search." Doc. 18 at 1; Doc. 34 at 1. Defendant challenges the warrant authorizing the search on the grounds that it lacked probable cause, that the FBI included false information and omitted material information in the supporting affidavit intentionally or recklessly, that the warrant lacked specificity, and that the warrant's triggering event never occurred. See Doc. 18; Doc. 33. Defendant also argues that the warrant was void *ab initio*, making the warrantless search unconstitutional. Doc. 34 at 1. Finally, Defendant "alleges a prejudicial and deliberate violation of Rule 41." Id.

In the Motion to Compel Discovery, Defendant asks the Court to compel the Government to provide him with the network investigative technique's full source or programming code. Doc. 37 at 1. The defense argues that the full code is relevant not only to Defendant's defense at trial but also to his First and Third Motions to Suppress. Id. at 1–2.

Other courts across the country have considered various challenges to the particular warrant used in this case. See United States v. Werdene, No. 2:15-cr-00434, ECF No. 33 (E.D.

Pa. May 18, 2016); United States v. Levin, No. 15-10271, 2016 WL 2596010 (D. Mass. May 5, 2016); United States v. Arterbury, No. 15-cr-182, ECF No. 47 (N.D. Okla. Apr. 25, 2016) (adopting the report and recommendation of a magistrate judge, ECF No. 42); United States v. Epich, No. 15-cr-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); United States v. Stamper, No. 1:15-cr-109, ECF No. 48 (S.D. Ohio Feb. 19, 2016); United States v. Michaud, No. 3:15-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). The Western District of Washington also has considered a similar discovery motion requesting the full source code. See Michaud, No. 3:15-cr-05351, ECF No. 205 (W.D. Wash. May 18, 2016).

The Court held hearings to address these Motions on May 19, 2016, May 26, 2016, and June 14, 2016. The Court **FINDS**, for the reasons stated herein, that probable cause supported the warrant's issuance, that the warrant was sufficiently specific, that the triggering event occurred, that Defendant is not entitled to a Franks hearing, and that the magistrate judge did not exceed her jurisdiction or authority in issuing the warrant. Furthermore, the Court **FINDS** suppression unwarranted because the Government did not need a warrant in this case. Thus, any potential defects in the issuance of the warrant or in the warrant itself could not result in constitutional violations, and even if there were a defect in the warrant or in its issuance, the good faith exception to suppression would apply. Therefore, the Court **DENIES** Defendant's First and Third Motions to Suppress.

The Court additionally **FINDS** that Defendant is not entitled to the full source code at this stage of the proceeding. Thus, the Court **DENIES** Defendant's Motion to Compel Discovery, Doc. 37. The Government raised a timeliness issue concerning this Motion in its response; however, the Court **GRANTED** Defendant's request to file the Motion late at the hearing on May 26, 2016. Additionally, Defendant submitted a Consent Motion for Leave to

File an Expert Declaration Relevant to the Motion to Compel Discovery, Doc. 83, which the Court **GRANTS**.

I. FACTUAL BACKGROUND

The prosecution of Mr. Matish stems from the Government's investigation of Playpen, a website that contained child pornography. At the hearing on May 19, 2016, the Court heard testimony from FBI Special Agent ("SA") Daniel Alfin and SA Douglas Macfarlane. The Court also admitted several Defense Exhibits. See Def. Exs. 1A, 1B, 2, 3, 4, 5, 6. Doc. 58. The Court admitted Ex. 5 under seal. Id. Additionally, the Court received a brief of amicus curiae from the Electronic Frontier Foundation. See Doc. 42. These sources, in addition to the parties' briefs, informed the Court's understanding of the relevant facts, which are recounted below.

i. The Tor Network

Playpen operated on "the onion router" or "Tor" network. The U.S. Naval Research Laboratory created the Tor network in an attempt to protect government communications. The public now can access the Tor network. Many people and organizations use the Tor network for legal and legitimate purposes; however, the Tor network also is replete with illegal activities, particularly the online sexual exploitation of children.

A person can download the Tor browser from the Tor website. See Tor Project: Anonymity Online, https://www.torproject.org (last visited May 23, 2016). SA Alfin testified that the Tor network possesses two primary purposes: (1) it allows users to access the Internet in an anonymous fashion and (2) it allows some websites – hidden services – to operate only within the Tor network. Although a website's operator usually can identify visitors to his or her site through the visitors' Internet Protocol ("IP") addresses, Tor attempts to keep a user's IP address hidden. Additionally, people who log into a hidden service cannot identify or locate the website

itself. Furthermore, all communications on hidden services are encrypted. Thus, the Tor network attempts to provide anonymity protections both to operators of a hidden service and to visitors of a hidden service. There are index websites of Tor hidden services that users can search, although these indexes behave differently than a typical search engine like Google. According to SA Alfin, more than 1,000 servers all over the world exist in the Tor network. Because Tor attempts to keep users' IP addresses hidden, the Government cannot rely on traditional identification techniques to identify website visitors who utilize the Tor network.

ii. Playpen

Both parties agree that Playpen contained child pornography. While SA Alfin described Playpen as being entirely dedicated to child pornography, Doc. 59 at 51–52, the Government conceded in its briefs that some of Playpen's sections and forums did not consist entirely of child pornography. See Doc. 24 at 11 (noting that the "vast majority" of Playpen's sections, forums, and sub-forums were "categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims"). The Government characterizes Playpen as a hidden service, but Defendant disputes that Playpen always resembled a hidden service, claiming that "due to an error in Playpen's connections with the Tor network, it could be found and viewed on both the Tor network and the regular Internet for at least part of the time that it was operating." Doc. 18 at 5.

The Government notes that the "scale of child sexual exploitation on the site was massive: more than 150,000 total members created and viewed tens of thousands of postings related to child pornography." Doc. 24 at 4. Additionally, "[i]mages and videos shared through the site were highly categorized according to victim age and gender, as well as the type of sexual activity. The site included forums for discussion of all things related to child sexual exploitation,

including tips for grooming victims and avoiding detection." Id. at 4. The victims displayed on Playpen were both foreign and domestic, and some represent children known to the Government. Upon registering for an account with Playpen, potential users were warned not to enter a real email address or post identifying information in their profiles.

In December 2014, a foreign law enforcement agency discovered Playpen and alerted the FBI. After locating Playpen's operator, the FBI executed a search of his home in Florida on February 19, 2015, seizing control of Playpen. The FBI did not immediately shut Playpen down; instead, it assumed control of Playpen, continuing to operate it from a government facility in the Eastern District of Virginia from February 20, 2015 through March 4, 2015. As of February 20, 2015, Playpen had 158,094 members from all over the world, 9,333 message threads, and 95,148 posted messages. Doc. 18 at 6; Doc. 24 at 9. Defendant argues a substantial increase in the usage of Playpen occurred after the Government took it over. While the Government concedes that there was some increase, it disputes the unsupported figures in Defendant's briefs.

iii. The NIT Warrant and the Supporting Affidavit

On February 20, 2015, an experienced and neutral federal magistrate judge authorized the FBI to deploy a network investigative technique ("NIT") on Playpen's server to obtain identifying information from activating computers, which the warrant defines as computers "of any user or administrator who logs into [Playpen] by entering a username and password." Def. Ex. 1A. It is undisputed that the FBI could not identify the locations of any of the activating computers prior to deploying the NIT. The NIT is a set of computer code that in this case instructed an activating computer to send certain information to the FBI. This information included:

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

2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other activating computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the activating computer;
5. the activating computer's Host Name;
6. the activating computer's active operating system username; and
7. the activating computer's media access control ("MAC") address.

Def. Ex. 1A. In order to determine a target's location, the FBI only needed to identify the first piece of information described above. SA Macfarlane acted as the affiant, and he signed the warrant application. SA Macfarlane has nineteen (19) years of federal law enforcement experience.

The NIT Warrant application described Playpen's home page logo as depicting "two images [of] partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, 'No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out.'" Def. Ex. 1B ¶ 12. This description was inaccurate at the time the magistrate judge signed the warrant, although SA Macfarlane did not know of the inaccuracies at the time he sought the magistrate's authorization. A very short time before the FBI assumed control of Playpen, the logo changed from depicting two partially clothed prepubescent females with their legs spread apart to displaying a single image of a female. SA Alfin described this image as "a single prepubescent female wearing fishnet stockings and posed in a sexually suggestive manner." Doc. 59 at 33. The text underneath the logo remained unchanged. SA Alfin participated in the search of Playpen's operator's home in Florida, and he testified that during the search he saw the website displayed on the operator's computer. However, though SA Alfin admits to viewing the new logo, he testified that "it went unobserved by me because it was an insignificant change to the Web site." Doc. 59 at 10.

Even though the warrant authorized the FBI to deploy the NIT as soon as a user logged into Playpen, SA Alfin testified that the Government did not deploy the NIT against Mr. Matish in this particular case until after someone with the username of "Broden" logged into Playpen, arrived at the index site, went to the bestiality section – which advertised prepubescent children engaged in sexual activities with animals – and clicked on the post titled "Girl 11YO, with dog." In other words, the agents took the extra precaution of not deploying the NIT until the user first logged into Playpen and second entered into a section of Playpen which actually displayed child pornography. At this point, testified SA Alfin, the user apparently downloaded child pornography as well as the NIT to his computer. Thus, the FBI deployed the NIT in a much narrower fashion than what the warrant authorized.

After determining a user's IP address via the NIT, the FBI can send a subpoena to an Internet Service Provider ("ISP"), which will be able to identify the computers that possessed that IP address on a particular date and time. Based on this information, a different experienced and neutral magistrate judge authorized a residential search warrant for Mr. Matish's home, which the FBI executed on July 29, 2015. Pursuant to this second warrant, the FBI seized several computers, hard drives, cell phones, tablets, and video game systems.

iv. Discovery Disputes

Defendant first requested discovery pertaining to the NIT code in March 2016. Initially, the Government declined to disclose any part of the NIT code. Therefore, on May 6, 2016, Defendant submitted the Motion to Compel Discovery. Doc. 37. The Government responded in opposition on May 17, 2016. Doc. 56. Defendant replied on May 23, 2016. Doc. 60. On May 25, 2016, the Government requested permission to file a surreply, Doc. 62, which the Court orally granted at a hearing on May 26, 2016. The Government filed the surreply on June 1,

2016. Doc. 74. On June 10, 2016, Defendant submitted a Consent Motion for Leave to File an Expert Declaration Relevant to this Motion. Doc. 83. After Defendant submitted the Motion to Compel Discovery, Doc. 37, after the Government responded, Doc. 56, and after Defendant replied, Doc. 60, the Government made the NIT instructions, as well as the information obtained via the NIT's execution, available for review. See Doc. 74 at 9. Additionally, on June 14, 2016, the Government made available to the defense the two-way network data stream, which details the information sent to and from Defendant's computer and the FBI. Defendant asserted at a hearing on May 26, 2016 that the NIT instructions do not represent the entire NIT source code, and he now asks for the remaining pieces of the code.

