



June 30, 2020

Jonathan Manes  
Roderick & Solange MacArthur Justice Center  
160 East Grand Avenue, Sixth Floor  
Chicago, IL 60611

FOIPA Request No.: 1416471-000  
Civil Action No.: 18-cv-1488  
*Privacy International et al v. FBI et al*  
Subject: Hacking Techniques

Dear Mr. Manes:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Below you will find checked boxes under applicable statutes for the exemptions asserted to protect information exempt from disclosure. The appropriate exemptions are noted on the processed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely pursuant to applicable exemptions. An Explanation of Exemptions is enclosed to further explain justification for withheld information.

<b>Section 552</b>		<b>Section 552a</b>	
<input type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)	<input type="checkbox"/> (d)(5)	
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)	<input type="checkbox"/> (j)(2)	
<input type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)	<input type="checkbox"/> (k)(1)	
_____	<input type="checkbox"/> (b)(7)(D)	<input type="checkbox"/> (k)(2)	
_____	<input checked="" type="checkbox"/> (b)(7)(E)	<input type="checkbox"/> (k)(3)	
_____	<input type="checkbox"/> (b)(7)(F)	<input type="checkbox"/> (k)(4)	
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)	<input type="checkbox"/> (k)(5)	
<input checked="" type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)	<input type="checkbox"/> (k)(6)	
<input checked="" type="checkbox"/> (b)(6)		<input type="checkbox"/> (k)(7)	

300 pages were reviewed and 118 pages are being released.

Please see the paragraphs below for relevant information specific to your request and the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

- Documents were located which originated with, or contained information concerning, another Government Agency [OGA].
- This information has been referred to the OGA(s) for review and direct response to you.
- We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. "Part 1" of the Addendum includes standard responses that apply to all requests. "Part 2" includes additional standard responses that apply to all requests for records about yourself or any third party individuals. "Part 3" includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

Although your request is in litigation, we are required by law to provide you the following information:

If you are not satisfied with the Federal Bureau of Investigation's determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at [ogis@nara.gov](mailto:ogis@nara.gov); telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing [foipaquestions@fbi.gov](mailto:foipaquestions@fbi.gov). If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

Please direct any further inquiries about this case to the Attorney representing the Government in this matter. Please use the FOIPA Request Number and/or Civil Action Number in all correspondence or inquiries concerning your request.

See additional information which follows.

Sincerely,



Michael G. Seidel  
Acting Section Chief  
Record/Information  
Dissemination Section  
Information Management Division

Enclosures 3

Please be advised that as of June 8, the Record Information/Dissemination Section (RIDS) resumed operating at full staffing levels amidst the ongoing COVID-19 national emergency. The enclosed FOIPA release represents a work product that could be generated for you under these unprecedented circumstances and the limited time we were fully staffed during the month of June. We appreciate your patience and understanding as we work to release as much information, to as many requesters as possible, as this emergency continues.

This interim contains pages 18-cv-1488(FBI)-1133 – 18-cv-1488(FBI)-1432.

To minimize costs to both you and the FBI, duplicate copies of the same document were not processed.

## FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.

### Part 1: The standard responses below apply to all requests:

- (i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on the [www.fbi.gov/foia](http://www.fbi.gov/foia) website.
- (ii) **Intelligence Records.** To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that any such records do or do not exist.

### Part 2: The standard responses below apply to all requests for records on individuals:

- (i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.
- (ii) **Requests for Records about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.
- (iii) **Requests for Records for Incarcerated Individuals.** The FBI can neither confirm nor deny the existence of records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA exemptions (b)(7)(E), (b)(7)(F), and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (b)(7)(F), and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

### Part 3: General Information:

- (i) **Record Searches.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems or locations where responsive records would reasonably be found. A standard search normally consists of a search for main files in the Central Records System (CRS), an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. Unless specifically requested, a standard search does not include references, administrative records of previous FOIPA requests, or civil litigation files. For additional information about our record searches, visit [www.fbi.gov/services/information-management/foipa/requesting-fbi-records](http://www.fbi.gov/services/information-management/foipa/requesting-fbi-records).
- (ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.
- (iii) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheet. These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at [www.fbi.gov/about-us/cjis/identity-history-summary-checks](http://www.fbi.gov/about-us/cjis/identity-history-summary-checks). Additionally, requests can be submitted electronically at [www.edo.cjis.gov](http://www.edo.cjis.gov). For additional information, please contact CJIS directly at (304) 625-5590.
- (iv) **National Name Check Program (NNCP).** The mission of NNCP is to analyze and report information in response to name check requests received from federal agencies, for the purpose of protecting the United States from foreign and domestic threats to national security. Please be advised that this is a service provided to other federal agencies. Private Citizens cannot request a name check.

## EXPLANATION OF EXEMPTIONS

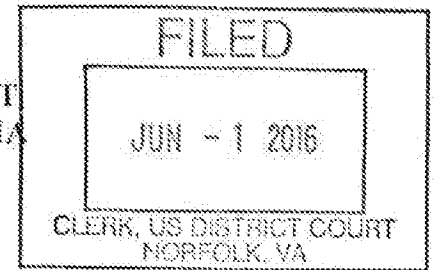
### SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information ( A ) could reasonably be expected to interfere with enforcement proceedings, ( B ) would deprive a person of a right to a fair trial or an impartial adjudication, ( C ) could reasonably be expected to constitute an unwarranted invasion of personal privacy, ( D ) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, ( E ) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or ( F ) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

### SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

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



UNITED STATES of AMERICA,

v.

Criminal No. 4:16cr16

\*\*UNDER SEAL\*\*

EDWARD JOSEPH MATISH, III,

Defendant.

OPINION & ORDER

This matter is before the Court on Defendant Edward Matish, III's ("Defendant" or "Matish") First Motion to Suppress ("First Motion"), Doc. 18, and Third Motion to Suppress ("Third Motion"), Doc. 34. Trial in this case is scheduled for June 14, 2016.

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.

In the Motions, 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.

Other courts across the country have considered various challenges to the particular warrant used in this case. See United States v. Michaud, No. 3:14-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016); United States v. Stamper, No. 1:15-cr-109, ECF No. 48 (S.D. Ohio Feb. 19, 2016); United States v. Levin, No. 15-10271, 2016 WL 2596010 (D. Mass. Apr. 20, 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. Werdene, No. 2:15-cr-00434, ECF No. 33 (E.D. Pa. May 18, 2016); United States v. Epich, No. 15-cr-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016).

The Court held hearings to address these Motions on May 19, 2016 and May 26, 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** that suppression is not warranted 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.

## 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 Agents Daniel Alfin and 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, <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, a Tor user's IP address remains 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 provides anonymity protections to both operators of a hidden service and to visitors of a hidden service. There exist 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, there are more than 1,000 servers all over the world in the Tor network. Because Tor users' IP addresses remain 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, subdivided 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 capable 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 instructions or 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 downloaded several images of 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 capable 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.

## **II. 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) (citing United States v. Leon, 468 U.S. 897, 958 (1084)). 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 describes Playpen's home page and registration terms in detail, and it details Playpen's content. See Def. Ex. 1B. Examining the totality of these circumstances leads to the conclusion that there existed a fair probability that those accessing Playpen intended to view and trade child pornography and that the NIT would help uncover evidence of 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 was justified in concluding 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 information that could be used to identify oneself. 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.”<sup>1</sup> 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 was indeed dedicated to child pornography. The affidavit also detailed sections, forums, and sub-forums visible upon logging into the site, most of which referenced

---

<sup>1</sup> “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.

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, 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] 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. 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. 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 at its face, the Court **CONCLUDES** that the magistrate judge possessed ample probable cause to issue the NIT Warrant.

### **III. 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. 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.

#### **IV. 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 Fed. Appx. 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.” Id. at 473 (citing 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 basis 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. (citing Epich, 2016 WL 953269, at \*2; Michaud, 2016 WL 337263, at \*4–5) (emphasis in original).

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 search 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 Agent 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.

## V. 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 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.

## **VI. 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 **CONCLUDES** 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. Levin, 2016 WL 2596010, at \*7; Arterbury, No. 15-182, ECF No. 47; Michaud, 2016 WL 337263, at \*6; Stamper, No. 1:15-cr-109, ECF No. 48; Werdene, No. 2:15-cr-00434, ECF No. 33. 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." Id.). However, whenever someone entered Playpen, he or she made "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. 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).

**VII. 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 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, 298 (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 v. Maryland, 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 may have held peering into a gap in closed blinds 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, <https://www.torproject.org> (last accessed 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 violation of the Fourth Amendment, 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 “This IP address is using Tor,” destroys any expectation of privacy in a Tor user’s IP address. See Tor, <https://www.torproject.org/docs/faq.html.en> (last accessed 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 just 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/> (last accessed May 24, 2016) (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 and 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](http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0) (last accessed May 24, 2016). 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> (last visited May 19, 2016), 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 (last accessed May 24, 2016); Sony, see Peter Elkind, *Sony Pictures: Inside the Hack of the Century*, FORTUNE (July 1, 2015), <http://fortune.com/sony-hack-part-1/> (last accessed May 24, 2016); 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> (last accessed May 24, 2016); Target, see id.; the New York Times, see Nicole Perloth, *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> (last accessed May 24, 2016); 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> (last accessed May 24, 2016); 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> (last accessed May 24, 2016), all have experienced hacks that resulted in the compromise of unprecedented amounts of data previously thought to be private. 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, no longer hold merit, 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/> (last accessed May 24, 2016) (noting that

“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/> (last accessed May 24, 2016) (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 – is usually 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.

**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.

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.

**VIII. Even if the Government Did Need to Obtain a Warrant, and Even if the NIT Warrant Were Invalid, the Good Faith Exception Applies**

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.

**A. Legal Standards**

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) (citing 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 Leon, the Supreme Court established a good faith exception to the exclusionary rule. See 468 U.S. at 922. Under this exception, the 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 Fourth Circuit has noted that there are four circumstances in which the Leon good faith exception will not apply:

- (1) if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;
- (2) if the issuing magistrate wholly abandoned

his judicial role in the manner condemned in Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979); (3) if the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) if under the circumstances of the case the warrant is so facially deficient – i.e., in failing to particularize the place to be searched or the things to be seized – that the executing officers cannot reasonably presume it to be valid.

Id. (citing United States v. DeQuasie, 373 F.3d 509, 519–20 (4th Cir. 2004) (quoting Leon, 468 U.S. at 923)) (internal quotations omitted).

## **B. Analysis**

None of the four exceptions to the Leon good faith exception apply in this case. As the Western District of Washington concluded, “[b]ecause reliance on the NIT Warrant was objectively reasonable, the officers executing the warrant acted in good faith, and suppression is unwarranted.” Michaud, 2016 WL 337263, at \*7. Indeed, an experienced and capable 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. Additionally, it does not appear to the Court that the experienced and capable magistrate judge abandoned her judicial role in issuing this warrant, and 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. Balance Considerations and Public Policy**

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.<sup>2</sup> 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 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 that the Government has subjected to seldom used regulation through prior restraint, see U.S. Const. amend. I, similar to how 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,<sup>3</sup> the balance between any Tor user's alleged privacy interests and the Government's deployment of a NIT to access very limited identifying information weighs in

---

<sup>2</sup> 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.

<sup>3</sup> 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 expresses no opinion on this particular police tactic, but it does note that when pictures of children appear online, the harm remains in perpetuity.

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; it must be allowed to utilize advanced technology to keep up with our world's ever-advancing technology and novel criminal methods.

**X. CONCLUSION**

For the reasons listed above, the Court **DENIES** Defendant's First and Third Motions to Suppress, Docs. 18, 34.

The Clerk is **DIRECTED** to maintain this Order **UNDER SEAL** and to deliver a copy of this Order to all counsel of record in a confidential manner.

It is so **ORDERED**.

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

\_\_\_\_\_  
HENRY COKE MORGAN, JR. *HCM*  
SENIOR UNITED STATES DISTRICT JUDGE

Norfolk, Virginia  
June 1, 2016



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT TACOMA

UNITED STATES OF AMERICA,  
  
Plaintiff,  
  
v.  
  
JAY MICHAUD,  
  
Defendant.

CASE NO. 3:15-cr-05351-RJB  
  
ORDER DENYING DEFENDANT’S  
MOTIONS TO SUPPRESS  
EVIDENCE

These matters come before the Court on Defendant’s Motion to Suppress Evidence (Dkt. 26) and Defendant’s Second Motion to Suppress Evidence and Motion for *Franks* Hearing (Dkt. 65). The Court has considered the parties’ responsive briefing and the remainder of the file herein, as well as the testimony of FBI Special Agent Daniel Alfin and Christopher Soghoian, Principal Technologist for the Speech and Technology Project at the American Civil Liberties Union, elicited at an evidentiary hearing held on January 22, 2016. Dkt. 47, 69, 90, 94, 111. Having orally denied Mr. Michaud’s motion for a *Franks* hearing (Dkt. 135), the sole issue before the Court, raised by both of Mr. Michaud’s motions, is whether to suppress evidence of what Mr. Michaud argues is fruit of an unreasonable search. At oral argument, the parties agreed

1 that the Court should decide the issue based on the submitted record, as supplemented by the  
2 testimony adduced at the hearing. *See* Dkt. 135.

### 3 I. FACTUAL BACKGROUND

#### 4 a. Website A

5 Mr. Jay Michaud, a resident of Vancouver, Washington, is charged with receipt and  
6 possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), (a)(4), (b)(1), and  
7 (b)(2). Dkt. 117. The charges against Mr. Michaud stem from Mr. Michaud's alleged activity on  
8 "Website A," a website that, according to the FBI, was dedicated to the advertisement and  
9 distribution of child pornography. Dkt. 47-5, at ¶¶14-16. Website A was created in August of  
10 2014, and by the time that the FBI shut the site down, on March 4, 2015, Website A had over  
11 200,000 registered member accounts and 1,500 daily visitors, making it "the largest remaining  
12 known child pornography hidden service in the world." Dkt. 47-1, at ¶19; Dkt. 50-1, at ¶3.

13 According to the three warrant applications submitted in this case, the main page of the  
14 site featured a title with the words, "Play Pen." Dkt. 47-1, at ¶¶12. *See also* Dkt. 47-5, at ¶¶18-  
15 37; Dkt 47-2, at ¶¶11-21. *See also* Dkt. 90-1, at 2. The main page, which required users to login  
16 to proceed, also featured "two images depicting partially clothed prepubescent females with their  
17 legs apart." *Id.* Text on the same page read, "No cross-board reposts, .7z preferred, encrypt  
18 filenames, include preview, Peace out." *Id.* "No cross-board reposts," appeared to prohibit the  
19 reposting of material from other websites, while ".7z preferred," referred to a preferred method  
20 of compressing large files. *Id.* After logging in, registered users would next view a page with  
21 hyperlinks to forum topics, the clear majority of which advertise child pornography. *Id.*, at ¶¶14-  
22 18. *See also* Dkt. 65-2, at 1-4.

#### 23 b. The Title III Warrant

24

1 On February 20, 2015, agents from the Federal Bureau of Investigation executed a Title  
2 III warrant to intercept the communications of Website A. Dkt. 47-5, at ¶¶4 and pp. 57-62.  
3 Website A operated on the Tor network, a publicly available alternative internet service that  
4 allows users to mask identifying information, such as Internet Protocol (“IP”) addresses. *Id.*, at  
5 ¶¶18-36. For approximately 14 days, from February 20, 2015 through March 4, 2015, the FBI  
6 administered Website A from a government-controlled computer server located in Newington,  
7 Virginia, which forwarded a copy of all website communications, through the server, to FBI  
8 personnel in Linthicum, Maryland. Dkt. 47-1, at ¶30; Dkt. 47-5, ¶¶38, 52 and p. 60. Based on the  
9 authority of the Title III warrant, the FBI captured communications of users accessing Website  
10 A, including user “Pewter.” The FBI apparently did not post any new content but allowed  
11 registered users to access the site and to continue to post content. *See id.*

12 *c. The NIT Warrant*

13 While controlling Website A, the FBI sought to identify the specific computers, and  
14 ultimately the individuals, accessing the site, by deploying a network investigating technology  
15 (“NIT”) that “cause(d) an activating computer—wherever located—to send to a computer  
16 controlled by or known to the government, network level messages containing information that  
17 may assist in identifying the computer, its location, [and] other information[.]” Dkt. 47-1, at 34.  
18 Prior to deploying the NIT, on February 20, 2015 the FBI sought and obtained a warrant (“the  
19 NIT Warrant”), which was issued by a magistrate judge in the Eastern District of Virginia. *Id.*  
20 The NIT Warrant cover sheet reads as follows:

21 “An application by a federal law enforcement officer . . . requests the search of  
22 the following person of property located in the Eastern District of  
Virginia (*identify the person or describe the property to be searched and give its  
location*):

23 See Attachment A

1 The person or property to be searched, described above, is believed to conceal  
(*identify the person or describe the property to be seized*):  
2 See Attachment B[.]” Dkt. 47-1, at 39.

3 Attachment A reads as follows:

4 Attachment A

5 Place to be Searched

6 This warrant authorizes the use of a network investigative technique (“NIT”) to be  
7 deployed on the computer server described below, obtaining information described in  
8 Attachment B from the activating computers below.

9 The computer server is the server operating the Tor network child pornography  
10 website referred to herein as the TARGET WEBSITE, as identified by its URL –  
11 [omitted]— which will be located at a government facility in the Eastern District of  
12 Virginia.