The Court held a hearing to address this matter on June 14, 2016. At the hearing, the Court heard testimony from SA Alfin. The defense did not offer any additional testimony or evidence at the hearing, instead relying upon the declarations filed with its pleadings. With his briefing, Defendant submitted three declarations from Mr. Vlad Tsyrklevich, a computer security engineer, see Doc. 78, Dr. Matthew Miller, an Assistant Professor of Computer Science and Information Technology, see Doc. 60, Ex. C, and Dr. Christopher Soghoian, a "researcher focused on privacy, computer security and government surveillance," Doc. 83.

II. Defendant Is Not Entitled to Discovery of the Full NIT Source Code

A. Legal Standards

i. Disclosure

Under Federal Rule of Criminal Procedure 16(a)(1)(E), "[u]pon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies of portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the

item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant." Fed. R. Crim. P. 16(a)(1)(E). This rule differs from that announced in Brady v. Maryland, 373 U.S. 83, 87 (1963), "which rests upon due process considerations[] and provides the minimum amount of pretrial discovery granted in criminal cases." E.g., United States v. Caro, 597 F.3d 608, 620 (4th Cir. 2010) (citing United States v. Baker, 453 F.3d 419, 424 (7th Cir. 2006) ("Rule 16 . . . is broader than Brady."); United States v. Conder, 423 F.2d 904, 911 (6th Cir. 1970) ("We are . . . of the view that the disclosure required by Rule 16 is much broader than that required by the due process standards of Brady.")).

In United States v. Armstrong, the Supreme Court of the United States clarified that, "in the context of Rule 16 'the defendant's defense' means the defendant's response to the Government's case in chief." 517 U.S. 456, 462 (1996). Thus, in order for "the defendant to show materiality under this rule, there must be some indication that the pretrial disclosure of the disputed evidence would [] enable[] the defendant significantly to alter the quantum of proof in his favor." Caro, 597 F.3d at 621 (quoting United States v. Ross, 511 F.2d 757, 763 (5th Cir. 1975)) (internal quotations omitted). Hence, "evidence is material as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." Caro, 597 F.3d at 621 (quoting United States v. Lloyd, 922 F.2d 348, 351 (D.C. Cir. 1993)) (internal quotations omitted).

ii. Law Enforcement Privilege

The Fourth Circuit has not directly addressed the law enforcement privilege. However, other circuits have considered how district courts should evaluate a party's assertion of the law

enforcement privilege. Courts agree that the party asserting the law enforcement privilege bears the burden of showing that the privilege applies. See, e.g., In re The City of New York, 607 F.3d 923, 944 (2d Cir. 2010) (citing In re Sealed Case, 856 F.2d 268, 271–72 (D.C. Cir. 1988)). In order to illustrate that the privilege applies, the party "must show that the documents contain information that the law enforcement privilege is intended to protect," which "includes information pertaining to law enforcement techniques and procedures, information that would undermine the confidentiality of sources, information that would endanger witness and law enforcement personnel [or] the privacy of individuals involved in an investigation, and information that would otherwise . . . interfere[] with an investigation." In re The City of New York, 607 F.3d at 944 (quoting In re Department of Investigation of City of New York, 856 F.2d 481, 484 (2d Cir. 1988)) (internal quotations omitted). If "the party asserting the privilege successfully shows that the privilege applies, the district court then must balance the public interest in nondisclosure against 'the need of a particular litigant for access to the privileged information,'" as the privilege is qualified, not absolute. In re The City of New York, 607 F.3d at 948 (quoting In re Sealed Case, 856 F.2d at 272).

When evaluating claims of privilege in the criminal context, courts should remain cognizant of the fact that "[w]hile the public's interest in effective law enforcement . . . support[s] the creation of the privilege, [it does] not extinguish a criminal defendant's strong interest in effective cross-examination of adverse witnesses." United States v. Green, 670 F.2d 1148, 1155 (D.C. Cir. 1981); see also United States v. Van Horn, 789 F.2d 1492, 1507 (11th Cir. 1986) (comparing the qualified law enforcement privilege to the informant's privilege and recognizing that the "privilege must give way, however, where the informant's identity or knowledge is 'relevant and helpful to the defense of an accused, or is essential to a fair

determination of a cause.'" (quoting Roviaro v. United States, 353 U.S. 53, 60–61 (1957))). Thus, in criminal cases, district courts should balance the Government's need to keep certain information private with the defendant's need for the information. E.g., Van Horn, 789 F.2d at 1508 (stressing "that the necessity determination requires a case by case balancing process" and that there are no established "fixed rules about the discoverability of electronic surveillance techniques in criminal cases").

Courts have noted that to "assess both the applicability of the privilege and the need for the documents, the district court must ordinarily review the documents in question." In re The City of New York, 607 F.3d at 948. If filing the documents under seal remains insufficient to protect the privileged information, the court may review them *ex parte* and *in camera*. Id. at 948–49.

B. Analysis

i. Disclosure

The parties agree that the information requested is within the Government's control, that the Government does not plan to use the actual code during its case in chief, and that the code was not obtained from and does not belong to Defendant. The parties dispute, however, whether the defense has shown materiality under Fed. R. Crim. P. 16(a)(1)(E)(i).

Defendant asserts two main arguments to support his claim of materiality. First, Defendant explains that "Mr. Matish expects to challenge the government's chain of custody regarding the supposed linkage between his computer and [Playpen]." Doc. 60 at 4. In order to do so, "the defense intends to challenge the accuracy of the identifying data that the government claims connects Mr. Matish to both 'Broden' and specific activity on the Website," focusing on "the government's recent assertion that some of the information that was used to link 'Broden' to

Mr. Matish's computer was not in fact gathered from Mr. Matish's computer and securely transferred in encrypted form to the FBI, but rather was sent unencrypted over the traditional [I]nternet." Id. at 4–5. The defense also expects to "challenge the government's case by arguing to the jury that child pornography found in the unallocated space of Mr. Matish's computer came from somewhere or someone else, or at least that the government cannot prove beyond a reasonable doubt that Mr. Matish intentionally downloaded illegal pictures." Id. at 5. To support this argument, Defendant relies on the supposition that "the security settings on Mr. Matish's computer had been compromised by the government's NIT," leaving his computer vulnerable to hackers and malware. Id.

The Court considers the declarations submitted by Defendant less persuasive than SA Alfin's declaration and testimony, because SA Alfin testified and was subjected to cross-examination. Although Defendant's declarants did not testify and were not subject to cross-examination in this case, the Court is aware that Dr. Soghoian testified for the defense at a hearing in Michaud, 3:15-cr-05351. Defendant's declarations left a number of important questions unanswered. For example, Mr. Tsyrklevich's declaration and Dr. Miller's declaration are parallel, and Dr. Miller's declaration largely adopts Mr. Tsyrklevich's declaration with little substance added. See Doc. 78; Doc. 60, Ex. C.

Notably, the purposes for which Defendant asks for access to the missing source code are based upon speculation as to what the declarants might find. The defense lacks any evidence to support the hypotheses and instead relies upon the *ipse dixit* that the source code is needed because its declarants opine that it is needed. Such speculation remains insufficient to serve as a basis to compel discovery. Cf. Caro, 597 F.3d at 621.

For example, the defense aims to discover whether the NIT's deployment compromised Defendant's computer's security. In response to the defense's declarations – and his own admission – that an exploit potentially could make fundamental changes or alterations to a computer system, SA Alfin explained that he executed the NIT in question on a computer under his control. This NIT's deployment, testified SA Alfin, did not affect any security program or device on the computer. On the other hand, none of the three declarants presented by Defendant tested the NIT on Defendant's computer, which is available to them, or on their own computers to determine if it affected their security systems.

Defendant also questions the data's chain of custody, due in part to the NIT program's failure to encrypt its return message from Defendant's computer. The defense's declarants hypothesize that the return message became vulnerable to tampering while in transit on the Internet. As defense counsel argued, during such transmission, the information "was susceptible to being tampered with." Doc. 86 at 37. Indeed, defense counsel agreed that during unencrypted transmission, "anybody can tamper with it." Id. at 38. In his testimony, SA Alfin stated that it only took one (1) second for the NIT data stream to transfer the information to the FBI. Thus, anyone seeking to tamper with the data stream during that timeframe must have known in depth the FBI's activity so as to complete their "hacking operation" within one second. Rather than encrypting and decrypting the information sent to the FBI, the Government produced the data in literal form. Again, the defense has not searched Defendant's computer to decipher whether there is any evidence of tampering with this message. Defendant's declarants likewise have not produced any evidential basis supporting an interruption in the chain of custody.

Defendant expresses doubt concerning the credibility of the Government's evidence, specifically SA Alfin's declaration and testimony. However, SA Alfin twice was subjected to

cross-examination by Defendant's attorney, whereas the declarations presented by the defense were immune from cross-examination, and, the Court **FINDS**, left many questions unanswered. Another example is that an examination of Defendant's computer may have uncovered evidence either of hacking or an alternate source of the child pornography, but, as it stands, the declarants' inaction leaves their hypotheses with no evidence to support them. At least two of Defendant's declarants are familiar with a similar case in Washington State, see Michaud, 3:15-cr-05351, and have been involved with these issues for many months. See Doc. 78; Doc. 60, Ex. C. Therefore, they have had ample opportunity to examine Defendant's computer or other computers as did SA Alfin.

Defense counsel makes much of SA Alfin's testimony that he did not know, nor had he examined, the exploit code. SA Alfin explained that the exploit represents "a defect in a lock that would allow someone with the proper tool to unlock it without possessing the key." See Doc. 74, Ex. 1 ¶ 11. Thus, through the exploit, the FBI could deploy the NIT onto Defendant's computer. Yet, the Government now has furnished the NIT's operating instructions, which the defense's declarants could apply to Defendant's computer or to other computers ultimately to determine how – if at all – the NIT affected Defendant's computer.

The Court **FINDS** *ex parte* and *in camera* inspection of the exploit unnecessary. Such examination would not have assisted the Court in dealing with the issues before it. The technicalities of such an examination are better left to computer experts. The Court places its reliance on the declaration and testimony of SA Alfin. SA Alfin explained that the exploit code did not produce any additional information but merely opened the lock to Playpen. Indeed, SA Alfin did not believe it was necessary to examine the exploit code since it would not furnish him with any additional information. Defendant's declarants did not furnish any evidence to dispute

SA Alfin's testimony that there was nothing to be gained by examining the exploit code, nor have the declarants offered a specific reason for any such exam.

The Government declined to furnish the source code of the exploit due to its immateriality and for reasons of security. The Government argues that reviewing the exploit, which takes advantage of a weakness in the Tor network, would expose the entire NIT program and render it useless as a tool to track the transmission of contraband via the Internet. SA Alfin testified that he had no need to learn or study the exploit, as the exploit does not produce any information but rather unlocks the door to the information secured via the NIT. The defense claims it needs the exploit to determine whether the FBI closed and re-locked the door after obtaining Defendant's information via the NIT. Yet, the defense lacks evidentiary support for such a need. The lack of any evidence to support the hypotheses of Defendant's declarants, coupled with their failure to examine Defendant's computer and the fact that the Government knew of the "Broden" account prior to the NIT's deployment,[1] further coupled with the miniscule timeframe in which the unencrypted reply was subject to tampering, all suggest that the defense has failed to advance the speculative hypotheses of its declarants to the realm of significantly altering the quantum of proof or of strongly indicating that the exploit "will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." Caro, 597 F.3d at 621 (quoting Lloyd, 922 F.2d at 351) (internal quotations omitted).

Accordingly, the Court **FINDS** that the defense has failed to meet the test under Caro, 597 F.3d at 621, for requiring the Government to produce the exploit source code.

[1] SA Alfin testified without contradiction that the FBI uncovered the user "Broden," which it later linked to Defendant's computer, before it deployed the NIT.

ii. Qualified Law Enforcement Privilege

The Government asserts that the law enforcement privilege applies to the full source code, excluding the already-provided NIT instructions and the corresponding data stream. See Doc. 56 at 22; Doc. 74 at 13. Although the Court technically does not reach the issue of Government privilege, assuming *arguendo* that it did, the Court believes that the scales tip substantially in favor of the Government. In considering this issue, the Court examined – in addition to the parties' briefs – a classified brief submitted by the Government.

The Government alleges that disclosure of the code "would be harmful to the public interest" because it "could diminish the future value of important investigative techniques, allow individuals to devise measures to counteract these techniques in order to evade detection, [and] discourage cooperation from third parties and other governmental agencies who rely on these techniques in critical situations." Doc. 56 at 22.

Courts have held similar law enforcement techniques subject to the qualified privilege. See In re The City of New York, 607 F.3d at 944 (finding that the privilege clearly applies to Field Reports that "contain detailed information about the undercover operations of the NYPD"); see also Van Horn, 789 F.2d at 1508 (finding a qualified privilege in the nature and location of electronic surveillance equipment); Green, 670 F.2d at 1150 (finding that "the Government has a qualified privilege during a suppression hearing not to disclose its surveillance locations"). Like police Field Reports, In re The City of New York, 607 F.3d at 944, police surveillance locations, Green, 670 F.2d at 1150, and electronic surveillance equipment locations, Van Horn, 789 F.2d at 1508, the full NIT source code includes information pertaining to law enforcement techniques, procedures, and information that could endanger the public if released. Thus, the Government has shown that the privilege applies.

However, the recognition of the privilege cannot end the Court's consideration. E.g., Green, 670 F.2d at 1155. Indeed, after finding that the privilege applies to the exploit, the Court must balance the Government's right to keep the information private with Defendant's right to inspect the information. E.g., id. This particular issue concerns the public interest in nondisclosure and Defendant's rights to put on a defense and to confront witnesses against him under the Sixth and Fourteenth Amendments. At its core, this case embodies the fundamental collision between the duty of our Government to protect its citizens from the dangers caused by child pornography with the implied right of privacy under the Fourth Amendment. Notably, the Government already has found that protecting its citizens outweighs the First Amendment's right of freedom of speech, for it applies prior restraint to child pornography. E.g., Osborne v. Ohio, 495 U.S. 103 (1990); see also New York v. Ferber, 458 U.S. 747 (1982). The Government further has recognized the dangers caused by child pornography in enacting severe punishment, including mandatory minimum sentences, for the possession of child pornography. See 18 U.S.C. § 2252A(b)(1).

Defendant already has received the NIT instructions and the two-way data stream, and the Government's disclosure of this information, coupled with its assurance to the Court that none of the images recovered from Defendant's computer serve as a basis for any charge filed in this case, see Doc. 86 at 56, further lessens the defense's need for the additional information it seeks. Hence, even if the Court were to find the exploit code material under Rule 16(a)(1)(E), the Court **FINDS** that the Government's need to protect the code outweighs Defendant's need for it.

Therefore, the Court **FINDS** that Defendant has failed to show that the full NIT code – specifically, the exploit – is material under Rule 16(a)(1)(E). Thus, the Court **DENIES**

Defendant's Motion to Compel Discovery, Doc. 37. Additionally, even if the Court were to find that Defendant made a sufficient showing of materiality, the Court would not require the Government to disclose the full source code due to the law enforcement privilege.

iii. Malware

The parties debate whether the NIT constitutes malware. See Doc. 74 at 12; Doc. 83. Black's Law Dictionary defines malicious technology, or malware, as "any electronic or mechanical means, esp. software, used to monitor or gain access to another's computer system without authorization for the purpose of impairing or disabling the system." *Malicious Technology*, Black's Law Dictionary (10th ed. 2014), available at Westlaw BLACKS. Whether the NIT constitutes malware is immaterial to this Court's decisions concerning the Motions to Suppress and the Motion to Compel Discovery. The Court notes, however, that perhaps malware is a better description for the program through which the provider of the pornography attempted to conceal its distribution of contraband over the Internet than for the efforts of the Government to uncover the pornography. Due to the negative connotations associated with the word "malware," the defense's declarations and tweets criticizing the NIT and their insistence on describing it as malware suggest that they simply do not believe that the Government should be permitted to possess this tool. See Doc. 83; Doc. 89, Exs. 2, 3, 4, 6, 7. Yet, "[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system." United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012).

III. Probable Cause Supported the Issuance of the NIT Warrant

A. Legal Standards

The Fourth Amendment to the United States Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As the Supreme Court of the United States noted in Illinois v. Gates, "probable cause is a fluid concept – turning on the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules." 462 U.S. 213, 232 (1983). Therefore, a magistrate considering whether probable cause supports the issuance of a search warrant simply must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." Id. at 238. In order for a magistrate to conclude that probable cause exists, a warrant application's supporting affidavit must be more than conclusory and bare bones; indeed, the affidavit "must provide the magistrate with a substantial basis for determining the existence of probable cause." Id. at 239. Probable cause is not subject to a precise definition, and it is a relaxed standard. See United States v. Allen, 631 F.3d 164, 172 (4th Cir. 2011); see also United States v. Martin, 426 F.3d 68, 76 (2d Cir. 2005). When examining an affidavit, a magistrate may rely on law enforcement officers, who may "draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person," as long as the affidavit contains facts to support the law

enforcement officer's conclusions. United States v. Johnson, 599 F.3d 339, 343 (4th Cir. 2010) (quoting United States v. Arvizu, 534 U.S. 266, 273 (2002)) (internal quotations omitted); see also United States v. Brown, 958 F.2d 369, at *5 (4th Cir. 1992) (noting that "magistrates, in making probable cause determinations, may rely upon an experienced police officer's conclusions as to the likelihood that evidence exists and where it is located").

A court reviewing whether a magistrate correctly determined that probable cause exists should afford the magistrate's determination of probable cause great deference. See Gates, 462 U.S. at 236. Therefore, "the duty of a reviewing court is simply to ensure that the magistrate had a 'substantial basis for . . . conclud[ing] that' probable cause existed." Id. at 238–39 (quoting Jones v. United States, 362 U.S. 257, 271 (1960)); see also United States v. Blackwood, 913 F.2d 139, 142 (4th Cir. 1990). A reviewing court should "resist the temptation to 'invalidate warrant[s] by interpreting affidavit[s] in a hypertechnical, rather than a commonsense, manner.'" Blackwood, 913 F.2d at 142 (quoting Gates, 462 U.S. at 236).

B. Analysis

Defendant first challenges the NIT Warrant on its face, arguing that it is not based on probable cause, even if the Court were to ignore the warrant application's inaccuracies. See Doc. 18 at 11–12; Doc. 33 at 3. The Government, in contrast, argues that the facts contained in the 31-page affidavit written by a 19-year FBI veteran with specialized training and experience in this field, "along with the reasonable inferences to be drawn therefrom, support probable cause to believe that registered users of Playpen intended to view and trade child pornography." Doc. 24 at 17.

The Court **FINDS** that the magistrate possessed a substantial basis for determining that probable cause existed to support the issuance of the NIT Warrant. Taking the affidavit at face value, it outlines numerous affirmative steps that one must take to find Playpen on the Tor network, it fully describes Playpen's home page and registration terms, and it details Playpen's content. See Def. Ex. 1B. Examining the totality of these circumstances leads to the conclusion that a fair probability existed that those accessing Playpen intended to view and trade child pornography and that the NIT would help uncover evidence of these crimes.

The affidavit describes the Tor network and its emphasis on anonymity. See Def. Ex. 1B at 10–11. It states that "the TARGET WEBSITE is a Tor hidden service." Id. ¶ 10. It explains that a user cannot access a hidden service unless he or she knows the particular website address. Id. The affidavit, therefore, describes numerous affirmative steps that one must take even to find Playpen on the Tor network. The Court credits SA Alfin's testimony that it would be extremely unlikely for someone to stumble innocently upon Playpen. The magistrate thus justifiably concluded that the chances of someone innocently discovering, registering for, and entering Playpen were slim.

Additionally, the affidavit illustrates Playpen's home page, detailing the picture of the two prepubescent females as well as the text. Id. ¶ 12. The affiant explained that based on his training and experience, he knew that "'no cross-board reposts' refers to a prohibition against material that is posted on other websites from being 're-posted' to the TARGET WEBSITE; and '.7z' refers to a preferred method of compressing large files or sets of files for distribution." Id. ¶ 12. The affidavit also explained that users viewed a warning message upon accessing the "register an account" hyperlink, informing them not to enter a real email address or to post

identifying information. Id. ¶ 13. It also warned that the website "is not able to see your IP . . ." Id. ¶ 13.