13 The activating computers are those of any user or administrator who logs into the  
14 TARGET WEBSITE by entering a username and password. The government will not  
15 employ this network investigative technique after 30 days after this warrant is authorized,  
16 without further authorization. *Id.*, at 37.

17 Attachment B reads as follows:

18 Attachment B

19 Information to be Seized

20 From any “activating” computer described in Attachment A:

- 21 1. the “activating” computer’s actual IP address, and the date and time that the  
22 NIT determines what that IP address is;

- 1 2. a unique identifier generated by the NIT (e.g., a series of numbers, letters,
- 2 and/or special characters) to distinguish data from that other “activating”
- 3 computers, that will be sent with and collected by the NIT;
- 4 3. the type of operating system running on the computer, including type (e.g.,
- 5 Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
- 6 4. information about whether the NIT has already been delivered to the
- 7 “activating” computer;
- 8 5. the “activating” computer’s Host Name;
- 9 6. the “activating” computer’s active operating system username; and
- 10 7. the “activating” computer’s media access control (“MAC”) address;
- 11 that is evidence of violations of . . . [child pornography-related crimes]. *Id.*, at 38.

12 Both Attachment A and Attachment B, which the NIT Warrant incorporated, are identical in  
 13 content to the attachments submitted in the warrant application. *Id.*, at 4, 5, 37, 38.

14 *d. Warrant issued in the Western District of Washington (“the Washington Warrant”)*

15 After obtaining the NIT warrant, the FBI deployed the NIT, obtaining the IP address and  
 16 other computer-related information connected to a registered user, “Pewter,” who allegedly  
 17 accessed Website A for 99 hours between October 31, 2014 and March 2, 2015. Dkt. 47-2, at  
 18 ¶26. “Pewter” had apparently accessed 187 threads on Website A, most related to child  
 19 pornography. *Id.*, at ¶27. With the IP address in hand, the FBI ultimately ascertained the  
 20 residential address associated with “Pewter,” an address at which Mr. Michaud resided, in  
 21 Vancouver, Washington. *Id.*, at ¶¶35, 36. A magistrate judge in the Western District of  
 22 Washington issued a warrant to search that address, and the FBI subsequently seized computers  
 23 and storage media allegedly containing contraband. *See generally, id.*

1 *e. Evidentiary testimony of SA Alfin and Dr. Christopher Soghoian*

2 SA Alfin's testimony explained how the NIT was deployed against Mr. Michaud. While  
3 the FBI administered Website A from a government-controlled computer, between February 20,  
4 2015 and March 4, 2015, a registered user, "Pewter," logged into Website A and accessed a  
5 forum entitled, "Preteen videos—girls HC." (HC stands for "hardcore.") The FBI setup the NIT  
6 so that accessing the forum hyperlink, not Website A's main page, triggered the automatic  
7 deployment of the NIT from the government-controlled computer in the Eastern District of  
8 Virginia, to Pewter's computer in Vancouver, Washington, where the NIT collected the IP  
9 address, MAC address, and other computer-identifying information, and relayed that information  
10 back to the government-controlled server in the Eastern District of Virginia, after which the  
11 information was forwarded to FBI personnel for data analysis.

12 SA Alfin also explained a discrepancy in the content of Website A's main page. While  
13 the warrant application for the NIT describes a main page featuring two prepubescent females  
14 with legs spread apart, Dkt. 47-1, at ¶12, by the time that the FBI submitted the warrant  
15 application, on February 20, 2015, the main page had been changed to display only one young  
16 female with legs together. *Compare* Dkt. 90-1, at 2 and Dkt. 90-1, at 4. According to SA Alfin,  
17 the main page changed several hours prior to the arrest of a Website A administrator, in the early  
18 evening hours of February 19, 2015. After the arrest, SA Alfin viewed Website A and other  
19 material on the administrator's computer, at which point SA Alfin saw the newer version of  
20 Website A's main page but did not notice the picture changes. The balance of Website A's focus  
21 on child pornography apparently remained unchanged, in SA Alfin's opinion. The new picture  
22 also appears suggestive of child pornography, especially when considering its placement next to  
23 the site's suggestive name, Play Pen.

1 Dr. Christopher Soghoian, testifying on behalf of Mr. Michaud, explained how the Tor  
2 network functions and theorized about how the NIT may have been deployed.

## 3 II. DISCUSSION

4 Mr. Michaud raises two<sup>1</sup> primary Fourth Amendment issues: whether deploying the NIT  
5 from the Eastern District of Virginia, to Mr. Michaud's computer, located outside that district,  
6 exceeded the scope of the NIT Warrant's authorization; and whether the NIT Warrant lacks  
7 particularity and amounts to a general warrant. In addition to those constitutional issues, Mr.  
8 Michaud raises the issue of a statutory violation, that is, whether the NIT Warrant violates Fed.  
9 R. Crim. P. Rule 41(b). Based on those issues, Mr. Michaud requests suppression of evidence  
10 secured through the NIT and all fruits of that search.

11 a. Whether deploying the NIT to a computer outside of the Eastern District of Virginia  
12 exceeded the scope of the NIT Warrant's authorization.

13 Mr. Michaud argues that the NIT Warrant authorized deployment of the NIT only to  
14 computers within one geographical location, the Eastern District of Virginia. Dkt. 65, at 15-17.  
15 Dkt. 139, at 3, 4. He asserts that because the FBI deployed the NIT to Mr. Michaud's computer,  
16 located outside of that district, the search and seizure exceeded the scope of the NIT Warrant. *Id.*

17 The Fourth Amendment to the United States Constitution provides that "no Warrants  
18 shall issue, but upon probable cause, supported by Oath or affirmation, and particularly  
19 describing the place to be searched, and the persons or things to be seized." If the execution of a  
20 search or seizure exceeds the scope of a warrant, the subsequent search or seizure is

---

21 <sup>1</sup> In his motion for a *Franks* hearing, Mr. Michaud raised a third constitutional issue,  
22 challenging the probable cause underlying the NIT Warrant, which the Court denied at oral  
23 argument. Dkt. 135. *See* Dkt. 65, at 5-15. However, even if the NIT Warrant was not supported  
24 by probable cause, as Mr. Michaud argued, reliance on the NIT Warrant was objectively  
reasonable, *see supra*, so suppression is not warranted. *U.S. v. Needham*, 718 F.3d 1190, 1194  
(9<sup>th</sup> Cir. 2013).

1 unconstitutional. *Horton v. California*, 496 U.S. 128, 140 (1990). Whether a search or seizure  
2 exceeds the scope of a warrant is an issue that is determined “through an objective assessment of  
3 the circumstances surrounding the issuance of the warrant, the contents of the search warrant,  
4 and the circumstances of the search.” *U.S. v. Hurd*, 499 F.3d 963, 966 (9th Cir 2007)(*internal*  
5 *quotations and citations omitted*).

6 Mr. Michaud’s argument requires an overly narrow reading of the NIT Warrant that  
7 ignores the sum total of its content. While the NIT Warrant cover sheet does explicitly reference  
8 the Eastern District of Virginia, that reference should be viewed within context:

9 “An application by a federal law enforcement officer . . . requests the  
10 search of the following person of property located in the     Eastern     District  
11 of     Virginia     (*identify the person or describe the property to be searched*  
*and give its location*):  
See Attachment A[.]” Dkt. 47-1, at 39.

12 The warrant explicitly invites the magistrate judge to “give its location” in the blank space  
13 provided, wherein the phrase, “See Attachment A,” is inserted. Attachment A, subtitled “Place to  
14 be Searched,” authorizes deployment of the NIT to “all activating computers,” defined as “those  
15 of any user or administrator who logs into [Website A] by entering a username and password.”  
16 *Id.* Attachment A refers to the Eastern District of Virginia as the location of the government-  
17 controlled computer server from which the NIT is deployed. *Id.* A reasonable reading of the NIT  
18 Warrant’s scope gave the FBI authority to deploy the NIT from a government-controlled  
19 computer in the Eastern District of Virginia against anyone logging onto Website A, with any  
20 information gathered by the NIT to be returned to the government-controlled computer in the  
21 Eastern District of Virginia.

22 The warrant application reinforces this interpretation, which is objectively reasonable.  
23 The warrant application, when detailing how the NIT works, explains that the NIT “may cause  
24



1 an activating computer—*wherever located*—to send to a computer controlled by or known to the  
2 government [in the Eastern District of Virginia], network level messages *containing information*  
3 *that may assist in identifying* the computer, *its location*, and other information[.]” Dkt. 47-1, at  
4 ¶46 (emphasis added). The execution of the NIT Warrant is also consistent with and supports this  
5 interpretation. *See* Dkt. 47-5, at ¶¶13-18. Because this interpretation is objectively reasonable,  
6 execution of the NIT Warrant consistent with this interpretation should be upheld, even if there  
7 are other possible reasonable interpretations. *Bergquist v. County of Cochise*, 806 F.2d 1364 (9th  
8 Cir. 1986) (*abrogated on other grounds by City of Canton, Ohio v. Harris*, 489 U.S. 378 (1989)).

9 b. Whether the NIT Warrant lacks specificity and amounts to a general warrant.

10 Mr. Michaud argues in the alternative that if the NIT Warrant did not limit the NIT’s  
11 deployment to computers within one geographic location, the Eastern District of Virginia, the  
12 NIT Warrant is also unconstitutional because it lacks specificity and amounts to a general  
13 warrant. Dkt. 65, at 17; Dkt. 111, at 20.

14 Whether a warrant lacks specificity depends on two factors, particularity and breadth.  
15 “Particularity means the ‘warrant must make clear . . . exactly what it is that he or she is  
16 authorized to search for and seize.’” *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702  
17 (9<sup>th</sup> Cir. 2009)(quoting *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 857 (9<sup>th</sup>  
18 Cir. 1991). Warrants do not lack particularity where they “describe generic categories of items . .  
19 . if a more precise description of the items . . . is not possible.” *Id.* (citing to *United States v.*  
20 *Spilotro*, 800 F.2d 959, 963 (9<sup>th</sup> Cir. 1986)). “Breadth” inquires as to whether the scope of the  
21 warrant exceeds the probable cause on which the warrant is based. *Id.*

22 As a threshold matter, it appears that even if Mr. Michaud was correct in arguing that the  
23 NIT Warrant is unconstitutional because it is a general warrant, suppression may not be required

1 because the officers acted in good faith when executing the warrant. *See supra*, II(c)(3). *See also*,  
2 *United States v. Negrete Gonzales*, 966 F.2d 1277, 1283 (9<sup>th</sup> Cir. 1992) (citing to *United States v.*  
3 *Leon*, 468 U.S. 897 (1984)). The NIT Warrant does not, however, lack sufficient specificity. The  
4 warrant states with particularity exactly what is to be searched, namely, computers accessing  
5 Website A. Dkt. 47-1, at 37. According to the warrant application upon which the NIT Warrant  
6 was issued, Website A is unmistakably dedicated to child pornography. Although the FBI may  
7 have anticipated tens of thousands of potential suspects as a result of deploying the NIT, that  
8 does not negate particularity, because it would be highly unlikely that Website A would be  
9 stumbled upon accidentally, given the nature of the Tor network.

10 The second factor, breadth, considers whether the NIT Warrant exceeded the probable  
11 cause on which it was issued. While the warrant application certainly provides background facts  
12 not found in the NIT Warrant itself, *compare* Dkt. 47-1, at 2-36 and Dkt. 47-1, at 37-40, the NIT  
13 Warrant does not authorize anything beyond what was requested by the warrant application. In  
14 fact, the NIT Warrant language found in Attachment A and Attachment B is identical to the  
15 scope of the warrant requested. *Id.*, at 4, 5, 37, 38. Both the particularity and breadth of the NIT  
16 Warrant support the conclusion that the NIT Warrant did not lack specificity and was not a  
17 general warrant.

18 c. Whether the NIT Warrant violates Fed. R. Crim. P. Rule 41(b).

19 Concerning Fed. R. Crim. P. Rule 41(b), Mr. Michaud makes three primary arguments:  
20 (1) the NIT Warrant violates the plain text of Rule 41(b), (2) the Rule 41(b) violation requires  
21 suppression, because the violation was the result of an intentional and deliberate disregard of  
22 Rule 41(b), and results in prejudice to Mr. Michaud, and (3) the good faith exception does not  
23 “save” the Rule 41(b) violation because it does not apply. Dkt. 26, at 8-16; Dkt. 69, at 3-11.

1       ***1. Plain text of Rule 41(b).***

2       According to Mr. Michaud, the NIT Warrant violates the general provision of Rule 41(b),  
3 subdivision (b)(1), because the rule prohibits the magistrate judge in the Eastern District of  
4 Virginia from issuing a warrant to search or seize a computer outside of her district, including  
5 Vancouver, Washington. Dkt. 26, at 11-13. Mr. Michaud also argues against the applicability of  
6 the rule's other subdivisions, which carve out exceptions for searches outside of the district. Dkt.  
7 26, at 13, 14.

8       18 U.S.C. § 3103, which governs the grounds for issuing search warrants, directly  
9 incorporates Rule 41(b). Subdivision (b)(1) states the general rule, that “a magistrate with  
10 authority in the district . . . has the authority to issue a warrant to search for and seize a person or  
11 property located within the district.” Fed. R. Crim. P. 41(b)(1). Exceptions apply where a person  
12 or property “might move or be moved outside the district before the warrant is executed,”  
13 subdivision (b)(2), when federal law enforcement investigates terrorism, subdivision (b)(3),  
14 when a tracking device installed within the district travels outside the district, subdivision (b)(4),  
15 and where the criminal activities occur on a United States territory, commonwealth, or other  
16 location under the control of the United States other than a state, subdivision (b)(5).

17       Rule 41(b) is to be applied flexibly, not rigidly. *United States v. Koyomejian*, 970 F.2d  
18 536, 542 (9<sup>th</sup> Cir. 1992). In *United States v. New York Tel. Co.*, 434 U.S. 159 (1977), the  
19 Supreme Court addressed the general relationship of technology and Rule 41, concluding that  
20 Rule 41 “is sufficiently flexible to include within its scope electronic intrusions authorized upon  
21 a finding of probable cause.” *Id.*, at 169. The *New York Tel. Co.* court noted that a flexible  
22 reading of Rule 41 is reinforced by Fed. R. Crim. P. 57(b), which provides that in the absence of  
23 controlling law, “a judge may regulate practice in any manner consistent with federal law, these  
24

1 rules and the local rules[.]” *Id.*, at 170.<sup>2</sup> Although *New York Tel. Co.* addressed a now-  
2 superseded subdivision of Rule 41 and a different technology, the pen register, the flexibility  
3 applied to Rule 41 has since been applied to subsection (b) of Rule 41. *See, e.g., Koyomejian*,  
4 970 F.2d at 542.

5 In this case, even applying flexibility to Rule 41(b), the Court concludes that the NIT  
6 Warrant technically violates the letter, but not the spirit, of Rule 41(b). The rule does not directly  
7 address the kind of situation that the NIT Warrant was authorized to investigate, namely, where  
8 criminal suspects geographical whereabouts are unknown, perhaps by design, but the criminal  
9 suspects had made contact via technology with the FBI in a known location. In this context, and  
10 when considering subdivision (b)(1), a cogent, but ultimately unpersuasive argument can be  
11 made that the crimes were committed “within” the location of Website A, Eastern District of  
12 Virginia, rather than on personal computers located in other places under circumstances where  
13 users may have deliberately concealed their locations. However, because the object of the search  
14 and seizure was Mr. Michaud’s computer, not located in the Eastern District of Virginia, this  
15 argument fails. In a similar vein, a reasonable, but unconvincing argument can be made that  
16 subdivision (b)(2) applies, given the interconnected nature of communications between Website  
17 A and those who accessed it, but because Mr. Michaud’s computer was not ever physically  
18 within the Eastern District of Virginia, this argument also fails.

---

19  
20  
21 <sup>2</sup> Although not argued by the parties, a flexible interpretation of Rule 41(b) that accounts  
22 for changes in technology may also reconcile Rule 41(b) with 18 U.S.C. § 3103a, which provides  
23 that “[I]n addition to the grounds for issuing a warrant [under Rule 41(b)], a warrant may be  
24 issued . . . for . . . any property that constitutes evidence of a criminal offense.” As the parties  
appeared to agree at oral argument, § 3103a was enacted to codify the elimination of the mere  
evidence rule overturned in *Warden v. Hayden*, 387 U.S. 294 (1967), but neither party offered a  
satisfactory explanation to reconcile § 3103a with § 3103 and Rule 41(b).

1 Finally, applying subdivision (b)(4), which allows for tracking devices installed within  
2 one district to travel to another, stretches the rule too far. If the “installation” occurred on the  
3 government-controlled computer, located in the Eastern District of Virginia, applying the  
4 tracking device exception breaks down, because Mr. Michaud never controlled the government-  
5 controlled computer, unlike a car with a tracking device leaving a particular district. If the  
6 installation occurred on Mr. Michaud’s computer, applying the tracking device exception again  
7 fails, because Mr. Michaud’s computer was never physically located within the Eastern District  
8 of Virginia. The Court must conclude that the NIT Warrant did technically violate Rule 41(b),  
9 although the arguments to the contrary are not unreasonable and do not strain credulity.