In addition, the affidavit described Playpen's contents. It noted that "the entirety of the TARGET WEBSITE is dedicated to child pornography."[2] Id. ¶ 27. While Defendant disputes this characterization, it was not unreasonable for the affiant to conclude, or for the magistrate to accept, that the site indeed was dedicated to child pornography. The affidavit also detailed sections, forums, and sub-forums visible upon logging into the site, most of which referenced children. SA Alfin testified that even the topics listed on the home page that could refer to adult pornography actually referenced child pornography in the context of Playpen. The affiant also noted that he believed users employed Playpen's private message system to disseminate child pornography. Id. ¶ 22. Finally, the affidavit described sub-forums that contained "the most egregious examples of child pornography and/or [were] dedicated to retellings of real world hands on sexual abuse of children." Id. ¶ 27.

Therefore, it was not unreasonable for the magistrate judge to find that Playpen's focus on anonymity, coupled with Playpen's suggestive name, the logo of two prepubescent females partially clothed with their legs spread apart (or, as discussed below, the one scantily clad minor), and the affidavit's description of Playpen's content, endowed the NIT Warrant with probable cause. In fact, other courts have found that probable cause supported this exact NIT Warrant. In Epich, for example, the Eastern District of Wisconsin adopted a magistrate judge's report and recommendation, which "pointed to the complicated machinations through which users had to go to access the web site (meaning that unintentional users were unlikely to stumble onto it); the fact that the web site's landing page contained images of partially clothe[d]

[2] "Dedicated" to child pornography does not mean that every section actually consisted of child pornography – some forums apparently discussed how to prepare a child and examples of child abuse. This distinction may explain the seeming conflict between SA Alfin's testimony and the Government's brief.

prepubescent females with their legs spread apart; the existence of statements on the landing page that made it clear that users were not to re-post materials from other web sites, and provided information for compressing large files (such as video files) for distribution; the fact that the site required people to register to use it, and advised registrants to use fake e-mail addresses and emphasized that the site was anonymous; and the fact that once a user went through all of *those* steps to become a registered user, the user had access to the entire site, which contained images and/or videos that depicted child pornography." 2016 WL 953269, at *1–2. The court thus concluded that "anyone who ended up a registered user on the web site was aware that the site contained, among other things, pornographic images of children." Id. at 1. The magistrate judge in Epich additionally found that "the fact that one could become a registered user to the web site, and then view only information that did not contain illegal material, did not affect the probable cause determination that the Virginia magistrate judge made in issuing the warrant." Id. at 1–2. Similarly, in Michaud, the Western District of Washington stated that "it would be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor network." 2016 WL 337263, at *5. Thus, taking the NIT Warrant on its face, the Court **CONCLUDES** that the magistrate judge possessed ample probable cause to issue the NIT Warrant.

IV. A Franks Hearing Is Not Warranted

A. Legal Standards

In Franks v. Delaware, the Supreme Court held that if a "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 if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires

that a hearing be held at the defendant's request." 438 U.S. 154, 155–56 (1978). If, at the hearing, "the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, 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. However, no hearing is required if after "material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause." Id. at 172.

Because affidavits supporting search warrants are presumed valid, in order to "mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." Id. at 171–72. Therefore, "[t]here must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof." Id. at 171. The defendant can challenge an affidavit on the ground that the affiant intentionally or recklessly included false statements or on the ground that the affiant omitted material facts with the intent to make, or in reckless disregard of whether the omission made, the affidavit misleading. E.g., United States v. Colkley, 889 F.2d 297, 300 (4th Cir. 1990); see also United States v. Chandia, 514 F.3d 365, 373 (4th Cir. 2008). It is insufficient for the defendant to allege mere negligence on the part of the affiant. Colkley, 889 F.2d at 300. To make the necessary substantial preliminary showing, the defendant seeking a Franks hearing should furnish to the Court affidavits or sworn or otherwise reliable statements or satisfactorily explain their absence. Id. A defendant can make a substantial preliminary showing that a false statement was included in the affidavit with reckless disregard

for its truth by showing "that an officer acted with a high degree of awareness of [a statement's] probable falsity, that is, when viewing all the evidence the affiant must have entertained serious doubts as to the truth of his statements or had obvious reasons to doubt the accuracy of the information he reported." Miller v. Prince George's County, MD, 475 F.3d 621, 627 (4th Cir. 2007) (quoting Wilson v. Russo, 212 F.3d 781, 788 (3d Cir. 2000)) (internal quotations omitted).

In order to be material, the falsity or the omission in the affidavit "must do more than potentially affect the probable cause determination: it must be 'necessary to the finding of probable cause.'" Colkley, 889 F.2d at 301 (citing Franks, 438 U.S. at 156). In Colkley, the Fourth Circuit noted that "the district court need not have held a Franks hearing . . . because inclusion of the omitted information would not have defeated probable cause." Id. at 299–300. The Fourth Circuit stressed that the district court misstated the type of materiality Franks required when it held that "the affiant's omission 'may have affected the outcome' of the probable cause determination." Id. at 301. To determine whether the inaccuracies were necessary to find probable cause, a district court must "excise the offending inaccuracies and insert the facts recklessly omitted, and then determine whether or not the 'corrected' warrant affidavit would establish probable cause." Miller, 475 F.3d at 628; see also Martin, 426 F.3d at 75. To make this determination, courts apply the commonsense, totality-of-the-circumstances analysis articulated in Gates. See Colkley, 899 F.2d at 301–02.

B. Analysis

Defendant alleges that the NIT affidavit contains, at a minimum, recklessly misleading statements and omissions that are material to the probable cause determination, and that, therefore, a Franks hearing is warranted. Doc. 18 at 19. Defendant specifically focuses on "the application's false description of Playpen's home page, compounded by highly inaccurate

statements about how the Tor network functions and a cloud of misleading technical jargon." Id. at 23. Defendant further argues that the home page's false description was highly material to the magistrate's finding of probable cause. Id. at 20. He claims that the affidavit – if it did so at all – persuaded the magistrate judge that the site's dedication to child pornography would be apparent to anyone viewing the home page "by including a patently inaccurate description of the homepage." Id. Importantly, Defendant asserts that the inaccurate home page description was clearly relevant to a finding of probable cause, as evidenced by the allegedly dramatic increase in visitors to Playpen after the home page changed. See Doc. 33 at 12–13. Defendant alleges that the increase in visitors "strongly suggests that many new visitors viewed the revised Playpen homepage as a typical adult site (and had no trouble finding it by Tor search engine or otherwise)" and that "it seems quite plausible that the different content of the Playpen homepage – the misrepresentation at issue here – significantly affected a potential user's expectations as to the site's contents." Id. The Government admits that there was an increase in usage, but it challenges Defendant's numbers.

The Court **FINDS** that Defendant has not made a substantial showing to justify a Franks hearing. Although SA Alfin admitted that he saw Playpen as it appeared with the new logo on February 19, 2015, there is no evidence before the Court that SA Alfin ever informed SA Macfarlane of the change in the few hours between the conclusion of the residential search in Florida and SA Macfarlane's seeking the magistrate's authorization to use the NIT. The Court also finds that it was not reckless for the affiant not to examine the website one more time on the day he sought the warrant's authorization, as he had recently examined the website and confirmed that nothing had changed. Therefore, the Court **FINDS** that SA Macfarlane did not

act intentionally or with any doubt as to the validity of his affidavit when he brought the warrant to the magistrate judge.

Additionally, the Court **FINDS** that the logo change was not material to the probable cause determination. Although the Court questions what caused the increase in visitors after February 20, 2015, even if the warrant had included the description of the new logo instead of the description of the old logo, probable cause still would have existed. Indeed, SA Alfin described the new logo as depicting "a single prepubescent female wearing fishnet stockings and posed in a sexually suggestive manner." Doc. 59 at 33. Had SA Alfin or Macfarlane described the new image differently, then perhaps the logo change would have been material. However, the Court posits that replacing "two images depicting partially clothed prepubescent females with their legs spread apart," Def. Ex. 1B ¶ 12, with an image of "a single prepubescent female wearing fishnet stockings and posed in a sexually suggestive manner," Doc. 59 at 33, is not significant. Additionally, the logo change lacks significance because the probable cause rested not solely on the site's logo but also on the affiant's description that the entire site was dedicated to child pornography, Playpen's suggestive name, the affirmative steps a user must take to locate Playpen, the site's repeated warnings and focus on anonymity, and the actual contents of the site.

The Western District of Washington, in considering similar challenges to the same NIT Warrant, orally denied the defendant's request for a Franks hearing at a motions hearing. Michaud, 2016 WL 337263, at *1. In a subsequent opinion denying the defendant's motion to suppress, the court noted that although SA Alfin saw the newer version of Playpen's home page, he did not notice the picture changes. Id. at *3. The court stated that the balance of Playpen's "focus on child pornography apparently remained unchanged, in SA Alfin's opinion." Id.

Additionally, the court found that the "new picture also appears suggestive of child pornography, especially when considering its placement next to the site's suggestive name, Play Pen." Id.

Therefore, Defendant has not made a substantial preliminary showing that the affiant included the inaccurate description of Playpen's home page either intentionally or recklessly. Furthermore, even if Defendant had made such a showing, a Franks hearing is not warranted because the logo change was immaterial to the probable cause determination. Thus, the Court **DENIES** Defendant's request for a Franks hearing.

V. The NIT Warrant Did Not Lack Specificity

A. Legal Standards

The Fourth Amendment to the United States Constitution requires that search warrants particularly describe the place to be searched and the persons or things to be seized. U.S. Const. amend. IV. This requirement of particularity "applies to the warrant, as opposed to the application or the supporting affidavit submitted by the applicant." E.g., United States v. Hurwitz, 459 F.3d 463, 470 (4th Cir. 2006). By requiring warrants to state the scope of the proposed search with particularity, the Fourth Amendment "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." United States v. Talley, 449 F. App'x 301, 302 (4th Cir. 2011). Additionally, the "Fourth Amendment requires that a warrant be no broader than the probable cause on which it is based." Hurwitz, 459 F.3d at 473 (quoting United States v. Zimmerman, 277 F.3d 426, 432 (3d Cir. 2002)) (internal quotations omitted).

B. Analysis

Defendant argues that the NIT Warrant is overbroad. Doc. 18 at 23. Defendant bases this argument on the fact that the NIT Warrant authorized the FBI to search any of the tens of

thousands of computers that accessed Playpen, regardless of the user's activities on Playpen. Id. at 23–26. Indeed, the warrant "authorized the FBI to execute searches on a population of potential targets so large that it exceeds the population of Charlottesville, Virginia, and many other small cities." Id. at 26. Defendant claims that the NIT Warrant did not establish probable cause to search a particular location, because it "purportedly gave the FBI broad discretion in deciding when and against whom to deploy its malware technology." Id. at 23. Thus, Defendant likens the NIT Warrant to a general warrant. Id. at 24. Defendant analogizes to a case from the Eastern District of Arkansas, in which the court held that:

> [W]hen, as in this case, a warrant's scope is so broad as to encompass "any and all vehicles" at a scene, without naming any vehicle in particular, the probable cause on which it stands must be equally broad. Specifically, the Fourth Amendment requires that the probable cause showing in support of an "any and all vehicles" warrant must demonstrate that, at the time of the search, a vehicle's mere presence at the target location is sufficient to suggest that it contains contraband or evidence of a crime.