10 **2. Prejudice to Mr. Michaud and intentional and deliberate disregard of Rule 41(b).**

11 Rule 41(b) violations are categorized as either fundamental, when of constitutional  
12 magnitude, or technical, when not of constitutional magnitude. *Negrete-Gonzales*, 966 F.2d at  
13 1283. As concluded above, the NIT Warrant did not fail for constitutional reasons, but rather  
14 was the product of a technical violation of Rule 41(b). Sec. II(c)(1). In cases where a technical  
15 Rule 41(b) violation occurs, courts may suppress where a defendant suffers prejudice, “in the  
16 sense that the search would not have occurred . . . if the rule had been followed,” or where law  
17 enforcement intentionally and deliberately disregarded the rule. *United States v. Weiland*, 420  
18 F.3d 1062, 1071 (9<sup>th</sup> Cir. 2005) (citing to *United States v. Martinez-Garcia*, 397 F.3d 1205, 1213  
19 (9<sup>th</sup> Cir. 2005)).

20 In this case, suppression is not warranted on the basis of the technical violation of Rule  
21 41(b), because the record does not show that Mr. Michaud was prejudiced or that the FBI acted  
22 intentionally and with deliberate disregard of Rule 41(b). First, considering the prejudice, Mr.  
23 Michaud would have the Court interpret the definition of prejudice found in *Weiland* and  
24

1 elsewhere, “in the sense that the search would not have occurred . . . if the rule had been  
2 followed,” to mean that defendants suffer prejudice whenever a search occurs that violates Rule  
3 41(b). This interpretation makes no sense, because under that interpretation, all searches  
4 executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter  
5 how small or technical the error might be. Such an interpretation would defeat the need to  
6 analyze prejudice separately from the Rule 41(b) violation. Tracing the origin of the definition  
7 used in *Weiland* to its early use in the Ninth Circuit yields a more sensible interpretation of the  
8 well-established definition: “in the sense that the search would not have occurred . . . if the rule  
9 had been followed” suggests that courts should consider whether the evidence obtained from a  
10 warrant that violates Rule 41(b) could have been available by other lawful means, and if so, the  
11 defendant did not suffer prejudice. *See United States v. Vasser*, 648 F.2d 507, 511 (9th Cir.  
12 1980).

13 Applying that interpretation here, Mr. Michaud did not suffer prejudice. Mr. Michaud has  
14 no reasonable expectation of privacy of the most significant information gathered by deployment  
15 of the NIT, Mr. Michaud’s assigned IP address, which ultimately led to Mr. Michaud’s  
16 geographic location. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Although  
17 the IP addresses of users utilizing the Tor network may not be known to websites, like Website  
18 A, using the Tor network does not strip users of all anonymity, because users accessing Website  
19 A must still send and receive information, including IP addresses, through another computer,  
20 such as an Internet Service Provider, at a specific physical location. Even though difficult for the  
21 Government to secure that information tying the IP address to Mr. Michaud, the IP address was  
22 public information, like an unlisted telephone number, and eventually could have been  
23 discovered.

1 Mr. Michaud also fails to show that the FBI acted intentionally and with deliberate  
2 disregard of Rule 41(b). Mr. Michaud's arguments to the contrary rely only on thin inferences,  
3 which are insufficient. Mr. Michaud argues that the Rule 41(b) violation of the NIT Warrant,  
4 which was predicated on the FBI's warrant application, was so obvious that the mere submission  
5 of the warrant application shows an intent to disregard the rule. The NIT Warrant did technically  
6 violate Rule 41(b), but reasonable, although unavailing arguments can be made to the contrary.  
7 *See infra*, II(a) and (c)(2). Mr. Michaud points to one opinion by a magistrate judge, who denied  
8 a similar warrant application seeking authorization to search "Nebraska and elsewhere," as  
9 evidence of intent and deliberate disregard, but that magistrate judge, who sits in one of ninety-  
10 four judicial districts, ruled on an unsettled area of the law where there is no controlling circuit or  
11 Supreme Court precedent. *See United States v. Cottom* Findings and Recommendations,  
12 Nebraska CR13-0108JFB. *See also*, Dkt. 69-1; Dkt. 111-2. Mr. Michaud also argues intent and  
13 deliberate disregard are shown by that the fact that the Government has elsewhere argued that  
14 Rule 41(b) should be amended to account for changes in technology, but this argument also fails,  
15 given that reasonable minds can differ as to the degree of Rule 41(b)'s flexibility in uncharted  
16 territory. *See also*, Fed. R. Crim. P. 57(b).<sup>3</sup>

17 **3. Good faith.**

18 Mr. Michaud also argues that, because the NIT Warrant violated Rule 41(b) and the  
19 Constitution, suppression is required because the good faith exception does not apply; and that  
20 the FBI did not execute the NIT Warrant in good faith.

---

21  
22  
23 <sup>3</sup> It appears clear that Fed. R. Crim. P. 41 or 18 U.S.C. § 3103 should be modified to  
24 provide for issuance of warrants that involve modern technology. Furthermore, said rule only  
applies to magistrate judges and state judges, and does not address limits on warrants issued by  
other federal judicial officers.

1 Where a warrant is executed in good faith, even if the warrant itself is subsequently  
2 invalidated, evidence obtained need not be suppressed. *United States v. Leon*, 468 U.S. 897, 922  
3 (1984). Warrants may be invalidated for technical or fundamental (constitutional) violations. *See*  
4 *id.*, at 918 (technical violation) and *Negrete-Gonzales*, 966 F.2d at 1283 (constitutional  
5 violation). Whether a warrant is executed in good faith depends on whether reliance on the  
6 warrant was objectively reasonable. *Id.*, at 922.

7 ““Searches pursuant to a warrant will rarely require any deep inquiry into  
8 reasonableness.”” *Leon*, at 922 (quoting *Illinois v. Gates*, 462 U.S., 213, 267 (1983)).  
9 Nonetheless, reliance on the NIT Warrant was objectively reasonable. *See infra*, II(a) and (c)(2).  
10 Mr. Michaud’s argument that the good faith exception does not apply, because *Weiland*  
11 overrules *Negrete-Gonzales*, which explicitly analyzed good faith in the context of a Rule 41(b)  
12 violation, is unavailing. Although the *Weiland* court makes no mention of good faith, it did not  
13 reach the issue, because it affirmed a lower court’s finding that suppression was not appropriate  
14 where there was no showing of a Rule 41(b) violation of constitutional magnitude, prejudice to  
15 the defendant, or intentional and deliberate disregard of the rule. *Id.*, at 1072. Because reliance  
16 on the NIT Warrant was objectively reasonable, the officers executing the warrant acted in good  
17 faith, and suppression is unwarranted.

### 18 III. CONCLUSION

19 “The Fourth Amendment incorporates a great many specific protections against  
20 unreasonable searches and seizures. The contours of these protections in the context of  
21 computer searches pose difficult questions.” *United States v. Adjani*, 452 F.3d 1140, 1152  
22 (9th Cir. 2006)(*internal quotations and citations omitted*). What was done here was  
23 ultimately reasonable. The NIT Warrant was supported by probable cause and  
24



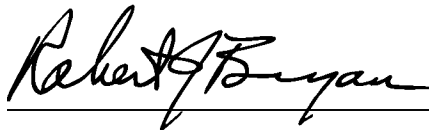
1 particularly described the places to be searched and the things to be seized. Although the  
2 NIT Warrant violated Rule 41(b), the violation was technical in nature and does not  
3 warrant suppression. Mr. Michaud suffered no prejudice, and there is no evidence that  
4 NIT Warrant was executed with intentional and deliberate disregard of Rule 41(b).  
5 Instead, the evidence shows that the NIT Warrant was executed in good faith. Mr.  
6 Michaud's motions to suppress should be denied.

7 \* \* \*

8 THEREFORE, it is HEREBY ORDERED that Defendant's Motion to Suppress Evidence  
9 (Dkt. 26) is DENIED. Defendant's Second Motion to Suppress Evidence and Motion for *Franks*  
10 Hearing (Dkt. 65) is DENIED.

11 The Clerk is directed to send uncertified copies of this Order to all counsel of record and  
12 to any party appearing *pro se* at said party's last known address.

13 Dated this 28<sup>th</sup> day of January, 2016.

14 

15 ROBERT J. BRYAN  
16 United States District Judge

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION**

United States of America,

Plaintiff,

v.

Case No. 1:15cr109

Richard Stamper,

Judge Michael R. Barrett

Defendant.

**OPINION & ORDER**

This matter is before the Court upon Defendant's Motion to Dismiss or Alternatively Suppress Evidence. (Doc. 33, SEALED). The Government filed a Response. (Doc. 34, SEALED). This Court held a hearing on the Motion on January 28, 2016. (Doc. 38). Defendant filed a Supplemental Post-Hearing Memorandum. (Doc. 39). The Government filed a Supplemental Memorandum (Doc. 40), to which Defendant filed a Response (Doc. 41, SEALED).

**I. BACKGROUND**

Defendant Richard Stamper has been charged with receipt and possession of child pornography in violation of 18 U.S.C. § 2252(a)(2), (a)(4), (b)(1) and (b)(2). These charges stem from an investigation conducted by Special Agents with the Federal Bureau of Investigation ("FBI") which led to the discovery of a website known as "Playpen." The Government alleges that the website, also referred to as "Website A" or "Target Website," contains child pornography. Website A was operating on an internet network known as

the Tor, or “the Onion Router.” The Tor network allows users to hide identifying information such as Internet Protocol addresses (“IP addresses”). One court has described how the Tor functions:

Tor directs internet traffic through a free, worldwide network of relays to conceal a user's location or usage from anyone attempting network surveillance or traffic analysis. Tor involves the application of layers of encryption (nested like layers of an onion) to anonymize communication by sending the original data to its destination without revealing the source IP address making it impossible to trace the communications back through the network to the actual user who sent the communication.

*United States v. Pierce*, No. 8:13CR106, 2014 WL 5173035, at \*3 (D. Neb. Oct. 14, 2014). Because Website A was operating on the Tor, as opposed to the “open” internet, the website could only be accessed if the user knew the web address of the website. (See Doc. 33-1, NIT Search Warrant Aff. ¶10).

Based on information from foreign law enforcement, the FBI determined that the computer server which hosted Website A was located at a web-hosting facility in North Carolina. (Doc. 33-1, NIT Search Warrant Aff. ¶ 28). The FBI obtained a Title III warrant to seize the server containing Website A. (Id.) The FBI allowed Website A to continue to operate, but assumed administrative control of the website from a government-controlled server located in Newington, Virginia. (See Doc. 33-1, NIT Search Warrant Aff. ¶ 30).<sup>1</sup>

FBI agents also obtained a search warrant from a magistrate judge in the Eastern District of Virginia authorizing the use of a “network investigative technique” (“NIT”) to be

---

<sup>1</sup>The NIT warrant itself stated that upon seizure of the server, the server operating Website A “will be located at a government facility in the Eastern District of Virginia.” (See Doc. 33-1, Attachment A).

deployed on the computer server. (Doc. 33-1, Attachment A) (“the NIT warrant”). The NIT warrant provided that once the NIT was deployed on the computer server, it would obtain information from the activating computers. (Id., Attachment A). Activating computers are the computers of users or administrators who log in with a user name and password to Website A. (Id.) Each time a user or administrator logged in to Website A, the NIT attempted to cause the activating computer to send specific information to a government-controlled computer located in the Eastern District of Virginia. (Doc. 33-1, NIT Search Warrant Aff. ¶ 36).

The NIT warrant limited the information to be seized by the NIT from the activating computers to information listed in Attachment B to the warrant: 1) the activating computer’s “actual IP address and the date and time that the NIT determines what the IP address is;” 2) “a unique identifier generated by the NIT...to distinguish data from that of other ‘activating’ computers;” 3) the type, version and architecture of the operating system running on the computer; 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.” (Doc. 33-1, Attachment B).

As a result of the NIT warrant, the FBI discovered that on February 3, 2015, a user registered for an account on Website A using the username “billnyepedoguy.” (Doc. 32-1, Residential Search Warrant Affidavit, ¶ 27). The Government explains that according to the statistics section of this user’s profile, the user “billnyepedoguy” had been actively logged into the website for a total of four hours, one minute and 57 seconds,

between February 3, 2015 and March 4, 2015. (Id.) The FBI also identified the IP address and MAC Address used by “billnyepedoguy” to log into Website A; and determined “billneypedoguy” used the host name of “badass” and log-on ID of “richard.” (Id., ¶ 28).

Using publicly available websites, the FBI was able to determine that the IP address associated with the user “billnyepedoguy” was operated by the internet service provider Time Warner Cable. (Doc. 32-1, Residential Search Warrant Affidavit, ¶ 34). An administrative subpoena was served on Time Warner Cable requesting information related to the user who was assigned to the IP address during the dates and times the user “billnyepedoguy” was accessing Website A. (Id.) The results of the subpoena showed that Defendant was the subscriber of the IP address. (Id., ¶ 35). In September of 2015, law enforcement agents obtained a search warrant from a magistrate judge in this district for Defendant’s home. Defendant has challenged this residential search warrant in a separate motion. (See Doc. 32, Motion to Suppress Evidence Seized Pursuant to SD Ohio Search Warrant).

Defendant moves to dismiss the indictment in this matter, or alternatively to suppress the evidence seized pursuant to the NIT warrant issued in the Eastern District of Virginia. Defendant argues that the magistrate judge in the Eastern District of Virginia did not have jurisdiction to issue a warrant allowing a NIT search of a computer in the Southern District of Ohio, or in any jurisdiction outside of the Eastern District of Virginia. Defendant explains that as a result, this Court must dismiss the indictment in this case. In the alternative, Defendant requests that the Court suppress the evidence seized as a

result of the NIT warrant and the fruits of that search based on violations of the Fourth Amendment.

## II. ANALYSIS

### A. Fourth Amendment

The Fourth Amendment prohibits “unreasonable searches and seizures” and provides that “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 text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is reasonableness.” *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995) (internal quotation marks omitted).

The Sixth Circuit has recognized the difficulty in applying the Fourth Amendment’s particularity requirement in the context of a search of a computer: “[t]he problem with applying this [requirement] to computer searches lies in the fact that [ ] images could be nearly anywhere on the computers. Unlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents.” *United States v. Evers*, 669 F.3d 645, 653 (6th Cir. 2012) (quoting *United States v. Richards*, 659 F.3d 527, 538, n.8 (6th Cir. 2011)). As a consequence:

given the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies, the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed the Fourth Amendment’s bedrock principle of reasonableness on a case-by-case basis: “While officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant, ... a computer search may be as

extensive as reasonably required to locate the items described in the warrant based on probable cause.” *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir.), *cert. denied*, 558 U.S. 1097, 130 S.Ct. 1028, 175 L.Ed.2d 629 (2009) (citations and internal quotation marks omitted).

*Id.* (quoting *Richards*, 659 F.3d at 538 (footnotes omitted)); *see also United States v. Ganas*, 755 F.3d 125, 134 (2d Cir. 2014) (“Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government’s modern, more sophisticated investigative tools.”); *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006) (“The fact of an increasingly technological world is not lost upon us as we consider the proper balance to strike between protecting an individual’s right to privacy and ensuring that the government is able to prosecute suspected criminals effectively.”).

Defendant’s Motion centers on Federal Rule of Criminal Procedure 41(b). Defendant argues that under Rule 41(b), a magistrate judge’s authority to issue a search warrant is limited to their own judicial district except under certain narrow circumstances.<sup>2</sup>

---

<sup>2</sup>Federal Rule of Criminal Procedure 41(b) provides in relevant part:

(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism

Defendant explains that none of those circumstances exist in this case.

The Sixth Circuit has explained “[a]lthough the purpose of Rule 41 is the implementation of the fourth amendment, the particular procedures it mandates are not necessarily part of the fourth amendment.” *United States v. Searp*, 586 F.2d 1117, 1121 (6th Cir. 1978), *cert. denied* 440 U.S. 921 (1979). Even where there is a failure to comply with Rule 41, a search may nevertheless be “reasonable” in the constitutional sense and meet the requirements of the Fourth Amendment. *Id.* at 1122. For this reason, the Sixth Circuit has instructed that “[v]iolations of Rule 41 alone should not lead to exclusion unless (1) there was ‘prejudice’ in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.” *Id.* at 1125 (quoting

---

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.



*United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir.1975)).

The handful of federal courts which have addressed the issue agree with Defendant and have found that a search warrant authorizing the use of a NIT does not comply with Rule 41.<sup>3</sup> However, these courts, with one exception, have found that the search is nevertheless “reasonable” and does not violate the Fourth Amendment.

**B. Judicial precedent and NIT search warrants**

**1. *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013).**

In *In re Warrant to Search a Target Computer at Premises Unknown*, an unknown person accessed a personal email account and used that email address to access the bank account of a man residing within the jurisdiction of the federal district court for the Southern District of Texas. 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013). The IP address of the computer which accessed these accounts came from a foreign country, but the location of the suspects and their computer was unknown. *Id.* The government requested a warrant authorizing: (1) a search for the target computer itself, and (2) a search for digital information stored on (or generated by) that computer. *Id.* at 757. The government sought to install data extracting software that had “the capacity to search the computer’s hard drive, random access memory, and other storage media; to activate the computer’s built-in camera; to generate latitude and longitude coordinates for the computer’s location; and to transmit the extracted data to the FBI.” *Id.* at 755.

---

<sup>3</sup>The absence of a provision permitting these types of searches has prompted calls for revisions to be made to Rule 41. See Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 Akron L. Rev. 315, 344 (2015) (explaining that the Department of Justice has proposed a change to Rule 41 to authorize search warrants using NITs).

The magistrate judge denied the application for the search warrant on three different grounds. First, the magistrate judge concluded that the warrant application did not satisfy any of the territorial limits found in Federal Rule of Criminal Procedure 41(b). The magistrate judge rejected the government's argument that the search warrant satisfied Rule 41(b)(1)—which authorizes a magistrate judge to issue a warrant to search property located within the district—because the information obtained from the target computer would be examined by the government within the magistrate judge's judicial district. *Id.* at 756. The magistrate judge explained:

The "search" for which the Government seeks authorization is actually two-fold: (1) a search for the Target Computer itself, and (2) a search for digital information stored on (or generated by) that computer. Neither search will take place within this district, so far as the Government's application shows. Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location. Before that digital information can be accessed by the Government's computers in this district, a search of the Target Computer must be made. That search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name. Since the current location of the Target Computer is unknown, it necessarily follows that the current location of the information on the Target Computer is also unknown. This means that the Government's application cannot satisfy the territorial limits of Rule 41(b)(1).

*Id.* at 757 (footnote omitted).

Next, the magistrate judge found that the warrant application did not satisfy the particularity requirement of the Fourth Amendment because the government failed to give any explanation of how the target computer would be found, or how the government's search technique would avoid infecting innocent computers and devices. *Id.* at 758-59.

Finally, the magistrate judge noted that the software described in the warrant

application would be able to access the computer's build-in camera to engage in "photo monitoring." *Id.* at 769. The magistrate judge explained that this type of access amounts to video surveillance, and would need to satisfy the Fourth Amendment warrant standards for video surveillance. *Id.* at 759-760. The magistrate judge concluded that the government had not met these standards. *Id.* at 760. Specifically, the government had not shown that other alternative investigative techniques were inadequate or that steps would be taken to minimize over-collection of data. *Id.*<sup>4</sup>

The magistrate judge noted that "there may well be a good reason to update the territorial limits of [Rule 41(b)] in light of advancing computer search technology." *Id.* at 761. However, the magistrate judge explained that "the extremely intrusive nature of such a search requires careful adherence to the strictures of Rule 41 as currently written, not to mention the binding Fourth Amendment precedent for video surveillance." *Id.* at 761.

**2. *United States v. Pierce*, 2014 WL 5173035 (D. Neb. Oct. 14, 2014).**

A year later, in *United States v. Pierce*, the federal district court for Nebraska denied a motion to suppress evidence derived from a NIT search warrant. Nos. 8:13CR106, 8:13CR107, 8:13CR108, 2014 WL 5173035, at \*3 (D. Neb. Oct. 14, 2014). The warrant authorized the FBI to deploy a NIT on a child pornography website operating from computers in Nebraska that used the Tor network for anonymity. *Id.* Once the NIT was installed on the website and the user accessed the website, the NIT sent out one or

---

<sup>4</sup>With regards to alternatives, the magistrate judge noted that "contemporaneous with this warrant application, the Government also sought and obtained an order under 18 U.S.C. § 2703 directing the Internet service provider to turn over all records related to the counterfeit email account, including the contents of stored communications." 958 F. Supp. 2d at 760.

more communications to the user's computer. *Id.* The user's computer then delivered information, such as the IP address, to a computer controlled by the FBI. *Id.* Administrative subpoenas were issued to the internet service providers to identify the owners of the IP addresses, which led to individual search warrants and charges against the defendants. *Id.*

The defendants did not challenge the probable cause for the issuance of the NIT warrant. *Id.* Instead, the defendants argued that the language in the warrant providing for notice to be delayed for thirty days violated Federal Rule of Criminal Procedure 41. *Id.* The court rejected this argument because the warrant clearly contemplated a period of thirty days after the discovery of an IP address to determine ownership of the computer connected to that address. *Id.* at \*4. In the alternative, the court concluded that the defendants failed to demonstrate prejudice or reckless disregard of proper procedure.<sup>5</sup>

**3. *United States v. Reibert*, 2015 WL 366716 (D. Neb. Jan. 27, 2015).**

A few months later, in *United States v. Reibert*, the federal district court for the District of Nebraska again denied a motion to suppress evidence derived from a NIT search warrant. No. 8:13CR107, 2015 WL 366716, at \*2 (D. Neb. Jan. 27, 2015). The NIT search warrant authorized the government to deploy the NIT on a website which was dedicated to advertising and distributing child pornography. *Id.* at \*4. The website operated on the Tor network in order to mask the users' actual IP addresses. *Id.* Once the NIT was deployed, each time a user accessed the website, the NIT sent one or more

---

<sup>5</sup>The court explained that under Eighth Circuit law: "when the government does not comply with the requirements of Rule 41, exclusion is warranted only if: (1) the defendant can demonstrate that he was prejudiced, or (2) 'reckless disregard of proper procedures is evident.'" 2014 WL 5173025, at \*5 (quoting *United States v. Spencer*, 439 F.3d 905, 913 (8th Cir. 2006)).

communications to the user's computer which would then cause the computer to send information, such as its IP address, to a government-controlled computer. *Id.* at \*5. Based on this information, the FBI obtained a residential search warrant for the defendant's home in Ohio. *Id.*

The defendant argued that the government conducted a warrantless search by employing a NIT. *Id.* at \*1. The defendant also argued that the NIT search warrant lacked probable cause. *Id.* The court rejected these arguments and cited Eighth Circuit caselaw which found probable cause existed where child pornography is traced to the defendant using an IP address. *Id.* at \*3. In the alternative, the court concluded that even if the NIT search warrant was not supported by probable cause, the good faith exception to the exclusionary rule identified in *United States v. Leon*, 468 U.S. 897, 922 (1984), would apply. *Id.* at \*3.

**4. *United States v. Welch*, 2016 WL 240775 (8th Cir. Jan. 21, 2016).**

Just a few weeks ago, the Eighth Circuit affirmed the district court's denial of the motion to suppress in *United States v. Pierce*, 2014 WL 5173035 (D. Neb. Oct. 14, 2014). On appeal, one of the co-defendants argued that the district court erred in admitting evidence obtained as a result of the NIT search warrant because he was provided notice beyond thirty days in violation of Federal Rule of Criminal Procedure 41. *United States v. Welch*, 2016 WL 240775, at \*2 (8th Cir. Jan. 21, 2016).

The Eighth Circuit began its analysis by noting: "Importantly, a Rule 41 violation amounts to a violation of the Fourth Amendment warranting exclusion 'only if a defendant is prejudiced or if reckless disregard of proper procedure is evident.'" *Id.* (quoting *United*

*States v. Spencer*, 439 F.3d 905, 913 (8th Cir. 2006)). The Eighth Circuit assumed, without deciding, that Rule 41 applied to the NIT search warrant. *Id.* at \*3. The court explained that it was still an open question as to whether the defendant's IP address—which is generated by a third party and assigned by the internet service provider—is the kind of “information” considered to be property under Rule 41. *Id.* at n.4. The court concluded that the notice given to the defendant did not comport with Rule 41. *Id.* However, the court concluded that the delay in notice appeared to be an error made in good faith and not a deliberate procedural violation. *Id.* The court also concluded that there was no evidence of prejudice: “Nothing in the record indicates that had the officers followed Rule 41 they would not have been able to search Welch's residence and obtain the evidence they did. The nature of the investigation indicates they could have easily obtained extensions had they sought them.” *Id.* at \*4. Therefore, the court concluded that the delayed notice to the defendant of the NIT warrant did not violate the Fourth Amendment. *Id.*

**5. *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).**

More recently, on January 28, 2016, the federal district court for the Western District of Washington denied a motion to suppress evidence based on the same NIT search warrant which is being challenged in this case. *United States v. Michaud*, No. 3:15CR5351, 2016 WL 337263, \*3 (W.D. Wash. Jan. 28, 2016).

The defendant in *Michaud* raised two Fourth Amendment arguments: whether deploying the NIT from the Eastern District of Virginia, to the defendant's computer, located outside that district, exceeded the scope of the NIT warrant's authorization; and

whether the NIT warrant lacks particularity and amounts to a general warrant. *Id.* at \*3. The defendant also argued that the NIT warrant violated Federal Rule of Criminal Procedure 41(b).

As to the first argument, regarding the scope of the NIT warrant, the court explained: “Whether a search or seizure exceeds the scope of a warrant is an issue that is determined ‘through an objective assessment of the circumstances surrounding the issuance of the warrant, the contents of the search warrant, and the circumstances of the search.’” *Id.* at \*3 (quoting *U.S. v. Hurd*, 499 F.3d 963, 966 (9th Cir. 2007)). The court explained that “while the NIT Warrant cover sheet does explicitly reference the Eastern District of Virginia, that reference should be viewed within context.” *Id.* at \*4.<sup>6</sup> The court explained that in the blank space on the warrant where the magistrate judge is to “give its location,” the blank has been filled in with “See Attachment A.” *Id.* The court explained further that:

Attachment A, subtitled “Place to be Searched,” authorizes deployment of the NIT to “all activating computers,” defined as “those of any user or administrator who logs into [Website A] by entering a username and password.” *Id.* Attachment A refers to the Eastern District of Virginia as the location of the government-controlled computer server from which the NIT is deployed. *Id.* A reasonable reading of the NIT Warrant’s scope gave the FBI authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto

---

<sup>6</sup>The cover sheet for the warrant stated:

An application by a federal law enforcement officer...requests the search of the following person of property located in the Eastern District of Virginia (*identify the person or describe the property to be searched and give its location*):

See Attachment A

*Id.* at \*4.

Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia.

*Id.* The court explained that the warrant application reinforces this objectively reasonable interpretation because when detailing how the NIT works, the warrant application explains that the NIT “may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government [in the Eastern District of Virginia], *network level messages containing information that may assist in identifying the computer, its location, and other information[.]*” *Id.* (emphasis added).

As to the second argument, that the NIT warrant lacks particularity and amounts to a general warrant, the court explained that whether a warrant lacks specificity depends on two factors: particularity and breadth. *Id.* (citing *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009)). The court concluded that the NIT warrant was not lacking in particularity and did not exceed the breadth—or scope—of the probable cause on which it was based. *Id.* at \*5. The court also concluded that even if the NIT Warrant was unconstitutional because it is a general warrant, suppression may not be required under *United States v. Leon*, 468 U.S. 897 (1984) because the officers were acting in good faith when executing the warrant. *Id.*

As to the final argument, that the NIT warrant violates Rule 41(b), the court found that the NIT technically violated the letter, but not the spirit of the rule. *Id.* The court explained: “The rule does not directly address the kind of situation that the NIT Warrant was authorized to investigate, namely, where criminal suspects geographical whereabouts are unknown, perhaps by design, but the criminal suspects had made contact via technology with the FBI in a known location.” *Id.* at \*6.



The court explained that because there was a technical violation of the Rule, and not a violation of a constitutional magnitude: “courts may suppress where a defendant suffers prejudice, ‘in the sense that the search would not have occurred...if the rule had been followed,’ or where law enforcement intentionally and deliberately disregarded the rule.” *Id.* (quoting *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005)). The court clarified that “prejudice” meant considering “whether the evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means.” *Id.* (citing *United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980)).

The court found that the defendant did not suffer prejudice:

Mr. Michaud has no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, Mr. Michaud's assigned IP address, which ultimately led to Mr. Michaud's geographic location. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Although the IP addresses of users utilizing the Tor network may not be known to websites, like Website A, using the Tor network does not strip users of all anonymity, because users accessing Website A must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a specific physical location. Even though difficult for the Government to secure that information tying the IP address to Mr. Michaud, the IP address was public information, like an unlisted telephone number, and eventually could have been discovered.

*Id.* at \*7. The court also found that the FBI did not act intentionally and with deliberate disregard of Rule 41(b). *Id.* Therefore, the court found that even if the NIT warrant was invalid, the FBI executed the warrant in good faith under *United States v. Leon*, 468 U.S. 897 (1984). *Id.* Accordingly, the court denied the defendant's motions to suppress. *Id.* at \*8.

### **C. The NIT search warrant in this case**

Defendant argues that *Michaud* is distinguishable because the district court in that case is applying Ninth Circuit caselaw. Defendant argues that even under the Ninth Circuit's analysis, suppression of evidence is warranted because Defendant suffered prejudice and law enforcement deliberately disregarded Rule 41(b). Finally, Defendant argues that the good faith exception does not save the warrant because the warrant was facially insufficient and it is clear from the facts that the agents knew the limits of the territorial jurisdiction of the court and ignored them when they obtained and executed the warrant.

#### **1. Scope of the NIT Search Warrant**

There is little to distinguish the facts of this case from *Michaud*. The Court also notes that there is little difference between the Ninth Circuit and the Sixth Circuit with regards to the applicable caselaw. Finally, the Court finds that the legal conclusions reached by the court in *Michaud* are in line with the courts which have addressed similar NIT search warrants. The Court finds *Michaud* persuasive.

The Court agrees that "a reasonable reading of the NIT Warrant's scope gave the FBI authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia." *Michaud*, 2016 WL 337263, \*4. The Sixth Circuit has explained that "when examining the legitimacy of search warrants, we are to follow a commonsensical and practical approach, as opposed to an overly technical review." *United States v. Bennett*,

170 F.3d 632, 639 (6th Cir. 1999) (citing *United States v. Ventresca*, 380 U.S. 102, 108, 85 S.Ct. 741, 746, 13 L.Ed.2d 684 (1965)). When the Government sought the NIT warrant, Website A was being operated from a government-controlled computer in the Eastern District of Virginia. While the NIT did send information to the activating computers, this only occurred after a user logged into the website. Any information sent by the activating computer was sent back to the Eastern District of Virginia. The information sent by the activating computer was limited and specified in the NIT warrant. This process was described in great detail in the NIT Search Warrant Affidavit:

In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the TARGET WEBSITE, which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the TARGET WEBSITE, located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other information.

(Doc. 33-1, Search Warrant Aff. ¶ 33). Defendant has not argued that the search conducted by the FBI agents went beyond the scope of what was described in the warrant.<sup>7</sup>

Moreover, the Court finds that the NIT Warrant was reasonable in the scope of the information searched. For this reason, this case is distinguishable from *In re Warrant to*

---

<sup>7</sup>Therefore, it is unnecessary for the Court to analyze whether the NIT Warrant amounted to a "general warrant." See *United States v. Garcia*, 496 F.3d 495, 507 (6th Cir. 2007) ("The test for determining if the officers engaged in an impermissible general search is whether their search unreasonably exceeded the scope of the warrant.") (citing *Brindley v. Best*, 192 F.3d 525, 531 (6th Cir. 1999)).

*Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013), where the issuance of the warrant was denied. In that case, the government sought to install data extracting software that had “the capacity to search the computer’s hard drive, random access memory, and other storage media; to activate the computer’s built-in camera; to generate latitude and longitude coordinates for the computer’s location; and to transmit the extracted data to the FBI.” *Id.* at 755. Here, the search was much less invasive. The information seized by the NIT from the activating computer did not include any information stored on the activating computer or even the location of the computer. The information seized did include the IP address, which did not identify the user of Website A until the FBI agents found the name of the internet service provider and then requested the name of the subscriber through an administrative subpoena. It was not until FBI agents secured a residential search warrant from a magistrate judge in this district that the agents were able to search the content of Defendant’s computer. Therefore, the Court concludes that the NIT Warrant was not unconstitutional in its scope and there is no basis to dismiss the indictment in this case, or suppress the evidence seized as a result of the NIT warrant.

## **2. Good faith**

However, even if the Court were to find that the NIT Search Warrant was unconstitutional because the use of the NIT allowed the FBI to extend its search to computers located outside of the Eastern District of Virginia, the Court finds that suppression is not required. The *Leon* good-faith exception, “which allows admission of evidence ‘seized in reasonable, good-faith reliance on a search warrant that is

subsequently held to be defective,” applies in this case. See *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). Only in exceptional circumstances is the good faith exception inappropriate: (1) if the issuing magistrate was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) if the issuing magistrate failed to act in a neutral and detached fashion and merely served as a rubber stamp for the police; (3) if the affidavit was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable, or where the warrant application was supported by nothing more than a bare bones affidavit; and (4) if the warrant was facially deficient in that it failed to particularize the place to be searched or the things to be seized. *Id.* at 914-15, 923.

Defendant argues that reliance on the warrant was not objectively reasonable because the warrant was facially deficient. Defendant argues that the NIT Warrant failed to particularize the place to be searched or the things to be seized because the FBI agents knew the limits of the territorial jurisdiction of the court and ignored them when they obtained and executed the warrant. Defendant relies on *United States v. Glover*, 736 F.3d 509 (D.C. Cir. 2013) to support his argument.

In *Glover*, the court found a wiretap warrant facially invalid because it authorized the placement of a listening device, or electronic “bug” on the target vehicle while it was outside the court’s jurisdiction. *Id.* at 515. While it may be tempting to analogize the “bug” to the NIT in this case, under that analogy, the NIT was “attached” to activating computers when the user logged into Website A, which was being operated from the

Eastern District of Virginia. It would be as if the users travelled to the Eastern District of Virginia, picked up the bug while they were there, and then carried it back home with them. The Court is not persuaded that the court's conclusion in *Glover* is applicable here. Therefore, the Court finds that even if the NIT Warrant is unconstitutional, the *Leon* good-faith exception allows the admission of the evidence seized as the result of the NIT.