United States v. Swift, 720 F.2d 1048, 1055–56 (E.D. Ark. 2010). According to Defendant, "[h]ere – like the mere presence of a car at the scene of a crime – the Government sought to search users' computers based on mere entry to the Playpen site even though it was not clear from the homepage that someone merely entering the Playpen site – perhaps for the first time – intended to access child pornography." Doc. 18 at 25.

The Government contends that the "NIT warrant described the places to be searched – activating computers of users or administrators that logged into Playpen – and the things to be seized – the seven pieces of information obtained from those activating computers – with particularity." Doc. 24 at 29. The Government asks the Court to "decline the defendant's invitation to read into the Fourth Amendment a heretofore undiscovered upper bound on the number of searches permitted by a showing of probable cause." Id. In the Government's view,

the fact that "a warrant authorizes the search of a potentially large number of suspects is an indication, not of constitutional infirmity, but a large number of criminal suspects." Id. at 35.

As noted in Levin, "NITs, while raising serious concerns, are legitimate law enforcement tools." 2016 WL 2596010, at *8. Without deciding the particularity issue presented by the NIT Warrant, the District of Massachusetts noted that of "special concern here is the particularity requirement, since, as the government points out, 'the defendant's use of the Tor hidden service made it impossible for investigators to know what other districts, if any, the execution of the warrant would take place in.'" Id. at *15. The court noted, however, that despite this difficulty, "at least two other courts have determined that this precise warrant was sufficiently particular to pass constitutional muster." Id. (emphasis in original) (citing Epich, 2016 WL 953269, at *2; Michaud, 2016 WL 337263, at *4–5).

First, in Michaud, the Western District of Washington considered this very issue. 2016 WL 337263, at *5. In Michaud, the defendant argued that the NIT Warrant amounted to a general warrant and lacked sufficient specificity; however, the court found that "both the particularity and breadth of the NIT Warrant support the conclusion that the NIT Warrant did not lack specificity and was not a general warrant." Id. Indeed, the court noted that the NIT Warrant "states with particularity exactly what is to be searched, namely, computers accessing" Playpen. Id. Additionally, the fact that the warrant authorized the FBI to search tens of thousands of potential targets "does not negate particularity, because it would be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor network." Id. The court further held that the NIT Warrant did not exceed the probable cause on which it was issued. Id.

Similarly, in Epich, the Eastern District of Wisconsin, adopting a magistrate judge's report and recommendation, rejected the defendant's particularity challenge to the NIT Warrant. 2016 WL 953269, at *2 (noting that the warrant "explained who was subject to the search, what information the NIT would obtain, the time period during which the NIT would be used, and how it would be used, as well as bearing attachments describing the place to be searched and the information to be seized").

The Court **FINDS** that the NIT Warrant did not violate the Fourth Amendment's particularity requirement. The Court also **FINDS** that the warrant was not broader than the probable cause upon which it was based. As discussed above – putting aside the admitted inaccuracies and the Franks issue – there existed a fair probability that anyone accessing Playpen possessed the intent to view and trade child pornography. Therefore, the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site. While Defendant claims Playpen includes sections and forums which do not actually contain child pornography, the only examples in the record concern ways to approach a child who will be the subject of the pornography and relations between adults and children, thus SA Alfin's description of the site as "entirely dedicated to child porn." Additionally, the warrant explicitly outlined the place to be searched – the computers of any user or administrator who logs into Playpen. Def. Ex. 1A. The warrant also detailed the seven items to be seized. Id. Therefore, the NIT Warrant met the Fourth Amendment's particularity requirements.

VI. The Triggering Event Occurred

A. Legal Standards

Anticipatory warrants are "based upon an affidavit showing probable cause that at some future time (but not presently) certain evidence of a crime will be located at a specified place." United States v. Grubbs, 547 U.S. 90, 94 (2006). Generally, these warrants "subject their execution to some condition precedent other than the mere passage of time – a so-called 'triggering condition.'" Id. If a warrant is subject to a triggering condition and "the government were to execute an anticipatory warrant before the triggering condition occurred, there would be no reason to believe the item described in the warrant could be found at the searched location; by definition, the triggering condition which establishes probable cause has not yet been satisfied when the warrant is issued." Id. Thus, it "must be true not only that *if* the triggering condition occurs 'there is a fair probability that contraband or evidence of a crime will be found in a particular place,' but also that there is probable cause to believe the triggering condition *will occur*." Id. at 96–97 (citing Gates, 462 U.S. at 238). However, "the Fourth Amendment does not require that the triggering condition for an anticipatory search warrant be set forth in the warrant itself." Id. at 99.

B. Analysis

Defendant contends that the NIT Warrant represents an anticipatory warrant "because it prospectively authorized searches whenever unidentified Playpen visitors signed on to the site, with the 'triggering event' for those searches being the act of accessing the site." Doc. 18 at 26. Defendant argues that merely logging into Playpen did not constitute the triggering event; rather "navigating through the internet homepage *described in the warrant application*" represented the triggering condition. Doc. 33 at 2. Since the warrant application incorrectly described Playpen's

home page logo, Defendant could not log into Playpen via the home page described in the warrant application because that home page no longer existed. Id. at 3. Thus, Defendant argues, "the search conducted here was not authorized by the NIT Warrant." Id.

The Government notes that Defendant's "claim that the NIT warrant was void because, as an anticipatory warrant, the 'triggering event' never occurred is little more than a rehash of the same probable cause and Franks challenges that have already been addressed." Doc. 24 at 35–36. The Government contends that the relevant triggering event was "the defendant's decision to enter his username and password into Playpen and enter the site." Id. The Government emphasizes that Defendant is not claiming that he never logged into Playpen. Id. at 36. Therefore, the Government contends that the triggering event did, in fact, occur. Id.

Defendant's argument that the triggering event never occurred is novel, but the Court **FINDS** that logging into Playpen – which the warrant application identified by its URL – represents the relevant triggering event. See Def. Ex. 1A. Thus, the triggering event was not conditional upon the website's home page logo but upon whether a user or administrator of Playpen logged into the site, which the warrant identified by its URL. The FBI deployed the NIT here after someone with the username "Broden" logged into Playpen. Thus, the Court **FINDS** that the triggering event did occur.

The Court notes that if it were to rule that logging into Playpen through the home page – exactly as it was described in the application – represented the triggering event, as opposed to ruling that simply logging into the website represented the triggering event, such a ruling would provide operators of websites such as Playpen with incentive to frequently change their home pages' appearances. While this consideration would not be an issue if the FBI had assumed control over the website prior to obtaining the search warrant – as it had in this case – if the FBI

obtained a warrant to search computers logging into a site that the FBI had not yet taken over, the website operator's ability to change his or her website's home page at will would always defeat probable cause for this type of anticipatory warrant. Again it should be noted that the Government did not employ the NIT until Defendant took the additional step of clicking on an actual child pornography forum or section within Playpen.

VII. Rule 41(b)(4) Authorized the Issuance of the NIT Warrant

A. Legal Standards

Both Federal Rule of Criminal Procedure 41(b) ("Rule 41(b)") and Section 636 of the Federal Magistrates Act ("Section 636") concern the scope of a magistrate judge's authority. Rule 41(b) details a magistrate judge's authority to issue a search warrant. See Fed. R. Crim. P. 41(b). It provides that:

> (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:
>
> (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.

Fed. R. Crim. P. 41(b). Section 636(a) of the Federal Magistrates Act addresses a magistrate judge's jurisdiction and provides, in relevant part:

> (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. As the District of Massachusetts noted in Levin, "the Court's analyses of whether the NIT Warrant was statutorily permissible and whether it was allowed under Rule 41(b) are necessarily intertwined." 2016 WL 2596010, at *3. Indeed, "[f]or the magistrate judge to have had jurisdiction to issue the warrant under Section 636(a), she must have had authority to do so under Rule 41(b)." Id. at *8 n.11.

B. Analysis

i. Defendant Has Standing to Challenge the Magistrate Judge's Authority and Jurisdiction

In Rakas v. Illinois, the Supreme Court of the United States stressed that "'Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.'" 439 U.S. 128, 133–34 (1978) (quoting Brown v. United States, 411 U.S. 223, 230 (1973)). Therefore, a "person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed" and thus cannot

vicariously assert the third party's Fourth Amendment rights. Id. at 134. In Rakas, the Supreme Court held that passengers of a car who "asserted neither a property nor a possessory interest in the automobile, nor an interest in the property seized" could not vicariously assert the owner and driver's potential claims that the search of the car violated the Fourth Amendment. Id. at 130, 148.

The Government argues that Defendant does not have standing to assert these challenges to the NIT Warrant, characterizing his Third Motion as one "regarding how the issuance of the NIT warrant would apply to a third party found outside of the Eastern District of Virginia." See Doc. 53 at 6.

However, the Government deployed the NIT onto Defendant's own computer, and Defendant is challenging the warrant that purportedly authorized the Government to search that computer. Thus, Defendant possesses standing to challenge the warrant upon which the Government relied. Cf. United States v. Castellanos, 716 F.3d 828, 846 (4th Cir. 2013) (detailing ways in which defendants can and cannot establish standing to assert Fourth Amendment claims). This case is readily distinguishable from those holding that defendants cannot assert third parties' Fourth Amendment rights. Unlike the passengers in the car in Rakas, 439 U.S. at 134, Defendant obviously possesses an interest in his own computer, and he thus has standing to contest the NIT Warrant on any grounds he sees fit. As Defendant notes, he challenges the warrant "by demonstrating the invalidity of the warrant that purported to authorize this search." Doc. 55 at 2. Hence, the Court **FINDS** that Defendant possesses standing to challenge the NIT Warrant under Rule 41(b) and Section 636.

ii. The Magistrate's Authority and Jurisdiction

Defendant argues that the magistrate judge "ignored the clearly established jurisdictional limits set forth in Federal Rule of Criminal Procedure 41" in authorizing the search of computers located anywhere in the world. Doc. 24 at 5–6. Defendant alleges that a warrant issued without authority under Rule 41 necessarily leads to a constitutional violation of Section 636. Doc. 34 at 10; Doc. 55 at 3. The Government contends that Rule 41(b)(1), (2), and (4) support the issuance of the warrant and that a violation of Rule 41 does not automatically result in a constitutional violation. Doc. 53 at 12–16

Several courts have held that the magistrate judge lacked authority and jurisdiction to issue the NIT Warrant used in this case. E.g., Werdene, No. 2:15-cr-00434, ECF No. 33; Levin, 2016 WL 2596010, at *7; Arterbury, No. 15-182, ECF No. 47; Stamper, No. 1:15-cr-109, ECF No. 48; Michaud, 2016 WL 337263, at *6. As the Eastern District of Pennsylvania noted in Werdene, "the courts generally agree that the magistrate judge in Virginia lacked authority under Rule 41 to issue the warrant, [but] they do not all agree that suppression is required or even appropriate." No. 2:15-cr-00434, ECF No. 33 (collecting cases). The Court disagrees with the other courts that have considered this issue and **FINDS** that the magistrate judge did not exceed her authority under Rule 41(b).

The Court **FINDS** that Rule 41(b)(4) authorized the magistrate judge to issue this warrant. Rule 41(b)(4) endows a magistrate with authority to issue a warrant authorizing the use of a tracking device. Fed. R. Crim. P. 41(b)(4). The tracking device must be installed within the magistrate judge's district, but 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.

The Court recognizes that other courts have held this provision inapplicable to the NIT Warrant. See, e.g, Levin, 2016 WL 2596010, at *6; see also Michaud, 2016 WL 337263, at *6 (noting that "If the 'installation' occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because [the defendant] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on [the defendant's] computer, applying the tracking device exception again fails, because [the defendant's] computer was never physically located within the Eastern District of Virginia."). However, whenever someone entered Playpen, he or she made, in computer language, "a virtual trip" via the Internet to Virginia, just as a person logging into a foreign website containing child pornography makes "a virtual trip" overseas. Indeed, in Kyllo v. United States, the Supreme Court held that where "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." 533 U.S. 27, 40 (2001). The majority expressly rejected the dissent's attempts to distinguish "off-the-wall" home surveillance and "through-the-wall" observation. Id. at 35–36. Thus, in Kyllo, the Supreme Court likened the Government's electronic surveillance of a home via thermal imaging devices to the Government's physical entrance of the surveilled home. Id. at 40. Accordingly, when users entered Playpen, they came into Virginia in an electronic manner, just as the police in Kyllo entered a home in an electronic manner. Id.

Because the NIT enabled the Government to determine Playpen users' locations, it resembles a tracking device. Thus, the NIT Warrant authorized the FBI to install a tracking device on each user's computer when that computer entered the Eastern District of Virginia – the

magistrate judge's district. Contrary to the opinion conveyed in Michaud, 2016 WL 337263, at *6, the installation did not occur on the government-controlled computer but on each individual computer that entered the Eastern District of Virginia when its user logged into Playpen via the Tor network. When that computer left Virginia – when the user logged out of Playpen – the NIT worked to determine its location, just as traditional tracking devices inform law enforcement of a target's location. Furthermore, as far as this case is concerned, all relevant events occurred in Virginia. The magistrate judge who issued the warrant thus did so with authority under Rule 41(b)(1)(4).

Because the Court **FINDS** that the magistrate judge complied with Rule 41(b) in issuing this warrant, her actions did not contravene Section 636, because she exercised authority that was "conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts." 28 U.S.C. § 636(a)(1).

VIII. Even If the Magistrate Judge Issued the NIT Warrant Without Authority or Jurisdiction, Suppression Is Not Warranted

A. The Government Did Not Need a Warrant to Deploy the NIT

The Court **FINDS** that no Fourth Amendment violation occurred here because the Government did not need a warrant to capture Defendant's IP address. Therefore, even if the warrant were invalid or void, it was unnecessary, so no constitutional violation resulted from the Government's conduct in this case.

i. Legal Standards

The Fourth Amendment provides, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S.

Const. amend. IV. Although holding that the Fourth Amendment protects a person's "reasonable expectation of privacy," the Supreme Court cautioned in Katz v. United States that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'" 389 U.S. 347, 349, 360 (1967).

Traditionally, the privacy concerns embedded in the Fourth Amendment only applied to government actors' physical trespasses. See, e.g., United States v. Jones, 132 S. Ct. 945, 949–50 (2012). The Supreme Court, however, expanded the notion of privacy in Katz, and Justice Harlan in concurrence developed a two-part test, which courts now regularly use to determine whether an action violates the Fourth Amendment: (1) the person must have exhibited an actual (subjective) expectation of privacy, and (2) that expectation must be (objectively) reasonable. 389 U.S. at 361 (Harlan, J., concurring). Hence, to establish a violation of one's rights under the Fourth Amendment, a defendant "must first prove that he had a legitimate expectation of privacy in the place searched or the item seized." United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000). In order to so prove, the defendant "must show that his subjective expectation of privacy is one that society is prepared to accept as objectively reasonable." Id. (citing California v. Greenwood, 486 U.S. 35, 39 (1988)).

In Katz, the Supreme Court considered whether a reasonable expectation of privacy exists within an enclosed telephone booth. 389 U.S. at 349. Noting that "the Fourth Amendment protects people, not places," the Court held that the defendant possessed a reasonable expectation of privacy in the words he uttered while in the telephone booth. Id. at 351, 359. In Smith v. Maryland, however, the Supreme Court distinguished Katz, stressing that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith, 442 U.S. 735, 744 (1979). In Smith, the Supreme Court held that a defendant possessed

no expectation of privacy in the phone numbers he dialed, and that, therefore, the installation and use of a pen register to capture the dialed phone numbers did not constitute a search. Id. at 745. The Court noted that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company . . ." Id. at 742. Indeed, regardless of the defendant's location or of the steps he took to maintain privacy, he "had to convey that number to the telephone company . . ." Id. at 743. Thus, the Government did not need a warrant to use the pen register to capture the phone numbers the defendant dialed. Id. at 745. The Ninth Circuit in United States v. Forrester described the dichotomy between Katz and Smith as "a clear line between unprotected addressing information and protected content information." 512 F.3d 500, 510 (9th Cir. 2007).

Like information revealed to a third party, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Katz, 389 U.S. at 351. In California v. Ciraolo, the Supreme Court wrote that the "Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares." 476 U.S. 207, 213 (1986). The Court continued, "[n]or does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point . . ." Id. at 213. Even 1,000 feet above a home represents a "public vantage point" "[i]n an age where private and commercial flight in the public airways is routine." Id. at 215. The defendant in Ciraolo could not reasonably "expect that his marijuana plants," which he grew in his fenced-in backyard, "were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet." Id. at 215. The Court thus held that police officers who used a plane flown above the defendant's backyard to observe his illegal marijuana plants did not conduct a search in violation of the Fourth Amendment. Id.

Similarly, in Minnesota v. Carter, the Supreme Court considered whether a police officer who peered through a gap in a home's closed blinds conducted a search in violation of the Fourth Amendment. 525 U.S. 83, 85 (1998). Although the Court did not reach this question, id. at 91, Justice Breyer in concurrence determined that the officer's observation did not violate the respondents' Fourth Amendment rights. Id. at 103 (Breyer, J., concurring). Justice Breyer noted that the "precautions that the apartment's dwellers took to maintain their privacy would have failed in respect to an ordinary passerby standing" where the police officer stood. Id. at 104. He specified that whether the officer conducted an illegal search cannot turn "upon 'gaps' in drawn blinds. Whether there were holes in the blinds or they were simply pulled the 'wrong way' makes no difference." Id. at 105. "One who lives in a basement apartment that fronts a publicly traveled street, or similar space, ordinarily understands the need for care lest a member of the public simply direct his gaze downward," he continued. Id. Thus, Justice Breyer opined that peering into a gap in closed blinds is a permissible act under the Fourth Amendment. Id. at 103.

ii. Analysis

a. Defendant Has No Expectation of Privacy in His IP Address

The Court first focuses on the Government's discovery of Defendant's IP address, as the IP address ultimately led the Government to Defendant. Without the IP address, the Government presumably would have been unable to locate Defendant, even if the NIT had provided the FBI with the six other pieces of information seized. Here, the Court **FINDS** that Defendant possessed no reasonable expectation of privacy in his computer's IP address, so the Government's acquisition of the IP address did not represent a prohibited Fourth Amendment search.

Generally, one has no reasonable expectation of privacy in an IP address when using the Internet. See, e.g., Forrester, 512 F.3d at 509–11. This lack of a reasonable expectation of privacy stems from the fact that Internet users "should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." Id. at 510. The Ninth Circuit noted that "IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." Id.

Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address. Presumably, one using the Tor network hopes for, if not possesses, a subjective expectation of privacy in his or her identifying information. Indeed, Tor markets itself as a tool to "prevent[] people from learning your location . . ." See Tor Project: Anonymity Online, https://www.torproject.org (last visited May 24, 2016). However, such an expectation is not objectively reasonable in light of the way the Tor network operates. In United States v. Farrell, researchers operating the Tor nodes observed the IP address of the alleged operator of Silk Road 2.0, a Tor hidden service. No. CR15-029, 2016 WL 705197, at *1 (W.D. Wash. Feb. 23, 2016). Pursuant to a subpoena, the researchers turned over the information to law enforcement. Id. In finding no Fourth Amendment violation, the Western District of Washington noted that "in order for [] prospective user[s] to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations." Id. at *2. The Western District of Washington noted that under "such a system, an individual would necessarily be disclosing his identifying information to complete strangers." Id. Indeed, the Tor Project itself even warns visitors "that the Tor network has

vulnerabilities and that users might not remain anonymous." Id. The court concluded that "Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network." Id. The court cautioned, however, that its decision was limited to the fact that the researchers "obtained the defendant's IP address while he was using the Tor network and [the researchers were] operating nodes on that network, and not by any access to his computer." Id. Accordingly, a magistrate judge's report and recommendation in the Northern District of Oklahoma that considered whether Playpen users possessed reasonable expectations of privacy in their IP addresses stated that "[w]ere the IP address obtained from a third-party, the [c]ourt might have sympathy for" the position that the defendant did not possess a reasonable expectation of privacy in it; however, "here the IP address was obtained through use of computer malware that entered Defendant's home, seized his computer and directed it to provide information that the Macfarlane affidavit states was unobtainable in any other way." Arterbury, No. 15-cr-182, ECF No. 42.

Other courts, however, have not limited the reasonable expectation of privacy inquiry to whether the FBI acquired a defendant's IP address by accessing his computer or by obtaining the information from a cooperative third party. E.g., Werdene, No. 2:15-cr-00434, ECF No. 33. For example, in another case involving Playpen, the Eastern District of Pennsylvania found that the defendant "had no reasonable expectation of privacy in his IP address," because "[a]side from providing the address to Comcast, his internet service provider, a necessary aspect of Tor is the initial transmission of a user's IP address to a third-party." Id. The court noted in Werdene that "the type of third-party to which [the defendant] disclosed his IP address – whether a person or an 'entry node' on the Tor network – does not affect the [c]ourt's evaluation of his reasonable expectation of privacy." Id. Because the defendant "was aware that his IP address had been

conveyed to a third party, [] he accordingly lost any subjective expectation of privacy in that information." Id. Thus, the Eastern District of Pennsylvania found that since the defendant "did not have a reasonable expectation of privacy in his IP address, the NIT cannot be considered a 'search' within the meaning of the Fourth Amendment." Id. Similarly, the Western District of Washington in Michaud stated that the defendant "ha[d] no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, [his] assigned IP address, which ultimately led to [his] geographic location." 2016 WL 337263, at *7. The Western District of Washington likened the defendant's IP address to an unlisted telephone number that "eventually could have been discovered." Id.

It is clear to the Court that Defendant took great strides to hide his IP address via his use of the Tor network. However, the Court **FINDS** that any such subjective expectation of privacy – if one even existed in this case – is not objectively reasonable. SA Alfin testified that when a user connects to the Tor network, he or she must disclose his or her real IP address to the first Tor node with which he or she connects. This fact, coupled with the Tor Project's own warning that the first server can see "[t]his IP address is using Tor," destroys any expectation of privacy in a Tor user's IP address. See Tor Project: FAQ, https://www.torproject.org/docs/faq.html.en (last visited May 24, 2016); see also Farrell, 2016 WL 705197, at *2. And, as the Eastern District of Pennsylvania noted, the fact that the Tor network subsequently bounces users' IP addresses "from node to node within the Tor network to mask [users'] identit[ies] does not alter the analysis of whether" an expectation of privacy in the IP addresses exists. Werdene, No. 2:15-cr-00434, ECF No. 33.

The Court recognizes that the NIT used in this case poses questions unique from the conduct at issue in Farrell, 2016 WL 705197. In Farrell, the Government never accessed the

suspect's computer in order to discover his IP address, whereas here, the Government deployed a set of computer code to Defendant's computer, which in turn instructed Defendant's computer to reveal certain identifying information. The Court, however, disagrees with the magistrate judge in Arterbury, who focused on this distinction, see No. 15-cr-182, ECF No. 42. As the Court understands it, Defendant's IP address was not located on his computer; indeed, it appears that computers can have various IP addresses depending on the networks to which they connect. Rather, Defendant's IP address was revealed in transit when the NIT instructed his computer to send other information to the FBI. The fact that the Government needed to deploy the NIT to a computer does not change the fact that Defendant has no reasonable expectation of privacy in his IP address. See Werdene, No. 2:15-cr-00434, ECF No. 33. Thus, the Government's use of a technique that causes a computer to regurgitate certain information, thereby revealing additional information that the suspect already exposed to a third party – here, the IP address – does not represent a search under these circumstances. Therefore, the Government did not need to obtain a warrant before deploying the NIT and obtaining Defendant's IP address in this case, so any potential defects in the warrant or in the issuance of the warrant are immaterial.

b. Defendant Has No Reasonable Expectation of Privacy in His Computer

While the Court holds that the use of the NIT, which resulted in the Government's ultimate capture of Defendant's IP address, does not represent a prohibited search under the Fourth Amendment, the Court acknowledges that the warrant purported to authorize searches of "activating computers." See Def. Ex. 1A. Without deploying the NIT to a user's computer, the Government would not have been able to observe any Playpen user's IP address. Additionally, the Government obtained the six other pieces of identifying data from users' computers; unlike its acquisition of the IP addresses, which the FBI observed and captured during transmission of

the data, the FBI gathered this additional data directly from suspects' computers. To be sure, "the appropriate [Fourth Amendment] inquiry [is] whether the individual had a reasonable expectation of privacy in the area searched, not merely in the items found." E.g., United States v. Horowitz, 806 F.2d 1222, 1224 (4th Cir. 1986). Thus, the Court will address whether Defendant possessed a reasonable expectation of privacy not only in his IP address but also in his computer, the "place to be searched." Def. Ex. 1A. The Court **FINDS** that Defendant did not possess a reasonable expectation of privacy in his computer.

Examining the search of computers in the Fourth Amendment context, in 2007, the Ninth Circuit held that a defendant had both a subjective expectation of privacy and an objectively reasonable expectation of privacy in his personal computer, even though the defendant had connected that computer to a network. See United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007). The Ninth Circuit noted that a "person's reasonable expectation of privacy may be diminished in 'transmissions over the Internet or email that have already arrived at the recipient.'" Id. (quoting United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004)). "However, the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer." Id. (citing Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001)). The Ninth Circuit stressed that "privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user." Id. at 1147 (citing Simons, 206 F.3d at 398). Similarly, in United States v. Bruckner, the Fourth Circuit noted that one has a reasonable expectation of privacy in his password-protected home computer. 473 F.3d 551, 555 (4th Cir. 2007). In Trulock v. Freeh, the Fourth Circuit held that "password-protected files [on a computer] are analogous to [a] locked footlocker inside the

bedroom;" thus, the defendant "had a reasonable expectation of privacy in the password-protected computer files." 275 F.3d 391, 403 (2001). Conversely, in Simons, the Fourth Circuit found that a government employer's remote searches of an employee's computer did not violate the Fourth Amendment, because, in light of the employer's Internet policy – which stated that the employer would monitor employees' use of the Internet – the remote searches did not constitute prohibited searches under the Fourth Amendment. 206 F.3d at 398. The Fourth Circuit further noted that because the employee "lacked a legitimate expectation of privacy in his Internet use," he also lacked a reasonable expectation of privacy in his computer's hard drive. Id. at 399.

Here, the NIT was programmed to collect very limited information. Like the pen register in Smith that only captured the numbers dialed, 442 U.S. at 742, the NIT only obtained identifying information; it did not cross the line between collecting addressing information and gathering the contents of any suspect's computer. Cf. Forrester, 512 F.3d at 510. Indeed, the Government obtained a traditional residential search warrant before searching the computer's contents in this case. Plus, Defendant lacked any expectation of privacy in the main piece of information the NIT allowed the FBI to gather – his IP address. E.g., Michaud, 2016 WL 337263, at *7. Additionally, while the Government could have deployed the NIT as soon as a user logged into Playpen, SA Alfin testified that in this particular case, the FBI took the extra step of not deploying the NIT until after the suspect actually accessed child pornography. These facts support the conclusion that the NIT's deployment does not represent a prohibited search under the Fourth Amendment. Cf. Forrester, 512 F.3d at 511.

Additionally, like the employee in Simons who was put on notice that his computer was not entirely private, 206 F.3d at 398, Defendant here should have been aware that by going on

Tor to access Playpen, he diminished his expectation of privacy. The Ninth Circuit found in 2007 that connecting to a network did not eliminate the reasonable expectation of privacy in one's computer, Heckenkamp, 482 F.3d at 1146–47; however, society's view of the Internet – and our corresponding expectation of privacy not only in the information we post online but also in our physical computers and the data they contain – recently has undergone a drastic shift.

For example, hacking is much more prevalent now than it was even nine years ago, and the rise of computer hacking via the Internet has changed the public's reasonable expectations of privacy. Cf. Lee Raine, *How Americans balance privacy concerns with sharing personal information: 5 key findings*, PEWRESEARCHCENTER (January 14, 2016), http://www.pewresearch.org/fact-tank/2016/01/14/key-findings-privacy-information-sharing/ (reporting that members of a focus group "worried about hackers," though "some accept that [privacy tradeoffs are] a part of modern life"). Now, it seems unreasonable to think that a computer connected to the Web is immune from invasion. Indeed, the opposite holds true: in today's digital world, it appears to be a virtual certainty that computers accessing the Internet can – and eventually will – be hacked.

In the recent past, the world has experienced unparalleled hacks. For example, terrorists no longer can rely on Apple to protect their electronically stored private data, as it has been publicly reported that the Government can find alternative ways to unlock Apple users' iPhones. See Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, THE NEW YORK TIMES (March 28, 2016), http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html? _r=0. In addition to politicians being targets of hacking, see Nicole Gaouette, *Intel chief: Presidential campaigns under cyber attack*, CNN (May 18, 2016), http://www.cnn.com/2016/05/18/politics/presidential-campaigns-cyber-attack/index.html, Ashley

Madison, see Alex Hern, *Ashley Madison hack: your questions answered*, THE GUARDIAN (August 20, 2015), https://www.theguardian.com/technology/2015/aug/20/ashley-madison-hack-your-questions answered; Sony, see Peter Elkind, *Sony Pictures: Inside the Hack of the Century*, FORTUNE (July 1, 2015), http://fortune.com/sony-hack-part-1/; Home Depot, see Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, THE WALL STREET JOURNAL (Sept. 18, 2014), http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571; Target, see id.; the New York Times, see Nicole Perlroth, *Hackers in China Attacked The Times for Last 4 Months*, THE NEW YORK TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html; a Panamanian law firm, see *Panama Papers: Leak firm Mossack Fonseca 'victim of hack'*, BBC NEWS (April 6, 2016), http://www.bbc.com/news/world-latin-america-35975503; and even the United States Government, Associated Press in Washington, *US government hack stole fingerprints of 5.6 million federal employees*, THE GUARDIAN (September 23, 2015), https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints, all have experienced hacks that resulted in the compromise of unprecedented amounts of data previously thought to be private. In arguing that Defendant needs the exploit source code to determine whether Defendant's computer experienced a hack or whether an outside source tampered with the information the NIT sent to the FBI, defense counsel even admitted that such hacks could occur by agreeing that when information travels via the Internet in unencrypted form, "anybody can tamper with it." Doc. 86 at 38. Cases identifying a reasonable expectation of privacy in personal computer files protected with only a password, see Bruckner, 473 F.3d at 554; see also Trulock, 275 F.3d at 403, can be distinguished, because in 2016 it now appears unreasonable to expect that simply utilizing a password provides any

practical protection. E.g., Caitlin Dewey, *It's been six months since the Ashley Madison hack. Has anything changed?*, THE WASHINGTON POST (January 15, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/01/15/its-been-six-months-since-the-ashley-madison-hack-has-anything-changed/ ("There was always a chance that the Ashley Madison hack, far from waking people up to the dangers of data breaches, would further normalize them."). Indeed, it is "doubtlessly easier to dismiss hacks this way, as external inevitabilities that no one can really help, than to go through the trauma and unease of reassessing the way we collectively use the Web." Id.

Tor users likewise cannot reasonably expect to be safe from hackers. Even if Tor users hope that the Tor network will keep certain information private – just as terrorists seem to expect Apple to keep their data private – it is unreasonable not to expect that someone will be able to gain access. See John W. Little, *Tor and the Illusion of Anonymity*, BLOGS OF WAR (August 6, 2013), http://blogsofwar.com/tor-and-the-illusion-of-anonymity/ (describing that the Federal Government discovered a way "to identify the true IP addresses [of] an unknown number to Tor users" and noting that this development "should serve as a huge wake-up call" to people who believe that using Tor endows them with unassailable privacy protections). Notwithstanding the identification difficulties posed by Tor and the machinations one must undergo to access a Tor hidden service, advances in technology continue to thwart Tor's measures.

Thus, hacking resembles the broken blinds in Carter. 525 U.S. at 85. Just as Justice Breyer wrote in concurrence that a police officer who peers through broken blinds does not violate anyone's Fourth Amendment rights, id. at 103 (Breyer, J., concurring), FBI agents who exploit a vulnerability in an online network do not violate the Fourth Amendment. Just as the area into which the officer in Carter peered – an apartment – usually is afforded Fourth

Amendment protection, a computer afforded Fourth Amendment protection in other circumstances is not protected from Government actors who take advantage of an easily broken system to peer into a user's computer. People who traverse the Internet ordinarily understand the risk associated with doing so. Thus, the deployment of the NIT to capture identifying information found on Defendant's computer does not represent a search under the Fourth Amendment, and no warrant was needed.

Although this Court recently noted in dicta that the possibility of hacking "is not enough to defeat an individual's reasonable expectation of privacy" because it is illegal, see United States v. Darby, No. 2:16-cr-36, ECF No. 31 at 10–11 (E.D. Va. June 3, 2016), this Court stresses that child pornography often resembles an international crime. Similarly, much hacking occurs by foreign nations where the governments condone or participate in hacking. Child pornography is not just a national issue; it is an international issue, and at least a portion of the pornography in this case arrived from foreign sources through the World Wide Web.

The Fourth Circuit issued its *en banc* decision in United States v. Graham, No. 12-4659 (4th Cir. May 31, 2016), almost simultaneously with this Court's initial Opinion and Order, which it filed under seal on June 1, 2016. Doc. 75. Therefore, this Court did not have the opportunity to incorporate Graham, No. 12-4659, in its initial order. In Graham, the Fourth Circuit held that the Government's warrantless acquisition of historical cell-site location information ("CSLI") from the defendants' cell phone providers fell within the third-party doctrine. Id. Therefore, the Government's conduct did not constitute a search in violation of the Fourth Amendment. Id.

Although the Fourth Circuit in Graham stressed that the Government obtained the data from a third party and did not collect it through direct surveillance of the defendants, the opinion

does illustrate the Fourth Circuit's understanding that the right of privacy in electronic data is not absolute, and it further recognizes that the Government's use of technology must not be frozen in time but instead keep pace with rapidly developing technology. See id. n.16 (citing Skinner, 690 F.3d at 778 ("Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system.")). Though Graham does not constitute binding precedent for this Court's current decision, it certainly supports the concept that the privacy of an IP address diminishes when revealed to third parties and that the Government has a right to advance beside technology. Thus, in today's world, the locked footlocker referenced in Trulock, 275 F.3d at 403, would be more akin to a bag carried on an airplane as the owner travels the world with his private information on display.

Additionally, while the Court **FINDS** that the Government did not need a warrant before deploying the NIT, the Court recognizes the need to balance an individual's privacy in any case involving electronic surveillance with the Government's duty of protecting its citizens. Here, the balance weighs heavily in favor of surveillance.[3] The Government should be able to use the most advanced technological means to overcome criminal activity that is conducted in secret, and Defendant should not be rewarded for allegedly obtaining contraband through his virtual travel through interstate and foreign commerce on a Tor hidden service. E.g., Werdene, No. 2:15-cr-00434, ECF No. 33 (noting that the defendant "seeks to 'serendipitously receive Fourth Amendment protection' because he used Tor in an effort to evade detection, even though an

[3] In Riley v. California, the Supreme Court held that "a warrant is generally required before" searching information on a cell phone, "even when a cell phone is seized incident to arrest." 134 S. Ct. 2473, 2493 (2014). Importantly, the Government had searched the contents of an arrestee's cell phone in Riley, including photographs and videos. Id. at 2481. Here, however, the Government did not use the NIT to view anything beyond limited identifying information. Additionally, as the Eastern District of Michigan noted, Riley "did not generate a blanket rule applicable to any data search of any electronic device in any context." No. 15-20631, 2016 WL 894452, at *4 (E.D. Mich. Mar. 9, 2016). Instead, the Supreme Court "simply held that application of the search incident to arrest doctrine to [searches of digital data] would untether the rule from the justifications underlying it historically." Id. (internal quotations omitted). Therefore, Riley does not control the Court's decision in this case.

individual who does not conceal his IP address does not receive those same constitutional safeguards") (citing United States v. Stanley, 753 F.3d 114, 121 (3d Cir. 2014)). Society thus is unprepared to recognize any privacy interests Defendant attempts to claim as reasonable in his search for pornographic material; indeed, even businesses dealing with heavily regulated products such as liquor and firearms do not possess reasonable expectations of privacy in their interstate commerce activities. See United States v. Biswell, 406 U.S. 311, 316 (1972); see also Colonnade Catering Corp. v. United States, 397 U.S. 72, 74, 77 (1970). The Court **FINDS** that due to the especially pernicious nature of child pornography and the continuing harm to the victims,[4] the balance between any Tor user's alleged privacy interests and the Government's deployment of the NIT to access very limited identifying information weighs in favor of the Government's use of technology to counteract the measures taken by people who access child pornography online. The Government's efforts to contain child pornographers, terrorists and the like cannot remain frozen in time; the Government must be allowed to utilize its own advanced technology to keep pace with our world's ever-advancing technology and novel criminal methods.

B. Even If the Issuance of the Warrant Represented a Nonconstitutional Violation of Rule 41(b), Suppression Is Still Unwarranted

The parties agree that two categories of Rule 41 violations exist: "those involving constitutional violations and all others." Doc. 34 at 10; Doc. 53 at 23; Simons, 206 F.3d at 403. Without a constitutional violation, suppression is warranted "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." Simons, 206 F.3d at 403.

[4] The Court does note, however, that it appears some of the continuing harm in this case occurred because the Government continued operating Playpen, rather than immediately shutting it down. The Court has no role in deciding what methods the executive branch utilizes in fulfilling its duty to protect our citizens so long as its methods are constitutional.

As discussed above, any potential Rule 41 violation did not result in a violation of Defendant's constitutional rights, for no warrant was needed. Thus, the Government's use of the NIT did not deprive Defendant of his Fourth Amendment rights. The Court here **FINDS** that suppression is not appropriate for any potential nonconstitutional violation of Rule 41(b) either, because Defendant was not prejudiced and there is no evidence of intentional or deliberate disregard of the rule.

Defendant argues that the search conducted pursuant to the warrant would not have occurred had the magistrate judge not issued the warrant, and that, therefore, he has suffered prejudice. Doc. 34 at 14. However, as detailed above, the FBI did not need a warrant to deploy the NIT, so Defendant has not shown prejudice.

Additionally, Defendant has failed to show an intentional or deliberate disregard of Rule 41(b). As the Eastern District of Pennsylvania noted in Werdene, the "warrant was candid about the challenge that the Tor network poses, specifically its ability to mask a user's physical location." No. 2:15-cr-00434, ECF No. 33. The affidavit also specifically stated that the NIT may be deployed against an "activating computer – wherever located." Def. Ex. 1B ¶ 46. Thus, the Court **FINDS** that the FBI did not attempt to mislead the magistrate judge in any way as to the locations of the activating computers. Therefore, Defendant has shown neither prejudice nor an intentional violation of Rule 41(b), so even if there were a nonconstitutional violation of Rule 41(b), suppression would be inappropriate.

C. The Good Faith Exception

Finally, even if the Government did need to obtain a warrant in order to deploy the NIT, and even if there existed defects in the warrant or in its issuance, the Court **FINDS** that suppression still would be inappropriate under the good faith exception to the exclusionary rule.

Generally, if a search violates the Fourth Amendment, "the fruits thereof are inadmissible under the exclusionary rule, a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect." United States v. Doyle, 650 F.3d 460, 466 (4th Cir. 2011) (quoting United States v. Calandra, 414 U.S. 338, 348 (1974)) (internal quotations omitted). However, because exclusion is so drastic a remedy, it represents a "last resort." United States v. Stephens, 764 F.3d 327, 335 (4th Cir. 2014). Hence, in United States v. Leon, the Supreme Court established a good faith exception to the exclusionary rule. See 468 U.S. 897, 922 (1984). Under this exception, a court need not exclude evidence obtained pursuant to a later-invalidated search warrant if law enforcement's reliance on the warrant was objectively reasonable. Doyle, 650 F.3d at 467.

The Leon good faith exception applies in this case. The agents' reliance on the NIT Warrant was objectively reasonable, and it appears to the Court that the agents acted in good faith. An experienced and neutral magistrate judge reviewed the warrant application and concluded that there existed probable cause to issue the NIT Warrant. As noted above, the FBI did not intentionally or recklessly mislead the magistrate judge in its quest to obtain the NIT Warrant, either on the scope of the warrant or on the information concerning the logo change. The warrant application detailed ample probable cause to support the issuance of the warrant. The affidavit also adequately described the items to be seized and the places to be searched. The FBI agents showed no improper conduct or misjudgment in relying upon the NIT Warrant.

Therefore, the Leon good faith exception would apply, even if the NIT's deployment constituted a search and even if the warrant were deficient in some respect.

IX. CONCLUSION

For the reasons listed above, the Court **DENIES** Defendant's First and Third Motions to Suppress, Docs. 18, 34, and Defendant's Motion to Compel Discovery, Doc. 37. The Court **GRANTS** Defendant's Consent Motion for Leave to File an Expert Declaration Relevant to the Motion to Compel Discovery, Doc. 83, and the Government's Motion to Unseal the Court's Opinion and Order denying Defendant's First and Third Motions to Suppress, Doc. 89.

The Clerk is **DIRECTED** to deliver a copy of this Order to all counsel of record.

It is so **ORDERED**.

/s/
Henry Coke Morgan, Jr.
Senior United States District Judge

HENRY COKE MORGAN, JR.
SENIOR UNITED STATES DISTRICT JUDGE

Norfolk, Virginia
June 21, 2016