**3. Rule 41(b)**

Finally, the Court finds that the NIT Warrant technically violates Rule 41(b). *Accord Michaud*, 2016 WL 337263, at \*6. However, exclusion is not necessary because there has not been a showing of prejudice or an intentional and deliberate disregard of the Rule. *See United States v. Searp*, 586 F.2d at 1121.

Defendant maintains that he has established prejudice based on two statements in the NIT Search Warrant Affidavit:

Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or "nodes," . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and failed or reasonably appear to be unlikely to succeed if they are tried. (Doc. 33-1, Search Warrant Aff. ¶ 31).

The government further submits that, to the extent that the use of the NIT can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation. (Doc. 33-1, Search Warrant Aff. ¶ 41).

Defendant argues that based on these statements, the search of his computer would not have occurred if Rule 41(b) had been followed. The Court disagrees. The information

seized by the NIT did not lead to Defendant directly. Instead, the FBI Agents only learned Defendant's IP Address as a result of the NIT Warrant. Defendant did not suffer prejudice by having this information revealed. This Court agrees with the court in *Michaud* on this point:

Mr. Michaud has no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, Mr. Michaud's assigned IP address, which ultimately led to Mr. Michaud's geographic location. See *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Although the IP addresses of users utilizing the Tor network may not be known to websites, like Website A, using the Tor network does not strip users of all anonymity, because users accessing Website A must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a specific physical location. Even though difficult for the Government to secure that information tying the IP address to Mr. Michaud, the IP address was public information, like an unlisted telephone number, and eventually could have been discovered.

*Michaud*, 2016 WL 337263, at \*7; see also *Smith v. Maryland*, 442 U.S. 735, 743-44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) (“[The Supreme] Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”); *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010) (“Federal courts have uniformly held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.”) (internal quotation marks and citations omitted).

Next, the Court finds that there is no evidence of intentional and deliberate disregard of Rule 41(b). The government specifically requested a search warrant authorizing that “the NIT may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government, network level messages

containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer, as described above and in Attachment B.” (Doc. 33-1, NIT Search Warrant Affidavit ¶ 46) (emphasis added).

Therefore, even though the NIT Warrant technically violates Rule 41(b), exclusion is not necessary.

### III. **CONCLUSION**

Based on the foregoing, Defendant’s Motion to Dismiss or Alternatively Suppress Evidence (Doc. 33, SEALED) is **DENIED**.

**IT IS SO ORDERED.**

*/s/ Michael R. Barrett*

---

Michael R. Barrett, Judge  
United States District Court



IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA,

v.

GABRIEL WERDENE,

*Defendant.*

CRIMINAL ACTION  
NO. 15-434

PAPPERT, J.

MAY 18, 2016

**MEMORANDUM**

Gabriel Werdene (“Werdene”) was indicted on September 17, 2015 on one count of possessing and attempting to possess child pornography pursuant to 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). The indictment was based on evidence obtained during a June 17, 2015 search of Werdene’s Bensalem, Pennsylvania home, which was conducted in accordance with a warrant issued by a magistrate judge in this judicial district. The Federal Bureau of Investigation (“FBI”) identified Werdene after a magistrate judge in Virginia issued a warrant permitting agents to deploy software that revealed the IP addresses of visitors to a child pornography website called Playpen.<sup>1</sup> FBI agents matched Werdene’s Playpen username, “thepervert,” to his IP address and then located his home in Bensalem based on that information.

Playpen’s patrons accessed the website through software called “Tor,” an acronym for “The onion router.” Tor conceals the IP addresses of people who visit certain websites, in Werdene’s case a website purveying child pornography. Otherwise stated, Tor enables people to use websites like Playpen to view, upload and share child pornography without being identified by traditional law enforcement investigative methods. To circumvent Tor, the FBI used a

---

<sup>1</sup> The parties refer to Playpen as “Website A,” ostensibly to preserve the anonymity of the site during the continued investigation of its users and administrators. A number of published articles and judicial opinions, *see infra* Section I.E, have already identified “Website A” as Playpen, eliminating the need for any further efforts to conceal its identity.

Network Investigative Technique (“NIT”). The NIT caused software to be activated whenever a Playpen user logged into the website with his username and password. The software caused the Playpen user’s computer to reveal its IP address to the FBI. The search warrant issued by the Virginia magistrate authorized the NIT.

Werdene moves to suppress the evidence seized from his home, arguing primarily that the magistrate judge in Virginia lacked jurisdiction under Federal Rule of Criminal Procedure 41 to authorize the NIT. Werdene contends that this violation of a procedural rule warrants suppression. While Rule 41 did not authorize the issuance of the warrant in Virginia, suppression is not the appropriate remedy. The magistrate judge’s failure to comply with Rule 41 did not violate Werdene’s Fourth Amendment rights because Werdene had no expectation of privacy in his IP address, and certainly not one that society would recognize as reasonable. Even if Werdene’s constitutional rights were violated, the good faith exception to the exclusionary rule precludes suppression. Finally, any nonconstitutional violation of Rule 41 did not prejudice Werdene, as that term has been defined by the Third Circuit Court of Appeals in the Rule 41 context. The Court denies the motion.

## I.

Playpen operated on the “dark web,” a collection of websites that use anonymity tools to hide those websites’ IP addresses and mask the identity of their administrators. Websites on the dark web can only be accessed using certain software such as Tor. (*See* Gov’t. Mem. in Opp. to Def.’s Mot. to Suppress (“Gov’t’s Opp.”), Ex. 1 ¶¶ 7–10, ECF No. 21.) Playpen, as its name connotes in this context, was “dedicated to the advertisement and distribution of child pornography, [and] the discussion of matters pertinent to child sexual abuse.” (*Id.*, Ex. 1 ¶ 6.) The website’s home page displayed an image of two partially clothed prepubescent females with

their legs spread. (*Id.*, Ex. 1 ¶ 12.) Upon arriving at the home page, a user was prompted to either register an account or login using his pre-existing username and password. (*Id.*) Prior to registering an account, a message was displayed which told the user, among other things, “NOT [to] . . . enter a real [email] address” and “[f]or your security you should not post information here that can be used to identify you.” (*Id.*, Ex. 1 ¶ 13.) The message also stated that “[t]his website is not able to see your IP address and can not [sic] collect or send any other form of information to your computer except what you expressly upload.” (*Id.*)

After successfully registering and logging into the site, the user reached a page which listed a number of “forums” or discussion boards on which users could post images, videos or text regarding various topics. The “forums” included “Jailbait – Boy,” “Jailbait – Girl,” “Preteen – Boy,” “Preteen – Girl,” “Jailbait Videos,” “Jailbait Photos,” “Pre-teen Videos,” “Pre-Teen Photos,” “Family – Incest” and “Toddlers.” (*Id.*, Ex. 1 ¶ 14.) Within the pre-teen videos and photos forums were “subforums” titled “Girls [hardcore],” “Boys [hardcore],” “Girls [softcore/non-nude]” and “Boys [softcore/non-nude].”<sup>2</sup> (*Id.*) Each forum contained a topic with titles, an author and the number of replies and views. (*Id.*, Ex. 1 ¶ 16.) Upon accessing a topic, the original post appeared at the top of the page with all corresponding replies to the original post below. (*Id.*) Typical posts contained text, links to external sites, and/or images. (*Id.*)

Playpen also included features available to all users of the website referred to as “Playpen Image Hosting” and “Playpen Video Hosting.” (*Id.*, Ex. 1 ¶ 23.) Those pages allowed users to upload images and videos of child pornography for other users to view. (*Id.*) Over 1,500 unique users visited Playpen daily and over 11,000 unique users visited the site over the course of a

---

<sup>2</sup> FBI Special Agent Douglas Macfarlane (“Agent Macfarlane”) stated in his warrant application to employ the NIT that “jailbait refers to underage but post-pubescent minors.” (Gov’t’s Opp., Ex. 1 ¶ 14 n.4.) Furthermore, “hardcore” typically depicts “penetrative sexually explicit conduct,” “softcore” depicts “non-penetrative sexually explicit conduct,” and “non-nude” depicts “subjects who are fully or partially clothed.” (*Id.*, Ex. 1 ¶ 14 n.5.)

week. (*Id.*, Ex. 1 ¶ 19.) According to statistics on the website, by March 2015 Playpen contained a total of 117,773 posts, 10,622 total topics and 214,898 total members. (*Id.*, Ex. 2 ¶ 12.)

**A.**

Playpen operated on and was only accessible through Tor. (*Id.*, Ex. 1 ¶ 7.) Unlike a public website, a user could not reach Playpen through a traditional web search engine, such as Google. (*Id.*, Ex. 1 ¶ 10.) Rather, he could only access the website by using Tor and inputting the “particular . . . combination of letters and numbers that” matched Playpen’s specific Tor-based web address. (*Id.*, Ex. 1 ¶¶ 9–10; Hr’g Tr. 38:9–13, ECF No. 29.)

Although the United States Naval Research Laboratory initially designed and implemented Tor for the primary purpose of protecting government communications, it is now “free software, [ ] available worldwide” to the public. (Gov’t’s Opp., Ex. 1 ¶ 7; Hr’g Tr. 7:13–17.) In order to access the Tor network, a user must take affirmative steps to install the software on his computer by either downloading an add-on to his web browser or downloading the Tor software available on its website. (Gov’t’s Opp., Ex. 1 ¶ 7.)

The use of Tor thwarts traditional IP identification and investigative techniques. (*Id.*, Ex. 2 ¶ 23.) Under those traditional methods, FBI agents can review IP address logs after they seize a website to determine which IP addresses visited the site. (*Id.*, Ex. 1 ¶ 22.) They can then conduct a publicly available search to determine which internet service providers (“ISPs”) owned the target IP address and issue a subpoena to the ISP to ascertain the identity of the user. (*Id.*)

The Tor software masks a user’s IP address by “bouncing their communications around a distributed network of relay computers run by volunteers all around the world.” (*Id.*, Ex. 1 ¶ 8.) As a result, “traditional IP identification techniques are not viable” because the last computer or

“exit node” is not the IP address of the actual user who visits the website. (*Id.*; *id.*, Ex. 2 ¶ 23.) It is also impossible to trace the IP address back to the originating computer. (*Id.*, Ex. 2 ¶ 23.) The Tor network “operates similarly to a proxy server—that is, a computer through which communications are routed to obscure a user’s true location.” (*Id.*, Ex. 1 ¶ 8.)

Tor also allows websites, such as Playpen, to operate as a “hidden service.” (*Id.*, Ex. 1 ¶ 9.) Tor masks the website server’s IP address and replaces it with a Tor-based web address. (*Id.*) The Tor-based address is usually a series of algorithm-generated characters such as “asdlk8fs9dfku7f” followed by the suffix “.onion.” (*Id.*) The user may obtain Playpen’s specific address from other users or through a link posted on one of Tor’s “hidden services” pages dedicated to child pornography and pedophilia. (*Id.*, Ex. 1 ¶ 10.)

## **B.**

In December 2014, a foreign law enforcement agency informed the FBI that it suspected a United States-based IP address was associated with Playpen. (*Id.*, Ex. 1 ¶ 28.) The FBI confirmed through a publicly available search that the IP address was owned by Centrilogic, a server hosting company headquartered in Lenoir, North Carolina. (*Id.*) The FBI subsequently obtained a search warrant for the server. (*Id.*) FBI agents examined the server and determined that it contained a copy of Playpen. They then stored the copy of the website on a computer server at a government facility in Newington, Virginia. Newington is located in the Eastern District of Virginia. (*Id.*)

Additional investigation revealed that a resident of Naples, Florida had administrative control of Playpen and the computer server in Lenoir. (*Id.*) On February 19, 2015 FBI personnel executed a court-authorized search of the suspected administrator’s residence in Naples. (*Id.*, Ex. 1 ¶ 30.) The FBI arrested the suspect and assumed administrative control of Playpen. (*Id.*)

On February 20, 2015, Agent Macfarlane applied to a United States Magistrate Judge in the Eastern District of Virginia for a warrant to use the NIT while the FBI assumed administrative control of Playpen on a copy of its server in Newington. (*See generally id.*, Ex. 1.)

Agent Macfarlane stated in the warrant application that the NIT was necessary to overcome the obstacles presented by Tor's masking capabilities. (*Id.*, Ex. 1 ¶ 31.) He stated that "other investigative procedures that are usually employed in criminal investigations of this type have been tried and failed or reasonably appear to be unlikely to succeed if they are tried." (*Id.*) The agent represented that the search would aid the FBI in its investigation by revealing "information that may assist in identifying the user's computer, its location, and the user of the computer." (*Id.*, Ex. 1 ¶ 34.) He explained in the warrant application that the NIT would "augment" the normal content that websites send to its visitors with "additional computer instructions." (*Id.*, Ex. 1 ¶ 33.) Specifically, those instructions "are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government," including the "activating" computer's actual IP address.<sup>3</sup> (*Id.*, Ex. 1 ¶ 33, Attach. B.) The NIT would deploy "each time that any user or administrator log[ged] into Playpen by entering a username and password." (*Id.*, Ex. 1 ¶ 36.) The FBI could then link a username and its corresponding activity on the site with an IP address. (*Id.*, Ex. 1 ¶ 37.)

Agent Macfarlane explained that the "NIT may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." (*Id.*, Ex. 1 ¶ 46 (emphasis

---

<sup>3</sup> Other information gathered from the NIT included: (1) a unique identifier generated by the NIT to distinguish data from that particular computer; (2) the type of operating system running on the computer; (3) information about whether the NIT has already been delivered to the "activating" computer; (4) the "activating" computer's host name; (5) the "activating" computer's active operating system username; and (6) the "activating" computer's media access control ("MAC") address. (Gov't's Opp., Ex. 1 Attach. B.)

added).) In Attachment A to the warrant application, which identified the “place to be searched,” Agent Macfarlane stated that the NIT would be “deployed on the computer server. . . . located at a government facility in the Eastern District of Virginia.” (*Id.*, Ex. 1 Attach. A.) It stated that the NIT would seek information from the “activating computers,” which “are those of any user or administrator who logs into [Playpen] by entering a username and password.” (*Id.*) On February 20, 2015, the magistrate judge issued the search warrant. (*Id.*, Ex. 1.)

### C.

While monitoring activity on Playpen after seizing a copy of the server, FBI agents observed someone with the username “thepervert” posting occasionally on the website’s forums. (*Id.*, Ex. 2 ¶¶ 25–27.) The profile page indicated that “thepervert” created his profile on January 26, 2015 and had been actively logged into the website for 10 hours and 18 minutes between that date and March 1, 2015. (*Id.*, Ex. 2 ¶ 26.) During that time, “thepervert” made approximately six postings on Playpen which included, among other things, hyperlinks to forums on both Playpen and external websites containing child pornography. (*Id.*, Ex. 2 ¶ 27.)

On February 28, 2015, after the NIT had already been deployed, “thepervert” logged into Playpen by entering his username and password. (*Id.*, Ex. 2 ¶ 28.) That triggered certain information on his computer, including his IP address, to be transmitted to the government. (*Id.*) During that browsing session, “thepervert” accessed forums depicting child pornography. (*Id.*, Ex. 2 ¶ 29.)

Using publicly available websites, FBI agents were able to determine that Comcast Cable (“Comcast”) operated the suspect’s IP address. (*Id.*, Ex. 2 ¶ 30.) They served upon Comcast an administrative subpoena/summons requesting information related to the IP address associated

with “thepervert.” (*Id.*, Ex. 2 ¶ 31.) According to the information received from Comcast, the IP address was assigned to Werdene. (*Id.*, Ex. 2 ¶¶ 31–33.)

On June 17, 2015, FBI agents sought and obtained from a Magistrate Judge in the United States District Court for the Eastern District of Pennsylvania a warrant to search Werdene’s home in Bensalem for “evidence, contraband, [and] fruits/instrumentalities” of child pornography. (*Id.*) On that same day, FBI agents searched Werdene’s home and obtained a laptop, a USB drive contained in a safe and one DVD, all containing child pornography. (Gov’t’s Opp. at 8.) Werdene lived alone and was not home at the time of the search. (*Id.*) FBI agents later interviewed him, where he admitted to using and downloading the material on his laptop. (*Id.*) Werdene was indicted on September 17, 2015. (*Id.*)

#### **D.**

On February 11, 2016 Werdene filed a motion to suppress all physical evidence seized from his home and “all fruits therefrom,” including any inculpatory statements he made. (Def.’s Mot. to Suppress at \*1, ECF No. 19.) He argues that the government “knowingly circumvented” Federal Rule of Criminal Procedure 41, which “limits the authority of a magistrate judge to issue a warrant and “serves as a bulwark against the very type of sweeping dragnet searches and unrestrained government surveillance that occurred in this case.” (Def.’s Mem. in Supp. of Mot. to Suppress (“Def.’s Mem.”) at 9, ECF No. 19.) He argues that the violation of Rule 41 is “of constitutional magnitude” and the evidence seized pursuant to the NIT should be suppressed. (*Id.* at 15–16.) He further argues that even if the Court does not find a constitutional violation, suppression is warranted because he was prejudiced by the government’s violation of the Rule. (*Id.* at 16–17.) Werdene also contends that the FBI acted with intentional and deliberate



disregard of Rule 41 because they misled the magistrate judge “with respect to the true location of the activating computers to be searched.” (*Id.* at 17.)

The Government argues that “[t]he fact that Rule 41 does not explicitly authorize some procedure does not mean that those procedures are unlawful.” (Gov’t’s Opp. at 17.) It argues that under these circumstances, Werdene’s use of Tor made it impossible for FBI agents to comply with the requirements of Rule 41 because he “made sure that his location could not be found.” (*Id.* at 18.) The Government further states that even if there was a violation of Rule 41, suppression is not the appropriate remedy because it was not of constitutional magnitude and there is no evidence that the FBI agents engaged in any conduct warranting application of the exclusionary rule. (*Id.* at 20–26.) The Court held a hearing on the motion on April 7, 2016. (ECF No. 27.)

#### E.

A number of federal courts have recently issued opinions in cases arising from the same NIT application and warrant issued in this case. *See United States v. Levin*, 15-cr-10271, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Arterbury*, 15-cr-182 (N.D. Okla. Apr. 25, 2016) (report and recommendation); *United States v. Epich*, 15-cr-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Stamper*, No. 15-cr-109 (S.D. Ohio Feb. 19, 2016); *United States v. Michaud*, 15-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). Similar to Werdene, the defendants in those cases lived outside of the Eastern District of Virginia and sought to suppress the evidence against them because of the Government’s alleged violations of Rule 41.<sup>4</sup>

---

<sup>4</sup> The issue that the court addressed in *Stamper* was not suppression for violation of Rule 41, but instead suppression for violation of the Fourth Amendment.

Although the courts generally agree that the magistrate judge in Virginia lacked authority under Rule 41 to issue the warrant, they do not all agree that suppression is required or even appropriate. *Compare Michaud*, 2016 WL 337263, at \*6–7 (finding violation of Rule 41(b) but suppression unwarranted because defendant was not prejudiced and FBI agents acted in good faith), *and Epich*, 2016 WL 953269, at \*2 (rejecting Defendant’s contention that Rule 41 was violated and finding suppression unwarranted even if it was), *with Levin*, 2016 WL 2596010, at \*7–15 (finding suppression warranted because Rule 41 “implicates substantive judicial authority,” Defendant was prejudiced even if the violation was technical, and the good faith exception to the exclusionary rule is not available because the warrant was void *ab initio*), *and Arterbury*, slip op. at 13–29 (same).

## II.

Rule 41(b) describes five scenarios in which a magistrate judge has authority to issue a warrant. Subsection (b)(1) states the general rule that “a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district.” FED. R. CRIM. P. 41(b)(1). The following four subsections provide that that a magistrate judge has authority to issue a warrant: (2) “if the person or property is located within the district but might move or be moved outside the district before the warrant is executed;” (3) if the magistrate judge sits in a district in which activities related to terrorism have occurred; (4) to install a tracking device within the district, though the magistrate judge may authorize the continued use of the device if the person or object subsequently moves or is moved outside of the district; and (5) where the criminal activities occur in the District of Columbia, any United States territory, or on any land or within any building outside of the country owned by the United States or used by a United States diplomat. FED. R. CRIM. P. 41(b)(2)–(5).

Werdene argues that the NIT warrant “is not authorized under any of these sections, and, therefore, plainly unlawful.” (Def.’s Mem. at 11.) He contends that in this case the “actual ‘place to be searched’ was not the server, but the ‘activating computers’ that would be forced to send data to that server.” (*Id.* at 13.) Accordingly, he contends that since his computer was located in Bensalem, outside the magistrate judge’s jurisdiction in the Eastern District of Virginia, the magistrate judge did not have authority to issue the warrant under any of Rule 41(b)’s five subsections.

During the hearing, Werdene’s counsel introduced as the lone defense exhibit a December 22, 2014 letter from United States Deputy Assistant Attorney General David Bitkower to Judge Reena Raggi, Chair of the Advisory Committee on Criminal Rules, regarding “Response to Comments Concerning Proposed Amendment to Rule 41.”<sup>5</sup> (Def.’s Ex. 1.) The letter addresses various issues related to proposed amendments to Rule 41, including concerns regarding the Fourth Amendment’s particularity and notice requirements, Title III wiretap orders, “remote search techniques” and, relevant to this case, new standards for obtaining a warrant “in cases involving Internet anonymizing technology.” (Def.’s Ex. at 1–2.)

In a section titled “Concealed through technological means,” the letter states that “[u]nder the proposed amendment, a magistrate judge in a district where activities related to a crime may have occurred will have authority to issue a warrant for a remote search if the location of the computer to be searched ‘has been concealed through technological means.’” (*Id.* at 10.) Counsel for Werdene contends the letter is evidence of a Rule 41 violation in her client’s case because “the law has not caught up with technology” and the evidence should be suppressed because “a violation is . . . a violation.” (Hr’g Tr. 17:15, 18:8–9.) The Court need not address whether or not law enforcement has to cease its investigative efforts while the process to amend

---

<sup>5</sup> Judge Raggi sits on the United States Court of Appeals for the Second Circuit.

the Federal Rules of Criminal Procedure plays out. As explained *infra*, a violation of Rule 41 does not end the inquiry. The facts of this case compel the conclusion that suppression is unwarranted.

The Government does not contend that the NIT warrant falls within any specific subsection of Rule 41. (Gov't's Opp. at 15–20.) It instead argues that Rule 41 is flexible, and the failure of Rule 41 to “authorize some procedure does not mean that those procedures are unlawful.” (*Id.* at 17.) The Government highlights the predicament with which the FBI agents were faced: the Defendant's use of Tor made it impossible for agents to know in which district it should seek a warrant, and they accordingly “sought [the] warrant in the only logical district—the one in which they had the server on which they would install the NIT.” (*Id.* at 16.)

“Rule 41(b) is to be applied flexibly, not rigidly.” *Michaud*, 2016 WL 337263, at \*5 (citing *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992)). Even a flexible application of the Rule, however, is insufficient to allow the Court to read into it powers possessed by the magistrate that are clearly not contemplated and do not fit into any of the five subsections. *See id.* at \*6 (“In this case, even applying flexibility to Rule 41(b), the Court concludes that the NIT Warrant technically violates the letter, but not the spirit, of Rule 41(b).”).

Subsection (b)(1) states that a magistrate judge may issue a warrant “to search for and seize a person or property located within the district.” The Government does not attempt to argue here, as it has done in similar cases in other districts, that the NIT targeted property in the Eastern District of Virginia because the Defendant initiated contact with the server in that location when accessing the website. *See Levin*, 2016 WL 2596010, at \*5 (“[S]ince Levin . . . ‘retrieved the NIT from a server in the Eastern District of Virginia, and the NIT sent [Levin’s] network information back to the server in that district,’ the government argues that the search . . .

can be understood as occurring within the Eastern District of Virginia.”); *Michaud*, 2016 WL 337263, at \*6 (“[A] cogent, but ultimately unpersuasive argument can be made that the crimes were committed ‘within’ the location of Website A, [the] Eastern District of Virginia, rather than on [a] personal computer located in other places under circumstances where users may have deliberately concealed their locations.”). Rather, the Government argues for a flexible application of the Rule because “as is often the case, Congress has not caught up with the changes in technology.” (Hr’g Tr. at 51:1–2.)

That Congress has “not caught up” with technological advances does not change the fact that the target of the NIT in Werdene’s case was located outside of the magistrate judge’s district and beyond her jurisdiction under subsection (b)(1). The property to be seized pursuant to the NIT warrant was not the server located in Newington, Virginia, but the IP address and related material “[f]rom any ‘activating’ computer” that accessed Playpen. (Gov’t’s Opp., Ex. 1 Attach. A.) Since that material was located outside of the Eastern District of Virginia, the magistrate judge did not have authority to issue the warrant under Rule 41(b)(1).

Subsections (b)(2)–(5) are also inapplicable to the NIT warrant: (b)(2) relates to a person or object located within the district at the time the warrant is issued but that the government has reason to believe might move or be moved outside the district; (b)(3) relates to terrorist activity; (b)(4) permits tracking devices to be installed on a person or property within the district; and (b)(5) allows the magistrate judge to issue a warrant when the activity occurs in certain territories outside of the district, none of which are applicable here. Subsections (b)(2) and (b)(4), the only provisions potentially applicable to this case, are both premised on the person or property being located within the district. It is uncontested that the computer information that the NIT targeted

was at all relevant times located beyond the boundaries of the Eastern District of Virginia. The magistrate judge was accordingly without authority to issue the NIT warrant under Rule 41.

### III.

“There are two categories of Rule 41 violations: those involving constitutional violations, and all others.” *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000) (citations omitted) (cited with approval in *United States v. Slaey*, 433 F. Supp. 2d 494, 498 (E.D. Pa. 2006) and *United States v. Sampson*, No. 07-cr-389, 2008 WL 919528, at \*4 (M.D. Pa. Mar. 31, 2008)). Courts have described violations of Rule 41 as either: (1) “substantive” or “constitutional” violations; or (2) “ministerial” or “procedural” violations. *See United States v. Levin*, No. 15-cr-10271, 2016 WL 2596010, at \*7 (D. Mass. May 5, 2016) (distinguishing between “substantive” and “procedural” violations of Rule 41); *see also United States v. Krueger*, 809 F.3d 1109, 1114 (10th Cir. 2015) (finding that the inquiry begins by determining whether the Rule 41 violation was of “constitutional import”); *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) (distinguishing between “substantive” and “procedural” violations of Rule 41); *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000) (distinguishing “constitutional” and “ministerial” violations of Rule 41).

#### A.

To demonstrate that the violation of Rule 41 was of constitutional magnitude, Werdene must show a violation of his Fourth Amendment rights. *See United States v. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988), *overruled on other grounds by United States v. Chapple*, 985 F.2d 729 (3d Cir. 1993). Specifically, he must articulate how the Government’s failure to comply with Rule 41(b) caused a search or seizure prohibited by the Fourth Amendment. He cannot do so.

Werdene does not argue that the Government violated his Fourth Amendment rights by seeking a warrant without probable cause. (Hr'g Tr. 23:16–22.) Rather, as the Government asserts, his argument is that Agent Macfarlane applied for the NIT warrant in the wrong district. (Gov't's Opp. at 15.) Werdene contends rather circularly that the Government's "violation of Rule 41 is of constitutional magnitude because it did not involve mere ministerial violations of the rule." (Def.'s Mot. at 16 (citation omitted).) He argues that the Fourth Amendment protects his use of his computer inside the privacy of his own home and "[a]llowing the Government to ignore the limits imposed by the Rule will invite further violations and undermine the core constitutional requirement that warrants particularly describe the place or places to be searched." (*Id.* (citations omitted).)

The Supreme Court of the United States has "uniformly . . . held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by the government action." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (collecting cases). That inquiry is analyzed in two parts: (1) whether the individual, through his conduct, "exhibited an actual (subjective) expectation of privacy;" and (2) whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" *Id.* (citations omitted).

In *Smith*, the Supreme Court addressed whether petitioner Michael Lee Smith had a reasonable expectation of privacy in the telephone numbers he dialed. 442 U.S. at 738. The government had used a pen register to record the numbers dialed from Smith's home in order to determine if he made threatening phone calls to another individual. *Id.* at 737. The Court rejected Smith's argument that he had a "reasonable expectation of privacy" in the numbers that

he dialed and held that the use of the pen register was, in fact, not a search. *Id.* at 742. It reasoned that “[a]ll telephone users realize that they must ‘convey’ phone numbers to the telephone companies, since it is through telephone company switching equipment that their calls are completed.” *Id.* It rejected Smith’s argument that he attempted to keep the numbers he dialed private by dialing them from his home phone because such numbers were “convey[ed] . . . to the telephone company in precisely the same way” regardless of his location. *Id.* at 743. Further, it held that Smith’s expectation of privacy was “not one that society is prepared to recognize as reasonable” because he voluntarily turned the information over to a third party, the telephone company. *Id.* at 743–44 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)) (internal quotation marks omitted).

The Third Circuit has similarly held that an individual has “no reasonable expectation of privacy in his IP address and so cannot establish a Fourth Amendment violation.” *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (citations omitted). “[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including [internet service providers].” *Id.*; see also *In re Nickelodeon Consumer Privacy Litig.*, No. 12-cv-07829, 2014 WL 3012873, at \*15 (D.N.J. July 2, 2014) (“Indeed, in the analogous Fourth Amendment context, email and IP addresses can be collected without a warrant because they constitute addressing information and do not necessarily reveal any more about the underlying contents of communications than do phone numbers, which can be warrantlessly captured via pen registers.”) (citation and internal quotation marks omitted); *United States v. Forrester*, 512 F.3d 500, 509–10 (9th Cir. 2008) (comparing IP addresses to the outside of a letter and the monitoring of IP addresses to a pen register). The Third Circuit in *Christie* 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." 624 F.3d. at 574 (citations and internal quotation marks omitted).

Werdene had no reasonable expectation of privacy in his IP address. Aside 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: "in order for a prospective user 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." *United States v. Farrell*, No. 15-cr-029, 2016 WL 705197, at \*2 (W.D. Wash. Feb. 23, 2016). The court in *Farrell* held that "[u]nder these circumstances Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network." *Id.*; *see also Michaud*, 2016 WL 337263, at \*7 ("Although the IP addresses of users utilizing the Tor network may not be known to websites, like [Playpen], using the Tor network does not strip users of all anonymity, because users . . . must still send and receive information, including IP addresses, through another computer . . .").<sup>6</sup>

That Werdene's IP address was subsequently bounced from node to node within the Tor network to mask his identity does not alter the analysis of whether he had an actual expectation of privacy in that IP address. In *Smith*, the petitioner argued that the numbers he dialed on his telephone remained private because they were processed through automatic switching equipment rather than a live operator. 442 U.S. at 745. The Court rejected that argument, finding that the

---

<sup>6</sup> In support of his argument, Werdene relies on *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). That case involved FBI agents seeking a warrant to install software on a computer whose location was not ascertainable. *Id.* at 755. The software could generate user records and take control of a computer's camera to generate photographs of the user. *Id.* The magistrate judge declined to issue the warrant because the jurisdictional requirements of Rule 41(b) were not met and because it violated the Fourth Amendment's particularity requirement and protections against intrusive video surveillance. *Id.* at 757-61. *In re Warrant* is distinguishable based on the intrusive and general nature of the information sought. Unlike the software in that case, the NIT targeted users who were accessing child pornography and revealed information in which they had no reasonable expectation of privacy.

telephone company's decision to use automatic equipment instead of a live operator did not "make any constitutional difference" in analyzing the petitioner's reasonable expectations of privacy. *Id.* Similarly, the type of third-party to which Werdene disclosed his IP address—whether a person or an "entry node" on the Tor network—does not affect the Court's evaluation of his reasonable expectation of privacy. He was aware that his IP address had been conveyed to a third party and he accordingly lost any subjective expectation of privacy in that information. *See Farrell*, 2016 WL 705197, at \*2 ("[T]he Tor Project [communicates to users] that the Tor network has vulnerabilities and that users might not remain anonymous.").<sup>7</sup>

## B.

Even if Werdene maintained a subjective expectation that his IP address would remain private through his use of Tor, that expectation is not "one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361. In *United States v. Stanley*, 753 F.3d 114 (3d Cir. 2014), Richard Stanley accessed his neighbor's wireless internet connection without permission to share child pornography. Police officers learned Stanley's IP address by analyzing the neighbor's router and located him by using a device known as a "MoocherHunter." *Id.* at 116. MoocherHunter is a mobile tracking software that is used with a directional antenna to locate a "mooching computer" by detecting the strength of the radio waves it is emitting. *Id.*

Stanley contended that the officers' use of MoocherHunter constituted a warrantless search and sought suppression of the evidence against him. *Id.* at 117. After the district court denied his motion, the Third Circuit affirmed, holding that the officers did not conduct a

---

<sup>7</sup> Werdene does not argue that he had a reasonable expectation of privacy in the other material gathered by the NIT, including the type of operating system running on the computer, his computer's active operating system username and his computer's MAC address. Nor does Werdene contend that any of that information was material to the investigation of his activities and his subsequent identification.

“search” within the meaning of the Fourth Amendment because Stanley did not have a reasonable expectation of privacy in his wireless internet signal. *Id.* at 119–22.

The Third Circuit reasoned that “while Stanley may have justifiably expected the path of his invisible radio waves to go undetected, society would not consider this expectation ‘legitimate’ given the unauthorized nature of his transmission.” *Id.* at 120 (citing *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (“[A] burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as ‘legitimate.’”)); *see also United States v. Jacobson*, 466 U.S. 109, 122 (1984) (“The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities.”). Werdene’s use of Tor to view and share child pornography is not only an activity that society rejects, but one that it seeks to sanction. *See, e.g.*, Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008, 42 U.S.C. §§ 17611, 17612 (authorizing the Attorney General to create a National Strategy for Child Exploitation Prevention and Interdiction and establishing a National Internet Crimes Against Children Task Force Program); *Stanley*, 753 F.3d at 121 (concluding that society would be unwilling to recognize Stanley’s privacy interests as “reasonable” where “the purpose of [his] unauthorized connection was to share child pornography”).

The Third Circuit further stated in *Stanley* that recognizing his expectation of privacy as “legitimate” would “reward him for establishing his Internet connection in such an unauthorized manner.” 753 F.3d at 121. Here, Werdene seeks to “serendipitously receive Fourth Amendment protection” because he used Tor in an effort to evade detection, even though an individual who

does not conceal his IP address does not receive those same constitutional safeguards. *Id.* (citing *United States v. Broadhurst*, No. 11-cr-00121, 2012 WL 5985615, at \*5 (D. Or. Nov. 28, 2012)). Since Werdene 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 and the violation at issue is therefore not constitutional. *See Martinez-Zayaz*, 857 F.2d at 136.

#### IV.

Werdene is left to contend that suppression is warranted even if the Government’s violation of Rule 41 was nonconstitutional, procedural or “ministerial.” (Def.’s Mem. at 16–17.) He relies on the Tenth Circuit Court of Appeals’s suppression standard in the context of a nonconstitutional Rule 41 violation. Specifically, in *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), the Tenth Circuit stated that it:

consider[s] whether the defendant can establish that, as a result of the Rule violation (1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision of the Rule.

*Id.* at 1114.<sup>8</sup> Werdene claims he was prejudiced because the NIT “would not have occurred[] but for the Rule 41 violation.” (Def.’s Mem. at 17.) He also contends that the Government “acted with intentional and deliberate disregard of Rule 41” as the Rule “simply does not permit remote, dragnet searches of computers outside of the authorizing district.” (*Id.*)

---

<sup>8</sup> In *Krueger*, the Tenth Circuit adopted the Ninth Circuit’s suppression standard for nonconstitutional violations of Rule 41 first articulated in *United States v. Stefanson*, 648 F.2d 1231, 1235 (9th Cir. 1981). Several other circuits also use the *Stefanson* test. *See, e.g., United States v. Comstock*, 805 F.2d 1194, 1207 (5th Cir. 1986); *United States v. Loyd*, 721 F.2d 331, 333 (11th Cir. 1983); *United States v. Gitcho*, 601 F.2d 369, 372 (8th Cir. 1979), *cert. denied*, 444 U.S. 871 (1979); *United States v. Mendel*, 578 F.2d 668, 673–74 (7th Cir. 1978), *cert. denied*, 439 U.S. 964 (1978).

The Third Circuit defines prejudice differently than the Tenth Circuit.<sup>9</sup> In the Third Circuit, a nonconstitutional violation of Rule 41 warrants suppression when it “caused prejudice or was done with intentional and deliberate disregard of the rule’s requirements.” *United States v. Cox*, 553 F. App’x 123, 128 (3d Cir. 2014); *see also United States v. Slaey*, 433 F. Supp. 2d 494, 498 (E.D. Pa. 2006). Our Circuit defines prejudice “in the sense that it offends concepts of fundamental fairness or due process.” *Hall*, 505 F.2d at 964; *see also United States v. Searp*, 586 F.2d 1117, 1125 (6th Cir. 1978) (“The Third Circuit has adopted a similar, but more restrictive ‘prejudice’ test, requiring suppression ‘only when the defendant demonstrates prejudice from the Rule 41 violation . . . in the sense that it offends concepts of fundamental fairness or due process.’”) (quoting *Hall*, 505 F.2d at 961); *United States v. Burka*, 700 F. Supp. 825, 830 (E.D. Pa. 1988) (articulating *Hall*’s prejudice standard). The Government’s actions in this case do not offend notions of fundamental fairness or due process.

After assuming control of Playpen and moving its server to a government facility in Newington, Virginia, Agent Macfarlane sought and obtained a warrant to employ the NIT in the Eastern District of Virginia. (Gov’t’s Opp., Ex. 1 ¶¶ 28, 30.) Before activating the NIT, Agent Macfarlane did not—and could not—know that Werdene resided in the Eastern District of Pennsylvania. Indeed, the only way in which the Government could have procedurally complied with Rule 41 was either through sheer luck (*i.e.*, Werdene’s location happened to be within the Eastern District of Virginia) or by applying for a warrant in every one of the ninety-four federal judicial districts. Agent Macfarlane’s warrant application, which was approved by a neutral and

---

<sup>9</sup> The Government also argues that *Krueger*’s facts are distinguishable from this case. (Gov’t’s Opp. at 17.) In *Krueger*, Homeland Security Investigations (“HIS”) agents sought and obtained a warrant from a magistrate judge in the District of Kansas to search properties in Oklahoma. *See United States v. Krueger*, 809 F.3d 1109, 1111 (10th Cir. 2015). There, it was clear in which district the HIS agents should have made their warrant request. Here, however, Werdene’s use of Tor to mask his IP address obscured his location from FBI agents. Unlike *Krueger*, the FBI agents could not know Werdene’s location prior to requesting the warrant.

detached magistrate judge, described the NIT process in copious detail. (*See generally* Gov't's Opp., Ex. 1.) The warrant application states that the NIT would deploy "each time that any user or administrator log[ged] into Playpen by entering a username and password." (*Id.*, Ex. 1 ¶ 36.) This enabled the FBI to link a username and its corresponding activity to an IP address. (*Id.*, Ex. 1 ¶ 37.) Agent Macfarlane specifically noted that the NIT could enable this process on users of Playpen "wherever located." (*Id.*, Ex. 1 ¶ 46.) The Government's nonconstitutional violation of Rule 41 does not offend concepts of fundamental fairness or due process and Werdene's motion to suppress cannot be granted on prejudice grounds. *See United States v. McMillion*, No. 08-cr-0205, 2011 WL 9110, at \*4 (M.D. Pa. Jan. 3, 2011), *aff'd*, 472 F. App'x 138 (3d Cir. 2012).

#### **B.**

Werdene also contends that the Government acted with intentional and deliberate disregard of Rule 41 because the FBI misled the magistrate judge "with respect to the true location of the activating computers to be searched." (Def.'s Mem. at 17.) Werdene claims that this was "egregious[] because it is a deliberate flaunting of the Rule[.]" (Hr'g Tr. 33:2-3.) A review of the record, and specifically Agent Macfarlane's warrant application, shows no deception on the Government's part. The warrant request was candid about the challenge that the Tor network poses, specifically its ability to mask a user's physical location. (Gov't's Opp., Ex. 1 ¶¶ 28, 30.) Agent Macfarlane stated that the NIT would be deployed "each time" that "any user" logged into Playpen "wherever" they were "located." (*Id.*, Ex. 1 ¶ 46.) As discussed *infra*,

Section V.D., the Government did not mislead the magistrate judge but was instead up front about the NIT's method and scope.<sup>10</sup>

## V.

Even if Werdene had a reasonable expectation of privacy in the information obtained by the NIT—rendering the Rule 41(b) violation constitutional in nature—suppression is not the appropriate remedy.

### A.

When the Government seeks to admit evidence collected pursuant to an illegal search or seizure, the exclusionary rule operates to suppress that evidence and makes it unavailable at trial. *See United States v. Katzin*, 769 F.3d 163, 169 (3d Cir. 2014) (en banc), *cert. denied*, 135 S. Ct. 1448 (2015) (citing *Herring v. United States*, 555 U.S. 135, 139 (2009)). The exclusionary rule was developed “[t]o deter Fourth Amendment violations.” *Id.*

Whether suppression is appropriate under the exclusionary rule is a separate question from whether a defendant's Fourth Amendment rights were violated. *See Hudson v. Michigan*, 547 U.S. 586, 591–92 (2006); *accord Herring*, 555 U.S. at 140. Exclusion is not a personal right conferred by the Constitution and was not “designed to ‘redress the injury’ occasioned by an unconstitutional search.” *Davis v. United States*, 564 U.S. 229, 236 (2011) (quoting *Stone v. Powell*, 428 U.S. 465, 486 (1976)). Rather, the exclusionary rule is “a judicially created means of effectuating the rights secured by the Fourth Amendment.” *Stone*, 428 U.S. at 482. The fact that a Fourth Amendment violation occurs does not mean that the evidence is automatically

---

<sup>10</sup> Werdene also argues that the Government violated Rule 41's notice requirement. (Def.'s Mem. at 18–20.) A careful reading of Agent Macfarlane's warrant application, however, shows that he requested the delay of any notice for up to 30 days under Rule 41(f)(3) and 18 U.S.C. § 3103(a)(b)(1) and (3) to avoid any tampering with Playpen while the investigation was ongoing. (Gov't's Opp., Ex. 1 ¶¶ 38–41.) He also noted that due to the anonymity of Playpen's users, “the investigation has not yet identified an appropriate person to whom such notice can be given.” (*Id.*, Ex. 1 ¶ 40.) Regardless, even if the notice requirement was violated, suppression is not an appropriate remedy because he was not prejudiced by the violation. *See supra* Section IV.A.

suppressed. *See Katzin*, 769 F.3d at 170 (citing *Herring*, 555 U.S. at 140). Indeed, “exclusion ‘has always been our last resort, not our first impulse.’” *Herring*, 555 U.S. at 140 (quoting *Hudson*, 547 U.S. at 591).

Application of the rule is instead “limited to those ‘unusual cases’ in which it may achieve its objective: to appreciably deter governmental violations of the Fourth Amendment.” *Katzin*, 769 F.3d at 170 (quoting *Leon*, 468 U.S. at 909). “Real deterrent value” alone, however, is insufficient for the exclusionary rule to apply. *Id.* at 171 (quoting *Davis*, 564 U.S. at 237). The deterrent value must also outweigh the “substantial social costs” of exclusion. *Leon*, 468 U.S. at 907. Such costs “often include omitting ‘reliable, trustworthy evidence’ of a defendant’s guilt, thereby ‘suppress[ing] the truth and set[ting] [a] criminal loose in the community without punishment.’” *Katzin*, 769 F.3d at 171 (quoting *Davis*, 564 U.S. at 237). Because this result runs contrary to the truth-finding functions of judge and jury, “exclusion is a bitter pill, swallowed only as a last resort.” *Id.* (citations and internal quotation marks omitted). Accordingly, exclusion is warranted “where the deterrent value of suppression . . . overcome[s] the resulting social costs.” *Id.* (citing *Davis*, 564 U.S. at 237).

The good faith exception to the exclusionary rule “was developed to effectuate this balance and has been applied ‘across a range of cases.’” *Id.* (quoting *Davis*, 564 U.S. at 238). *Leon* and its progeny highlight that “the deterrence benefits of exclusion ‘var[y] with the culpability of the law enforcement conduct’ at issue.” *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 143). The deterrent value of suppression tends to outweigh the costs “[w]here officers exhibit ‘deliberate,’ ‘reckless,’ or ‘grossly negligent’ disregard for Fourth Amendment rights.” *Id.* (quoting *Herring*, 555 U.S. at 144). When the police act with an “objectively reasonable good-faith belief” in the legality of their conduct, or when their conduct “involves



only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way.” *Id.* (citations and internal quotation marks omitted). Accordingly, discerning “whether the good faith exception applies requires courts to answer the ‘objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances.’” *Katzin*, 769 F.3d at 171 (quoting *Herring*, 555 U.S. at 145).

**B.**

Werdene relies on *United States v. Levin*, No. 15-cr-10271, 2016 WL 2596010 (D. Mass. May 5, 2016). In that case, the United States District Court for the District of Massachusetts addressed whether the NIT was a substantive or procedural violation of Rule 41 and whether the information obtained from the NIT should be suppressed. The court held, in relevant part, that: (1) the NIT warrant constituted a “substantive” or constitutional violation of Rule 41(b) in that it infringed on the defendant’s Fourth Amendment rights; and (2) that the good faith exception was not available in this context, *i.e.*, where a magistrate judge issued a warrant without proper jurisdiction. *Id.*

In finding that the NIT warrant was a substantive violation of Rule 41(b), the *Levin* court reasoned that “the violation here involved ‘substantive judicial authority’ rather than simply ‘the procedures for obtaining and issuing warrants.’” *Id.* at \*8 (quoting *Krueger*, 809 F.3d at 1115). The court “assume[d] that [the defendant] had a reasonable expectation of privacy as to the information obtained through the execution of the various warrants.” *Id.* at \*1 n.1. The court in *Levin* held that because Rule 41(b) “did not grant [the magistrate] authority to issue the NIT warrant . . . [she] was without jurisdiction to do so.” *Id.* at \*8.

The court went further, concluding that this jurisdictional flaw rendered the warrant “void *ab initio*.” *Id.* (citing, *inter alia*, *United States v. Master*, 614 F.3d 236, 241 (6th Cir. 2010)). It then stated that a warrant “void *ab initio*” was equivalent to “no warrant at all.” *Id.* at \*12. The court likened this situation to a “warrantless search” scenario which is “presumptively unreasonable” under the Fourth Amendment, and accordingly found a “substantive” or constitutional violation of Rule 41(b). *Id.* at \*12 (citing *United States v. Curzi*, 867 F.2d 36 (1st Cir. 1989)).

The court also held that the good faith exception was not available in cases where a warrant was void *ab initio* and, therefore granted the motion to suppress. *Id.* at \*10–13. In doing so, it relied on the Sixth Circuit Court of Appeals’s decision in *United States v. Scott*, 260 F.3d 512 (6th Cir. 2001). The *Levin* court stated that while “the Supreme Court has expanded the good-faith exception to contexts beyond those *Leon* specifically addressed,” none of those cases “involved a warrant that was void *ab initio*, and therefore none direct the conclusion that the good-faith exception ought apply to this case.” *Levin*, 2016 WL 2596010, at \*11.

### C.

*Levin*’s reliance on *Scott* was misplaced, particularly given the court’s acknowledgement that “the Sixth Circuit effectively reversed [*Scott*]” in *United States v. Master*, 614 F.3d 236 (6th Cir. 2010).<sup>11</sup> *Id.* at \*11; *see also United States v. Beals*, 698 F.3d 248, 265 (6th Cir. 2012) (recognizing that *Master* overruled *Scott*). In *Master*, the Sixth Circuit reexamined its holding in

<sup>11</sup> *Levin* later noted that “[e]ven in *Master* . . . the court acknowledged that the recent Supreme Court cases addressing the good-faith exception ‘do [ ] not directly overrule our previous decision in *Scott*.’” *Levin*, 2016 WL 2596010, at \*12 (citing *Master*, 614 F.3d at 243). It is therefore unclear whether or not *Levin* believed *Scott* was overruled. In any event, *Master* provided that “nothing in this opinion should cast doubt on the ultimate outcome in *Scott*. In that case, the officers made at best minimal attempts to find available, active magistrates before presenting the warrant to the retired judge.” *Master*, 614 F.3d at 242 n.3. Thus, *Master* simply noted that the officers’ actions in *Scott*, analyzed under the newly adopted good faith framework, fell below the standard necessary to apply the good faith exception to the exclusionary rule. To the extent *Levin* seeks to rely on *Master*’s footnote for the proposition that the good faith exception is inapplicable in this context, such a finding was clearly rejected by *Master*.

*Scott*—that the good faith exception could never apply where a warrant was void *ab initio*—in light of the Supreme Court’s decisions in *Herring* and *Hudson*. 614 F.3d at 242–43. *Master* found *Herring*’s separation of the suppression and Fourth Amendment violation inquiries to be “contrary to a foundational assumption of the opinion in *Scott* that: ‘Subject to a few exceptions, the exclusionary rule requires the suppression of evidence obtained in violation of the Fourth Amendment.’” *Id.* at 242 (quoting *Scott*, 260 F.3d at 514). The court stated:

Whereas *Scott* effectively required the government to qualify for an exception to the general rule of suppression, the Supreme Court has since emphasized that the decision to exclude evidence is divorced from whether a Fourth Amendment violation occurred. The exclusionary rule’s purpose is instead to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.

*Id.* (citations and internal quotation marks omitted). The Sixth Circuit accordingly found that the good faith exception *could* apply in situations where the warrant was void *ab initio*. *See id.* at 242–43.

Rather than rely on *Master*, the court in *Levin* instead deferred to *Scott*, stating that “[t]he *Master* court read the Supreme Court’s recent good-faith cases too broadly.” *Levin*, 2016 WL 2596010, at \*12. The court explained its reasoning in a footnote, stating that while *Herring* “makes much of the connection between the exclusionary rule and the goal of deterrence and culpability of law enforcement . . . it says nothing about whether the same calculus ought apply where there was never jurisdiction to issue a valid warrant in the first place.” *Id.* at \*12 n.22. *Levin* apparently discounted *Master*’s reliance on *Herring* because *Herring* did not hold that the good faith exception applies where a warrant was void *ab initio*, *i.e.*, it never dealt with an issue that *Levin* admits was one of “first impression in this Circuit, and an unresolved question more broadly.” *Id.* at \*10. *But see United States v. Knights*, 534 U.S. 112, 117 (2001) (criticizing as “dubious logic” the argument “that an opinion upholding the constitutionality of a particular

search implicitly holds unconstitutional any search that is not like it”); *Arizona v. Evans*, 514 U.S. 1, 13 (1995) (“Subsequent case law has rejected [a] reflexive application of the exclusionary rule.”) (citation omitted).

The Third Circuit has emphasized that courts “must be prepared to apply th[e] good-faith exception across a range of cases.” *Katzin*, 769 F.3d at 178 (quoting *Davis*, 564 U.S. at 238) (internal quotation marks omitted). Indeed, the court in *Katzin* found that the good faith exception applied in the context of a warrantless search where the officers “acted . . . upon an objectively reasonable good faith belief in the legality of their conduct.” *Id.* at 182. Moreover, it explicitly rejected the appellees’ argument that it would be “fabricat[ing] a new good faith ground,” stating that while “[t]he factual circumstances before us differ, [] we ground our application of the good faith exception in the same time-tested considerations.” *Id.* at 178 n.11. In other words, the legal status of the warrant under the Fourth Amendment does not inform the decision of whether the good faith exception is available in a given case; that inquiry is separate and must be considered in light of the exclusionary rule’s purpose and the officers’ conduct at issue. *See Master*, 614 F.3d at 243.

Additionally, as *Master* indicates, “the exclusionary rule was crafted to curb police rather than judicial misconduct.” *Id.* at 242 (citation omitted). Arguably, the magistrate judge’s lack of authority to issue the warrant has no impact on police misconduct. *See id.* Applying the rule here without exception makes little sense where it was the magistrate, not the agents, who determined that she had jurisdiction. *See, e.g., Emp’rs Ins. of Wausau v. Crown Cork & Seal Co.*, 905 F.2d 42, 45 (3d Cir. 1990) (“A federal court is bound to consider its own jurisdiction preliminary to consideration of the merits.”) (quoting *Trent Realty Assocs. v. First Fed. Sav. & Loan Ass’n of Phila.*, 657 F.2d 29, 36 (3d Cir. 1981)); *In re Warrant to Search a Target*

*Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (declining to issue a warrant under Rule 41(b) because, *inter alia*, the court lacked jurisdiction). The good faith exception is not foreclosed in the context of a warrant that is void *ab initio* and the Court must now determine if it applies.

**D.**

The question is whether “the agents acted with a good faith belief in the lawfulness of their conduct that was ‘objectively reasonable.’” *Katzin*, 769 F.3d at 182 (quoting *Davis*, 564 U.S. at 238). The Court must consider all of the circumstances and confine its inquiry to the “objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of that constellation of circumstances.” *Katzin*, 769 F.3d at 182 (quoting *Leon*, 468 U.S. at 922 n.23) (internal quotation marks omitted).

The agents in this case acted upon an objectively reasonable good faith belief in the legality of their conduct. Attachment A to the warrant application is titled “Place to be Searched” and specifically authorizes deployment of the NIT to “activating computers.” (Gov’t Opp., Ex. 1 Attach A.) “Activating computers” are defined as “those of any user or administrator who logs into [Playpen] by entering a username and password.” (*Id.*) Attachment A notes that the Eastern District of Virginia is where the NIT will be deployed. (*Id.*) Thus, an “objectively reasonable” reading of the warrant gave the agents “authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia.” *United States v. Michaud*, No. 15-cr-05351, 2016 WL 337263, at \*4 (W.D. Wash. Jan. 28, 2016).

Werdene claims that the Government acted with intentional and deliberate disregard of Rule 41 because the FBI misled the magistrate judge “with respect to the true location of the activating computers to be searched.” (Def.’s Mem. at 17.) This argument is belied by both the warrant and warrant application. Agent Macfarlane stated in the warrant application that the “NIT may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, *its location*, other information about the computer and the user of the computer.” (Gov’t Opp., Ex. 1 ¶ 46 (emphasis added).) With this information, the magistrate judge believed that she had jurisdiction to issue the NIT warrant. Contrary to Werdene’s assertion, this is not a case where the agents “hid the ball” from the magistrate or misrepresented how the search would be conducted. *See, e.g., Illinois v. Gates*, 462 U.S. 213, 264 (1983) (“Similarly, the good-faith exception would not apply if the material presented to the magistrate or judge is false or misleading.”) (citing *Franks v. Delaware*, 438 U.S. 154 (1978)).

While the *Levin* court found the good faith exception foreclosed in this scenario, it alternatively held that if the exception did apply, suppression was nonetheless appropriate. *See Levin*, 2016 WL 2596010, at \*13. The court reasoned that “it was not objectively reasonable for law enforcement—particularly a veteran FBI agent with 19 years of federal law enforcement experience—to believe that the NIT Warrant was properly issued considering the plain mandate of Rule 41(b).” *Id.* (citations and internal quotation marks omitted). Noting that “the conduct at issue here can be described as systemic error or reckless disregard of constitutional requirements,” the court found suppression appropriate. *Id.* (citations and internal quotation marks omitted).

The court in *Levin* did not analyze the “costs” associated with suppression. The Supreme Court has stated that these costs are “substantial,” *Leon*, 468 U.S. at 907, given that suppression “often excludes ‘reliable, trustworthy evidence’ of a defendant’s guilt, ‘suppress[es] the truth and set[s] [a] criminal loose in the community without punishment.’” *Katzin*, 769 F.3d at 186 (quoting *Davis*, 564 U.S. at 237). The court in *Levin* also did not address what deterrent effect, if any, suppression would have in this case. While the court found that the agents’ conduct constituted “systemic error or [a] reckless disregard of constitutional requirements,” it failed to address why that is the case. *Levin*, 2010 WL 2596010, at \*13. *Levin* seemed to overlook the Supreme Court’s directive that “the exclusionary rule is not an individual right and applies only where it result[s] in appreciable deterrence.” *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 909).

Further, to the extent a mistake was made in this case, it was not made by the agents in “reckless . . . disregard for Fourth Amendment rights.” *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 144). Rather, it was made by the magistrate when she mistakenly issued a warrant outside her jurisdiction. The agents consulted with federal attorneys before preparing the warrant application. (Gov’t’s Opp. at 24.) *See e.g.*, *Katzin*, 769 F.3d at 181 (stating that “[w]e have previously considered reliance on government attorneys in our good faith calculus and concluded that, based upon it in combination with other factors, ‘[a] reasonable officer would . . . have confidence in [a search’s] validity’”) (quoting *United States v. Tracey*, 597 F.3d 140, 153 (3d Cir. 2010)). They presented the magistrate judge with all relevant information to allow her to make a decision as to whether Rule 41(b) permitted her to issue the warrant. The FBI agents did not misrepresent how the search would be conducted or, most importantly, where it would be conducted.

A magistrate judge's mistaken belief that she had jurisdiction, absent any indicia of reckless conduct by the agents, does not warrant suppression. The Supreme Court has stated:

To the extent . . . proponents of exclusion rely on its behavioral effects on judges and magistrates in these areas, their reliance is misplaced . . . . [T]here exists no evidence suggesting that judges and magistrates are inclined to ignore or subvert the Fourth Amendment or that lawlessness among these actors requires application of the extreme sanction of exclusion . . . . And, to the extent that the rule is thought to operate as a "systemic" deterrent on a wider audience, it clearly can have no such effect on individuals empowered to issue search warrants. Judges and magistrates are not adjuncts to the law enforcement team; as neutral judicial officers, they have no stake in the outcome of particular criminal prosecutions. The threat of exclusion thus cannot be expected significantly to deter them.

*Leon*, 468 U.S. at 916–17. Exclusion of the evidence in this case would only serve to "punish the errors of judges and magistrates" and would not have any "appreciable" effect on law enforcement. *Id.* at 909, 916.

Had the agents lied to the magistrate and told her that all the information being sought would be gathered only in the Eastern District of Virginia, the Court's analysis would likely change because suppression deters misrepresentations made to the Court. *See, e.g., Franks*, 438 U.S. at 171 (finding exclusion appropriate where there is proof of "deliberate falsehood or of reckless disregard for the truth"). In this case, however, the agents provided the magistrate with all the information she needed to "satisfy [herself] of [her] jurisdiction before proceeding . . . ." *Packard v. Provident Nat'l Bank*, 994 F.2d 1039, 1049 (3d Cir. 1993) (citations omitted). Once the warrant was issued, albeit outside the technical bounds of Rule 41(b), the agents acted upon an objectively reasonable good faith belief in the legality of their conduct. *Cf. Leon*, 468 U.S. at 921 ("In the ordinary case, an officer cannot be expected to question the magistrate's . . . judgment that the form of the warrant is technically sufficient . . . . Penalizing the officer for the



magistrate’s error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations.”).

Here, as in *Katzin*, “the Government’s evidence against [the defendant] is substantial, and it is uncontested that the Government would have no case without it.” *Katzin*, 769 F.3d at 186. The “cost” of suppression, therefore, would be letting a “guilty and possibly dangerous defendant[] go free—something that ‘offends basic concepts of the criminal justice system.’” *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 908). Absent any appreciable deterrent effect on law enforcement, suppression would only serve to “exact[] a heavy toll on both the judicial system and society at large.” *Davis*, 564 U.S. at 237.

An appropriate order follows.

BY THE COURT:

/s/ Gerald J. Pappert  
GERALD J. PAPPERT, J.



FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 32

- Page 161 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9,11;
- Page 162 ~ b6 - 1,2; b7C - 1,2; b7E - 2,3,8,9;
- Page 163 ~ b6 - 1,3; b7C - 1,3; b7E - 1,2,3,9,11;
- Page 164 ~ b6 - 1,2; b7C - 1,2; b7E - 3,8,9;
- Page 165 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9,11;
- Page 166 ~ b6 - 1; b7C - 1; b7E - 2,3,9;
- Page 167 ~ b6 - 3,4; b7C - 3,4; b7E - 1,2,3,9,11;
- Page 168 ~ b6 - 1; b7C - 1; b7E - 3,8,9;
- Page 169 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9,11;
- Page 170 ~ b6 - 1; b7C - 1; b7E - 2,3,9;
- Page 171 ~ b6 - 3,4; b7C - 3,4; b7E - 1,2,3,9,11;
- Page 172 ~ b6 - 1; b7C - 1; b7E - 3,8,9;
- Page 173 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9,11;
- Page 174 ~ b6 - 1; b7C - 1; b7E - 2,3,9;
- Page 175 ~ b6 - 3; b7C - 3; b7E - 1,2,3,5,7,9;
- Page 176 ~ b6 - 1; b7C - 1; b7E - 3,8,9;
- Page 177 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9,11;
- Page 178 ~ b6 - 1; b7C - 1; b7E - 2,3,8,9;
- Page 179 ~ b6 - 1,3; b7C - 1,3; b7E - 1,2,3,9;
- Page 180 ~ b6 - 1; b7C - 1; b7E - 3,8,9;
- Page 181 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9,11;
- Page 182 ~ b6 - 1; b7C - 1; b7E - 2,3,9;
- Page 183 ~ b6 - 3; b7C - 3; b7E - 1,2,3,7,9;
- Page 184 ~ b6 - 1; b7C - 1; b7E - 3,8,9;
- Page 185 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9,11;
- Page 186 ~ b6 - 1; b7C - 1; b7E - 2,3,8,9;
- Page 187 ~ b6 - 1,3,4; b7C - 1,3,4; b7E - 1,2,3,9,11;
- Page 188 ~ b6 - 1; b7C - 1; b7E - 3,8,9;
- Page 189 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9,11;
- Page 190 ~ b6 - 1; b7C - 1; b7E - 2,3,9;
- Page 191 ~ b6 - 1,3; b7C - 1,3; b7E - 1,2,3,6,7,9;
- Page 192 ~ b6 - 1; b7C - 1; b7E - 3,8,9;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 2  
Page 1 ~ b7E - 2,3,7,9;  
Page 2 ~ b7E - 1,2,3,9;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 64

Page 1 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 2 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 3 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 4 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 5 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 6 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 7 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 8 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 9 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 10 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 11 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 12 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 13 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 14 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 15 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 16 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 17 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 18 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 19 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 20 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 21 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 22 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 23 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 24 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 25 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 26 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 27 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 28 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 29 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 30 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 31 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 32 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;  
Page 33 ~ b7E - 3,9;  
Page 34 ~ b7E - 1,2,3,9;  
Page 35 ~ b7E - 1,2,3,9;  
Page 36 ~ b7E - 3,9;  
Page 37 ~ b7E - 3,9;  
Page 38 ~ b7E - 3,9;  
Page 39 ~ b7E - 3,9;  
Page 40 ~ b7E - 3,9;  
Page 41 ~ b7E - 3,9;  
Page 42 ~ b7E - 3,9;  
Page 43 ~ b7E - 3,9;  
Page 44 ~ b7E - 3,9;  
Page 45 ~ b7E - 1,2,3,9;  
Page 46 ~ b7E - 3,9;  
Page 47 ~ b7E - 3,9;  
Page 48 ~ b7E - 3,9;

Page 49 ~ b7E - 1,2,3,9;  
Page 50 ~ b7E - 3,9;  
Page 51 ~ b7E - 1,2,3,9;  
Page 52 ~ b7E - 3,9;  
Page 53 ~ b7E - 3,9;  
Page 54 ~ b7E - 3,9;  
Page 55 ~ b7E - 3,9;  
Page 56 ~ b7E - 1,2,3,9;  
Page 57 ~ b7E - 3,9;  
Page 58 ~ b7E - 3,9;  
Page 59 ~ b7E - 3,9;  
Page 60 ~ b7E - 3,9;  
Page 61 ~ b7E - 1,2,3,9;  
Page 62 ~ b7E - 3,9;  
Page 63 ~ b7E - 3,9;  
Page 64 ~ b7E - 3,9;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 8

- Page 1 ~ b6 - -3; b7C - -3; b7E - -1,2,3,5,9;
- Page 2 ~ b6 - -1; b7C - -1; b7E - -1,2,3,7,9;
- Page 3 ~ b6 - -3; b7C - -3; b7E - -1,2,3,9;
- Page 4 ~ b6 - -3; b7C - -3; b7E - -1,2,3,5,9;
- Page 5 ~ b6 - -1; b7C - -1; b7E - -1,2,3,7,9;
- Page 6 ~ b6 - -3; b7C - -3; b7E - -1,2,3,9;
- Page 7 ~ b7E - 2,3,7,9;
- Page 8 ~ b7E - 2,3,7,9;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 1  
Page 1 ~ b7E - 1,11;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXX



FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 2

Page 1 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;

Page 2 ~ b6 - 3; b7C - 3; b7E - 1,2,3,9;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 16  
Page 1 ~ Referral/Consult;  
Page 2 ~ Referral/Consult;  
Page 3 ~ Referral/Consult;  
Page 4 ~ Referral/Consult;  
Page 5 ~ Referral/Consult;  
Page 6 ~ Referral/Consult;  
Page 7 ~ Referral/Consult;  
Page 8 ~ Referral/Consult;  
Page 9 ~ Referral/Consult;  
Page 10 ~ Referral/Consult;  
Page 11 ~ Referral/Consult;  
Page 12 ~ Referral/Consult;  
Page 13 ~ Referral/Consult;  
Page 14 ~ Referral/Consult;  
Page 15 ~ Referral/Consult;  
Page 16 ~ Referral/Consult;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 12  
Page 1 ~ Referral/Consult;  
Page 2 ~ Referral/Consult;  
Page 3 ~ Referral/Consult;  
Page 4 ~ Referral/Consult;  
Page 5 ~ Referral/Consult;  
Page 6 ~ Referral/Consult;  
Page 7 ~ Referral/Consult;  
Page 8 ~ Referral/Consult;  
Page 9 ~ Referral/Consult;  
Page 10 ~ Referral/Consult;  
Page 11 ~ Referral/Consult;  
Page 12 ~ Referral/Consult;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 12

- Page 1 ~ Duplicate;
- Page 2 ~ Duplicate;
- Page 3 ~ Duplicate;
- Page 4 ~ Duplicate;
- Page 5 ~ Duplicate;
- Page 6 ~ Duplicate;
- Page 7 ~ Duplicate;
- Page 8 ~ Duplicate;
- Page 9 ~ Duplicate;
- Page 10 ~ Duplicate;
- Page 11 ~ Duplicate;
- Page 12 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 5  
Page 1 ~ b5 - 1,2,3; b7E - 7,12;  
Page 2 ~ b5 - 1,2,3; b7E - 7,12;  
Page 3 ~ b5 - 1,2,3; b7E - 7,12;  
Page 4 ~ b5 - 1,2,3; b7E - 7,12;  
Page 5 ~ b5 - 1,2,3; b7E - 7;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 6  
Page 1 ~ b5 - 1,2,3; b7E - 7,12;  
Page 2 ~ b5 - 1,2,3; b7E - 7,12;  
Page 3 ~ b5 - 1,2,3; b7E - 7,12;  
Page 4 ~ b5 - 1,2,3; b7E - 7,12;  
Page 5 ~ b5 - 1,2,3; b7E - 5,7,12;  
Page 6 ~ b5 - 1,2,3; b7E - 7;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 8

- Page 1 ~ b7E - 3,7;
- Page 2 ~ b7E - 3,7;
- Page 3 ~ b7E - 3,7;
- Page 4 ~ b7E - 3,7,8;
- Page 5 ~ b7E - 3,7,8;
- Page 6 ~ b7E - 3,7,8;
- Page 7 ~ b7E - 3,7,8;
- Page 8 ~ b7E - 3,7,8;

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
Civil Action# 18-cv-1488

Total Deleted Page(s) = 14  
Page 1 ~ Referral/Consult;  
Page 2 ~ Referral/Consult;  
Page 3 ~ Referral/Consult;  
Page 4 ~ Referral/Consult;  
Page 5 ~ Referral/Consult;  
Page 6 ~ Referral/Consult;  
Page 7 ~ Referral/Consult;  
Page 8 ~ Referral/Consult;  
Page 9 ~ Referral/Consult;  
Page 10 ~ Referral/Consult;  
Page 11 ~ Referral/Consult;  
Page 12 ~ Referral/Consult;  
Page 13 ~ Referral/Consult;  
Page 14 ~ Referral/Consult;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXX