APPENDIX

Appendix A

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

15-CR-485 (FB)

UNITED STATES OF AMERICA

v.

NARAY PALANIAPPAN,

Defendant.

MEMORANDUM AND ORDER

BLOCK, Senior District Judge:

The defendant is charged with receipt and possession of child pornography. This memorandum and order addresses his (1) motion to suppress evidence, (2) motion to dismiss the indictment, and (3) motion to compel discovery. For the following reasons, the motions are denied.

1. Motion to Suppress

The Court holds that use of the Network Investigative Technique ("NIT") was a search and that the warrant for the search violated the geographic limitation of Federal Rule of Criminal Procedure 41(b)(1) in effect at the time.[11] The Court need not decide whether the violation was of constitutional magnitude, however, because suppression is not an appropriate remedy in either case.

"[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." *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975). There was no prejudice because the FBI could have obtained the same warrant from a district judge, *see United States v. Villegas*, 899 F.2d 1324, 1334 (2d Cir. 1990) ("[Rule 41] does not define the extent of the [district] court's power to issue a search warrant."), and because the FBI complied with the extended deadline for giving the defendant notice of the warrant.

---

[1] The Rule has since been amended—specifically to address concerns about the NIT warrant—to allow magistrates in any district to issue warrants "to use remote access to search electronic storage media . . . located within or outside that district." Fed. R. Crim. P. 41(b)(6).

Nor did the FBI intentionally and deliberately disregard Rule 41's geographical limitation on the magistrate judge's authority. The Playpen website's efforts to protect its users' anonymity posed a novel problem. The FBI disclosed the salient facts about its proposed solution to the magistrate judge, including the fact that the NIT would be installed on a server in Virginia, but deployed on any computer accessing the server, regardless of location. This reflects a reasoned judgment as to how to comply with Rule 41 in unique circumstances, not an attempt to flout it.

Even if the violation of Rule 41 was of constitutional magnitude, the good-faith exception of *United States v. Leon*, 468 U.S. 897 (1984), forecloses suppression. The unique circumstances made it reasonable for the FBI to rely on the magistrate judge's determination that she could authorize a remote search from a computer located in the Eastern District of Virginia. *See id*. at 920 ("In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient."). Contrary to the defendant's contention, the warrant did not, on its face, limit use of the NIT to computers located in the district. The problems that might create under Rule 41 were not so obvious as to make the executing officers' reliance on the warrant unreasonable. See *United States v. Workman*, 863 F.3d 1313, 1321 (10th Cir. 2017) ("We expect agents executing warrants to be reasonably well-trained, but we do not expect them to understand legal nuances the way that an attorney would.").

2. Motion to Dismiss

"Government involvement in a crime may in theory become so excessive that it violates due process and requires the dismissal of charges against a defendant even if the defendant was not entrapped." *United States v. Al Kassar,* 660 F.3d 108, 121 (2d Cir. 2011) (emphasis added). But "only Government conduct that 'shocks the conscience' can violate due process." *United States v. Rahman*, 189 F.3d 88, 131 (2d Cir. 1999). The burden of showing sufficiently outrageous conduct is "very heavy," *id.*, principally because courts are reluctant to abandon their "well-established deference to the Government's choice of investigatory methods." *Id.* "It does not suffice to show that the government created the opportunity for the offense, even if the government's ploy is elaborate and the engagement with the defendant is extensive." Al Kassar, 660 F.3d at 121.

Generally, "the government's involvement in a crime must involve either coercion or a violation of the defendant's person," *id.*, neither of which is present here. In *United States v. Chin*, 934 F.2d 393 (2d Cir. 1991), however, the Second Circuit concluded that a lack of harm to the defendant "does not end our analysis," *id.* at 399, and went on to consider the harm to third parties and, in particular, the victims of child pornography: Our concern is that, in contrast to the usual sting operation, in which the Government sets up a phony drug transaction or another sort of dummy crime, the government agent in this case encouraged

Chin to go out and commit a real crime, with real victims, just so Chin could later be arrested and prosecuted. In particular, [an undercover postal inspector] explicitly and repeatedly encouraged Chin to proceed with his trip to Amsterdam to obtain "Lolita materials," despite the fact that purchasing child pornography, by increasing the demand for such materials, serves to further the sexual exploitation of minors.

Id. The circuit court "cautioned law enforcement agents to think twice before engaging in investigative techniques that encourage individuals to commit actions that harm innocent third parties," *id*. at 400, but did not dismiss the indictment because the defendant could not establish "[a] necessary prerequisite for demonstrating that an undercover investigation violated the rights of third parties," *id*., namely, "proof that the governmental action actually caused the defendant to commit a crime that would otherwise not have been committed," *id*.

Here, the FBI delayed shutting down an existing website for two weeks. The child pornography itself was uploaded and retrieved by users like the defendant, just as it had been before February 20, 2015. Moving the site to a government server obviously meant greater government involvement, but the harm to victims was the same as letting the website continue to operate from its original server. The decision to leave the site operational arguably "created the opportunity for the offense," *Al Kassar*,

660 F.3d at 121, but it did not encourage the defendant or anyone else to visit the site.

Of course, the FBI could have decided to shut down the site immediately and prevent the further distribution of the images it hosted. But that option would have meant leaving users of the site unidentified and unapprehended, free to continue sharing child pornography by other means. See *United States v. Kim*, 2017 WL 394498, at *7 (E.D.N.Y. Jan. 27, 2017) ("[T]here is no evidence upon which the Court can conclude that individuals interested in child pornography would have been so easily deterred from obtaining it by the shutting down of the Playpen website."). Whether an immediate shutdown or a delay would have best served the long-term effort to combat child pornography is precisely the kind of difficult decision that courts should not second-guess.

3. Motion to Compel

Federal Rule of Criminal Procedure 16(a)(1)(E)(i)(E) requires the government to produce any item within its custody or control that is "material to preparing the
defense." The defendant argues that the "exploit code" that allowed the NIT to take advantage of a software vulnerability on the defendant's computer is material in two ways.

First, he argues that the exploit code might allow him to investigate whether the NIT transmitted information from his computer beyond the scope of the warrant authorizing its use. Rule 16 deals with information material to the defendant's case on the merits, not collateral issues like a motion to suppress. Cf. *United States v. Armstrong*, 517 U.S. 456, 463 (1996) ("Rule 16(a)(1)(C) authorizes defendants to examine Government documents material to the preparation of their defense against the Government's case in chief, but not to the preparation of selective-prosecution claims." (Emphasis added)).

Second, he argues that the exploit code might reveal that the NIT left his computer vulnerable to hacking, thus bolstering a claim that the pornography found on his computer was placed there without his knowledge. This would be speculative under the best of circumstances, but the defendant has already admitted to agents that he visited the website and downloaded the images he is charged with possessing.

SO ORDERED.

/S/ Frederic Block
FREDERIC BLOCK
Senior United States District Judge

Brooklyn, New York
April 27, 2018

Appendix B

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

Alexandria Division

IN THE MATTER OF THE SEARCH OF
COMPUTERS THAT ACCESS
upf45jv3bziuctml.onion

FILED UNDER SEAL
Case No. 1:15-SW-89

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Douglas Macfarlane, being first duly sworn, hereby depose and state:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") since April, 1996, and I am currently assigned to the FBI's Violent Crimes Against Children Section, Major Case Coordination Unit ("MCCU"). I currently investigate federal violations concerning child pornography and the

sexual exploitation of children and have gained experience through training in seminars, classes, and everyday work related to these types of investigations. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information, in conjunction with criminal investigations pertaining to child pornography the sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

2. I make this affidavit in support of an application for a search warrant to use a network investigative technique ("NIT") to investigate the users and administrators of the website upf45jv3bziuctml.onion (hereinafter "TARGET WEBSITE") as further described in this affidavit and its attachments. [2]

---

[1] The common name of the TARGET WEBSITE is known to law enforcement. The site remains active and disclosure of the

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies as described below; information gathered from the service of subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; my experience, training and background as a Special Agent with the FBI, and communication with computer forensic professionals assisting with the design and implementation of the NIT. This affidavit includes only those facts that I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation.

RELEVANT STATUTES

---

name of the site would potentially alert users to the fact that law enforcement action is being taken against the site, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms.

4. This investigation concerns alleged violations of: 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 225l(d)(l) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(l), Receiving and Distributing/Conspiracy to Receive and Distribute Child Pornography; and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Possession, Access or Attempted Access With Intent to View Child Pornography.
   a. 18 U.S.C. § 2252A(g) prohibits a person from engaging m a child exploitation enterprise. A person engages in a child exploitation enterprise if the person violates, inter alia, federal child pornography crimes listed in Title 18, Chapter 110, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons;
   b. 18 U.S.C. §§ 2251(d)(l) and (e) prohibits a person from knowingly making, printing or publishing, or causing to be made, printed or published, or conspiring to make, print or publish, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or (B) participation in any act of sexually

explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

c. 18 U.S.C. §§ 2252A(a)(2) and (b)(l) prohibits a person from knowingly receiving or distributing, or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

d. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITION OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

5. The following definitions apply to this Affidavit:
   a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the bulletin board administrator.
   b. "Child erotica," as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes,

drawings, and images or videos of minors that are not sexually explicit.

c. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer- generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(l) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A "web server," for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS")

server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work.

Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Hyperlink" refers to an item on a web page which, when selected, transfers the user

directly to another location in a hypertext document or to some other web page.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name - a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish

communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

m. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the Internet Service Provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

n. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs,

electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

p. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse including genital-genital, oral-genital, anal-genital or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

q. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

r. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper- Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

PROBABLE CAUSE

6. The targets of the investigative technique described herein are the administrators and users of the TARGET WEBSITE - upf45jv3bziuctml.onion - which operates as a "hidden service" located on the Tor network, as further described below. The TARGET WEBSITE is dedicated to the advertisement and distribution of child pornography, the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders use to abuse children, as well as methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes such as those described in paragraph 4 of this affidavit. The administrators and users of the TARGET WEBSITE regularly send and receive illegal child pornography via the website.

The Tor Network

7. The TARGET WEBSITE operates on an anonymity network available to Internet users known as "The Onion Router" or "Tor" network. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the

publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.[3]

8. The Tor software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no

[3] Users may also access the Tor network through so-called "gateways" on the open Internet such as "onion.to" and "tor2web.org," however, use of those gateways does not provide users with the anonymizing benefits of the Tor network.

practical way to trace the user's actual IP back through that Tor exit node IP. In that way, using 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.

9. Tor also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Tor network itself, entire websites can be set up as "hidden services." "Hidden services," like other websites, are hosted on computer servers that communicate through IP addresses and operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm- generated characters, such as "asdlk8fs9dflku7f' followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

Finding and Accessing the TARGET WEBSITE

10. Because the TARGET WEBSITE is a Tor hidden service, it does not reside on the traditional or "open" Internet. A user may only access the TARGET WEBSITE through the Tor network. Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the site. Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. The TARGET WEBSITE is listed in that section. Accessing the TARGET WEBSITE therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon the TARGET WEBSITE without understanding its purpose and content. In addition, upon arrival at the TARGET WEBSITE, the user sees images of prepubescent females partially clothed and whose legs are spread with instructions for joining the site

before one can enter. Accordingly, there is probable cause to believe that, for the reasons described below, any user who successfully accesses the TARGET WEBSITE has knowingly accessed with intent to view child pornography, or attempted to do so.

Description of the TARGET WEBSITE and Its Content

11. Between September 16, 2014 and February 3, 2015, FBI Special Agents operating in the District of Maryland connected to the Internet via the Tor Browser and accessed the Tor hidden service the TARGET WEBSITE at its then-current Uniform Resource Locator ("URL") mufl7i44irws3mwu.onion.[4] The TARGET WEBSITE appeared to be a message board website whose primary purpose is the advertisement and distribution of child pornography. According to statistics posted on the site, the TARGET WEBSITE contained a total of 95,148 posts, 9,333 total topics, and 158,094 total members. The website appeared to

[4] As of February 18, 2015, the URL of the TARGET WEBSITE had changed from muff7i44irws3mwu.onion to upf45jv3bziuctml.onion. I am aware from my training and experience that it is possible for a website to be moved from one URL to another without altering its content or functionality. I am also aware from the instant investigation that the administrator of the TARGET WEBSITE occasionally changes the location and URL of the TARGET WEBSITE in an effort to , in part, avoid law enforcement detection. On February 18, 2015, I accessed the TARGET

have been operating since approximately August 2014 which is when the first post was made on the message board.

12. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to the TARGET WEBSITE; and ". 7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' (a hyperlink to the registration page) with [TARGET WEBSITE name]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

13. Upon accessing the "register an account" hyperlink, the following message was displayed:

"VERY IMPORTANT. READ ALL OF THIS PLEASE.

I will add to this as needed.

The software we use for this forum requires that new users enter an email address, and checks that what you enter looks approximately valid. We can't tum this off but the forum operators do NOT want you to enter a real address, just something that matches the xxx@yyy.zzz pattern. No confirmation email will be sent. This board has been intentionally configured so that it WILL NOT SEND EMAIL, EVER. Do not forget your password, you won't be able to recover it.

After you register and login to this forum you will be able to fill out a detailed profile. For your security you should not post information here that can be used to identify you.

Spam, flooding, advertisements, chain letters, pyramid schemes, and solicitations are forbidden on this forum.

Note that it is impossible for the staff or the owners of this forum to confirm the true identity of users or monitor in realtime all messages posted, and as such we are not responsible for the content posted

---

WEBSITE in an undercover capacity at its new URL, and determined that its content has not changed.

by those users. You remain solely responsible for the content of your posted messages.

The forum software places a cookie, a text file containing bits of information (such as your username and password), in your browser's cache. This is ONLY used to keep you logged in/out. This website is not able to see your IP and can not collect or send any other form of information to your computer except what you expressly upload. For your own security when browsing or Tor we also recomend that you turn off javascript and disable sending of the 'referer' header."

14. After accepting the above terms, registration to the message board then requires a user to enter a usemame, password, and e-mail account; although a valid e-mail account was not required as described above. After successfully registering and logging into the site, the following sections, forums, and sub-forums, along with the corresponding number of topics and posts in each, were observed:

Section – Forum	**Topics**	**Posts**
General Category		
[the TARGET WEBSITE] information and rules	25	236
How to	133	863
Security & Technology	281	2,035

discussion		
Request	650	2,487
General discussion	1,390	13,918
The INDEXES	10	119
Trash Pen	87	1,273
[the TARGET WEBSITE] Chan		
Jailbait – Boy[6]	58	154
Jailbait – Girl	271	2,334
Preteen – Boy	32	257
Preteen – Girl	264	3,763
Jailbait Videos		
Girls	643	8,282
Boys	34	183
Jailbait Photos		
Girls	339	2,590
Boys	6	39
Pre-teen Videos		
Girls HC[7]	1,427	20,992

[6] Based on my training and experience, I know that "jailbait" refers to underage but post-pubescent minors

[7] Based on my training and experience, I know that the following abbreviations respectively mean: HC - hardcore, i.e., depictions of penetrative sexually explicit conduct; SC- softcore, i.e., depictions of non-penetrative sexually explicit conduct; NN - non-nude, i.e., depictions of subjects who are fully or partially clothed.

Girls SC/NN	514	5,635
Boys HC	87	1,256
Boys SC/NN	48	193
Pre-teen Photos		
Girls HC	433	5,314
Girls SC/NN	486	4,902
Boys HC	38	330
Boys SC/NN	48	193
Webcams		
Girls	133	2,423
Boys	5	12
Potpourri		
Family [TARGET WEBSITE] –		
Incest	76	1,718
Toddlers	106	1,336
Artwork	58	314
Kinky Fetish		
Bondage	16	222
Chubby	27	309
Feet	30	218
Panties, nylons, spandex	30	369
Peeing	101	865
Scat	17	232
Spanking	28	251
Vintage	84	878

Voyeur	37	454
Zoo	25	222
Other Languages		
Italiano	34	1,277
Portugues	69	905
Deutsch	66	570
Espanol	168	1,614
Nederlands	18	264
Pyccknn – Russian	8	239
Stories		
Fiction	99	505
Non-Fiction	122	675

15. An additional section and forum was also listed in which members could exchange usernames on a Tor-network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

16. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any

corresponding replies to the original post included the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as ".rar" files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

17. A review of the various topics within the "[the TARGET WEBSITE] information and rules," "How to," "General Discussion," and "Security & Technology discussion" forums revealed the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

18. A review of topics within the remaining forums revealed the majority contained discussions, as well as numerous images that appeared to depict child pornography ("CP") and child erotica of prepubescent females, males, and toddlers. Examples of these are as follows:

    On February 3, 2015, the user "Mr. Devi" posted a topic entitled "Buratino-06" in the forum "Pre-teen - Videos - Girls HC" that contained numerous images depicting CP of a prepubescent or early pubescent female. One of these images depicted the female being orally penetrated by the penis of a naked male.

On January 30, 2015, the user "MoDoM" posted a topic entitled "Sammy" in the forum "Pre-teen Photos - Girls HC" that contained hundreds of images depicting CP of a prepubescent female. One of these images depicted the female being orally penetrated by the penis of a male.

On September 16, 2014, the user "tutu0l" posted a topic entitled "9yo Niece - Horse.mpg" in the "Pre-teen Videos - Girls HC" forum that contained four images depicting CP of a prepubescent female and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent female. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

19. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. Analysis of available historical data seized from the TARGET WEBSITE, as described below, revealed that over 1,500 unique users visited the website daily and over 11,000 unique users visited the website over the course of a week.

20. A private message feature also appeared to be available on the site, after registering, that allowed users to send other users private messages , referred to as "personal messages or PMs," which are only accessible to the sender and recipient of the message. Review of the site demonstrated that the site administrator made a posting on January 28, 2015, in response to another user in which he stated, among other things, "Yes PMs should now be fixed. As far as a limit, I have not deleted one yet and I have a few hundred there now…"

21. Further review revealed numerous additional posts referencing private messages or PMs regarding topics related to child pornography, including one posted by a user stating, "Yes i can help if you are a teen boy and want to fuck your little sister. write me a private message."

22. Based on my training and experience and the review of the site by law enforcement agents, I believe that the private message function of the site is being used to communicate regarding the dissemination of child pornography and to share information among users that may assist in the identification of the users.

23. The TARGET WEBSITE also includes a feature referred to as "[the TARGET WEBSITE] Image Hosting". This feature of the TARGET

WEBSITE allows users of the TARGET WEBSITE to upload links to images of child pornography that are accessible to all registered users of the TARGET WEBSITE. On February 12, 2015, an FBI Agent accessed a post on the TARGET WEBSITE titled "Giselita" which was created by the TARGET WEBSITE user "Dark Ghost". The post contained links to images stored on "[the TARGET WEBSITE] Image Hosting". The images depicted a prepubescent female in various states of undress. Some images were focused on the nude genitals of a prepubescent female. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent female.

24. The TARGET WEBSITE also includes a feature referred to as "[the TARGET WEBSITE] File Hosting". This feature of the TARGET WEBSITE allows users of the TARGET WEBSITE to upload videos of child pornography that are in tum, only accessible to users of the TARGET WEBSITE. On February 12, 2015, an FBI Agent accessed a post on the TARGET WEBSITE titled "Vicky Coughing Cum" which was created by the TARGET WEBSITE user "clitflix". The post contained a link to a video file stored on "[the TARGET WEBSITE] File Hosting". The video depicted an adult male masturbating and ejaculating into the mouth of a nude, prepubescent female.

25. The TARGET WEBSITE also includes a feature referred to as "[the TARGET WEBSITE] Chat". On February 6, 2015, an FBI Special Agent operating in the District of Maryland accessed "[the TARGET WEBSITE] Chat" which was hosted on the same URL as the TARGET WEBSITE. The hyperlink to access "[the TARGET WEBSITE] Chat" was located on the main index page of the TARGET WEBSITE. After logging in to [the TARGET WEBSITE] Chat, over 50 users were observed to be logged in to the service. While logged in to [the TARGET WEBSITE] Chat, the following observations were made:

> User "gabs" posted a link to an image that depicted four females performing oral sex on each other. At least two of the females depicted were prepubescent.
>
> User "Rusty" posted a link to an image that depicted a prepubescent female with an amber colored object inserted into her vagina.
>
> User "owlmagic" posted a link to an image that depicted two prepubescent females laying on a bed with their legs in the air exposing their nude genitals.

Other images that appeared to depict child pornography were also observed

26. The images described above, as well as other images, were captured and are maintained as evidence.

THE TARGET WEBSITE SUB-FORUMS

27. While the entirety of the TARGET WEBSITE is dedicated to child pornography, the following sub-forums of the TARGET WEBSITE were reviewed and determined to contain the most egregious examples of child pornography and/or dedicated to retellings of real world hands on sexual abuse of children.
    - Pre-teen Videos - Girls HC
    - Pre-teen Videos - Boys HC
    - Pre-teen Photos - Girls HC
    - Pre-teen Photos - Boys HC
    - Potpourri - Toddlers
    - Potpourri - Family Play Pen - Incest
    - Spanking
    - Kinky Fetish - Bondage
    - Peeing
    - Scat[8]
    - Stories - Non-Fiction
    - Zoo
    - Webcams - Girls
    - Webcams - Boys

Identification and Seizure of the Computer Server Hosting the TARGET WEBSITE

28. In December of 2014, a foreign law enforcement agency advised the FBI that it suspected IP address 192.198.81.106, which is a United States-based IP address, to be associated with the TARGET WEBSITE. A publicly available website

[8] Based on my training and experience, "scat" refers to sexually explicit activity involving defecation and/or feces.

provided information that the IP Address 192.198.81.106 was owned by Centrilogic, a server hosting company headquartered at 80I Main Street NW, Lenoir, NC 28645-3907. Through further investigation, FBI verified that the TARGET WEBSITE was hosted from the previously referenced IP address. A Search Warrant was obtained and executed at Centrilogic in January 2015 and a copy of the server (hereinafter the "TARGET SERVER") that was assigned IP Address 192.198.81.106 was seized. FBI Agents reviewed the contents of the Target Server and observed that it contained a copy of the TARGET WEBSITE. A copy of the TARGET SERVER containing the contents of the TARGET WEBSITE is currently located on a computer server at a government facility in Newington, VA, in the Eastern District of Virginia. Further investigation has identified a resident ofNaples, FL, as the suspected administrator of the TARGET WEBSITE, who has administrative control over the computer server in Lenoir, NC, that hosts the TARGET WEBSITE.

29. While possession of the server data will provide important evidence concerning the criminal activity that has occurred on the server and the TARGET WEBSITE, the identities of the administrators and users of the TARGET WEBSITE would remain unknown without use of additional investigative techniques. Sometimes, non-Tor-based websites have IP address logs that can be used to locate and identify the board's users. In such cases, a publicly available lookup would be performed to determine what ISP owned the target IP address, and a subpoena would be sent to that ISP to determine the user to which the IP address

was assigned at a given date and time. However, in the case of the TARGET WEBSITE, the logs of member activity will contain only the IP addresses of Tor "exit nodes" utilized by board users. Generally, those IP address logs cannot be used to locate and identify the administrators and users of the TARGET WEBSITE. [9]

30. Accordingly, on February 19, 2015, FBI personnel executed a court-authorized search at the Naple_ s, FL, residence of the suspected administrator of the TARGET WEBSITE. That individual was apprehended and the FBI has assumed administrative control of the TARGET WEBSITE. The TARGET WEBSITE will continue to operate from the government-controlled computer server in Newington, Virginia, on which a copy ofT ARGET WEBSITE currently resides. These actions will take place for a limited period of time, not to exceed 30 days, in order to locate and identify the administrators and users of TARGET WEBSITE through the deployment of the network investigative technique described below. Such a tactic is necessary in order to locate and apprehend the TARGET SUBJECTS who are engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.

THE NETWORK INVESTIGATIVE TECHNIQUE

[9] Due to a misconfiguration of the TARGET WEBSITE that existed for an unknown period of time, the true IP Addresses ofa small number of users of the TARGET WEBSITE (that amounted to less than 1% of registered users of the TARGET WEBSITE) were captured in the Jog files stored on the Centrilogic server.

31. Based on my training and experience as a Special Agent, as well as the experience of other law enforcement officers and computer forensic professionals involved in this investigation, and based upon all of the facts set forth herein, to my knowledge a network investigative technique ("NIT") such as the one applied for herein consists of a presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location and identity of those users and administrators of the TARGET WEBSITE described in Attachment A who are engaging in the federal offenses enumerated in paragraph 4. 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," as described herein, other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

32. Based on my training, experience, and the investigation described above, I have concluded that using a NIT may help FBI agents locate the administrators and users of the TARGET WEBSITE. Accordingly, I request authority to use the NIT, which will be deployed on the TARGET WEBSITE, while the TARGET WEBSITE operates in the Eastern District of Virginia, to investigate any user or administrator who logs into the TARGET WEBSITE by entering a

username and password.[10]

33. 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. The NIT will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

---

[10] Although this application and affidavit requests authority to deploy the NIT to investigate any user who logs in to the TARGET WEBSITE with a username and password, in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation, in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users, such as those who have attained a higher status on Website l by engaging in substantial posting activity, or in particular areas of TARGET WEBSITE, such as the TARGET WEBSITE sub forums described in Paragraph 27.

34. The NIT will reveal to the government environmental variables and certain registry-type information that may assist in identifying the user's computer, its location, and the user of the computer, as to which there is probable cause to believe is evidence of violations of the statutes cited in paragraph 4. In particular, the NIT will only reveal to the government the following items, which are also described in Attachment B:
    a. The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
    b. A unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating" computers. That unique identifier will be sent with and collected by the NIT;
    c. 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);
    d. Information about whether the NIT has already been delivered to the "activating" computer;
    e. The "activating" computer's "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;
    f. the "activating" computer's active operating system username; and
    g. The "activating" computer's Media Access Control ("MAC") address. The equipment

that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

35. Each of these categories of information described above, and in Attachment B, may constitute evidence of the crimes under investigation, including information that may help to identify the "activating" computer and its user. The actual IP address of a computer that accesses the TARGET WEBSITE can be associated with an ISP and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

36. During the up to thirty day period that the NIT is deployed on the TARGET WEBSITE, which

will be located in the Eastern District of Virginia, each time that any user or administrator logs into the TARGET WEBSITE by entering a username and password, this application requests authority for the NIT authorized by this warrant to attempt to cause the user's computer to send the above-described information to a computer controlled by or known to the government that is located in the Eastern District of Virginia.

37. In the normal course of the operation of a web site, a user sends "request data" to the web site in order to access that site. While the TARGET WEBSITE operates at a government facility, such request data associated with a user's actions on the TARGET WEBSITE will be collected. That data collection is not a function of the NIT. Such request data can be paired with data collected by the NIT, however, in order to attempt to identify a particular user and to determine that particular user's actions on the TARGET WEBSITE.

REQUEST FOR DELAYED NOTICE

38. Rule 41(f)(3) allows for the delay of any notice required by the rule if authorized by statute. 18 U.S.C. § 3103a(b)(l) and (3) allows for any notice to be delayed if "the Court finds reasonable grounds to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in 18 U.S.C. § 2705) ... ," or where the warrant "provides for the giving of such notice within a reasonable period

not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay." Because there are legitimate law enforcement interests that justify the unannounced use of a NIT, I ask this Court to authorize the proposed use of the NIT without the prior announcement of its use. Announcing the use of the NIT could cause the users or administrators of the TARGET WEBSITE to undertake other measures to conceal their identity, or abandon the use of the TARGET WEBSITE completely, thereby defeating the purpose of the search.

39. The government submits that notice of the use of the NIT, as otherwise required by Federal Rule of Criminal Procedure 41(f), would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing the TARGET WEBSITE. It would, therefore, seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(l) and 18 U.S.C. § 2705).

40. Furthermore, the investigation has not yet identified an appropriate person to whom such notice can be given. Thus, the government requests authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing the

TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.

41. The government further submits that, to the extent that 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. Furthermore, the NIT does not deny the users or administrators access to the TARGET WEBSITE or the possession or use of the information delivered to the computer controlled by or known to the government, nor does the NIT permanently alter any software or programs on the user's computer.

TIMING OF SEIZURE / REVIEW OF INFORMATION

42. Rule 41(e)(2) requires that the warrant command FBI "to execute the warrant within a specified period of time no longer than fourteen days" and to "execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time." After the server hosting the TARGET WEBSITE is seized, it will remain in law enforcement custody. Accordingly, the government requests authority to employ the NIT onto the TARGET

WEBSITE at any time of day, within fourteen days of the Court's authorization. The NIT will be used on the TARGET WEBSITE for not more than 30-days from the date of the issuance of the warrant.

43. For the reasons above and further, because users of the TARGET WEBSITE communicate on the board at various hours of the day, including outside the time period between 6:00 a.m. and 10:00 p.m., and because the timing of the user's communication on the board is solely determined by when the user chooses to access the board, rather than by law enforcement, I request authority for the NIT to be employed at any time a user's computer accesses the TARGET WEBSITE, even if that occurs outside the hours of 6:00 a.m. and 10:00 p.m. Further, I seek permission to review information transmitted to a computer controlled by or known to the government, as a result of the NIT, at whatever time of day or night the information is received.

44. The government does not currently know the exact configuration of the computers that may be used to access the TARGET WEBSITE. Variations in configuration, e.g., different operating systems, may require the government to send more than one communication in order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the activating computers for up to 30 days after this warrant is authorized.

45. The Government may, if necessary, seek further authorization from the Court to employ the NIT on the TARGET WEBSITE beyond the 30-day period authorized by this warrant.

SEARCH AUTHORIZATION REQUESTS

46. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:
    a. 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;
    b. the use of multiple communications, without prior announcement, within 30 days from the date this Court issues the requested warrant;
    c. that the government may receive and read, at any time of day or night, within 30 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by or known to the government;
    d. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(t)(3) of the Federal Rules of Criminal Procedure, the government may delay

providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an "activating" computer that accessed the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

REQUEST FOR SEALING OF APPLICATION AFFIDAVIT

47. I further request that this application and the related documents be filed under seal. This information to be obtained is relevant to an ongoing investigation. Premature disclosures of this application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of this technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.[11]

48. Based on the information identified above, information provided to me, and my experience and training, I have probable cause to believe

[11] The United States considers this technique to be covered by law enforcement privilege. Should the Court wish to issue any written opinion regarding any aspect of this request, the United States requests notice and an opportunity to be heard with respect to the issue of law enforcement privilege.

there exists evidence, fruits, and instrumentalities of criminal activity related to the sexual exploitation of children on computers that access the TARGET WEBSITE, in violation of 18 U.S.C. §§ 2251 and 2252A.

49. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of these crimes.

50. Based on the information described above, there is probable cause to believe that employing a NIT on the TARGET WEBSITE, to collect information described in Attachment B, will result in the FBI obtaining the evidence and instrumentalities of the child exploitation crimes described above.

Sworn to under the pains and penalties of perjury.

/S/ Douglas Macfarlane
Special Agent

Sworn to and subscribed before me
this 20th day of February

/S/ Theresa Carroll Buchanan
Honorable Theresa Carroll Buchanan
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Place to be Searched

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

The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL -upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia.

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

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

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

2. a unique identifier generated by the NIT (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;

that is evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(l) and or (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(l), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography.

Appendix C

UNITED STATES DISTRICT COURT
for the Eastern District of Virginia

In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address) OF COMPUTERS THAT ACCESS upf45jv3bziuctml.onion

Case NO. 1:15-SW-89

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or 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

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 6, 2015 (not to exceed 14 days) in the daytime 6:00 a.m. to 10 p.m. at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Honorable Theresa Carroll Buchanan.

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized for 30 days (not to-exceed 30).

Date and time issued 2/20/2015 at 11:45
/S/

City and state: Alexandria. Virginia

Honorable Theresa Carroll Buchanan
U.S. Magistrate Judge
/S/

ATTACHMENT A

Place to be Searched

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

The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL

upf45jv3bziuctml.onion which will be located at a government facility in the Eastern District of Virginia.

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

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

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

2. a unique identifier generated by the NIT (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;

that is evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(l) and or (e), Advertising and Conspiracy to Advertise Child pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(l), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Access or

Attempted Access With Intent to View Child Pornography.

Appendix D

19-1660-cr
United States v. Palaniappan

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

SUMMARY ORDER

RULINGS BY SUMMARY ORDER DO NOT HAVE PRECEDENTIAL EFFECT. CITATION TO A SUMMARY ORDER FILED ON OR AFTER JANUARY 1, 2007, IS PERMITTED AND IS GOVERNED BY FEDERAL RULE OF APPELLATE PROCEDURE 32.1 AND THIS COURT'S LOCAL RULE 32.1.1. WHEN CITING A SUMMARY ORDER IN A DOCUMENT FILED WITH THIS COURT, A PARTY MUST CITE EITHER THE FEDERAL APPENDIX OR AN ELECTRONIC DATABASE (WITH THE NOTATION "SUMMARY ORDER"). A PARTY CITING TO A SUMMARY ORDER MUST SERVE A COPY OF IT ON ANY PARTY NOT REPRESENTED BY COUNSEL.

At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 17th day of March, two thousand twenty.

PRESENT:

BARRINGTON D. PARKER,
RAYMOND J. LOHIER, JR.,
Circuit Judges,
RICHARD K. EATON,*
Judge.

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

Docket No. 19-1660-cr

UNITED STATES OF AMERICA,
Appellee,

v.

NARAY PALANIAPPAN,
Defendant-Appellant.

FOR DEFENDANT-APPELLANT:
ADAM ELEWA (Zachary Margulis-Ohnuma, on the brief), The Law Office of Zachary Margulis-Ohnuma, New York, NY.

FOR APPELLEE:

---

* Judge Richard K. Eaton, of the United States Court of International Trade, sitting by designation.

DAVID GOPSTEIN, Assistant United States Attorney (Samuel P. Nitze, Assistant United States Attorney, on the brief), for Richard P. Donoghue, United States Attorney for the Eastern District of New York, Brooklyn, NY.

Appeal from a judgment of the United States District Court for the Eastern District of New York (Frederic Block, Judge).

Appeal from a judgment of the United States District Court for the Eastern District of New York (Frederick Block, *Judge*).

UPON DUE CONSIDERATION, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED that the judgment of the District Court is AFFIRMED.

Naray Palaniappan appeals from a judgment of the District Court (Block, J.) convicting him, after a guilty plea, of receipt of child pornography in violation of 18 U.S.C. § 2252(a) and sentencing him principally to a term of sixty months' imprisonment. On appeal, Palaniappan argues that the District Court erred in denying his motion to suppress evidence that the Government obtained from his home computer in Queens, New York. We assume the parties' familiarity with the underlying facts and the record of prior proceedings, to which we refer only as necessary to explain our decision to affirm.

In 2015, as part of its investigation into the child pornography website Playpen, the Federal Bureau of Investigation obtained a warrant authorizing it to

install a tracking software known as the Network Investigative Technique on all computers that accessed the site (NIT Warrant). One such computer belonged to Palaniappan and was tracked from February 20, 2015 to March 1, 2015.

Palaniappan was arrested on September 1, 2015.

After his arrest, Palaniappan moved to have all evidence that resulted from the NIT Warrant suppressed, arguing that the Warrant violated the Fourth Amendment, the Federal Magistrates Act, and the then-existing version of Rule 41 of the Federal Rules of Criminal Procedure.

The District Court denied Palaniappan's motion, reasoning that evidence obtained from an unlawful warrant may not be suppressed when, as the District Court concluded had occurred here, the Government procured and relied upon the warrant in good faith. *See United States v. Leon*, 468 U.S. 897, 922–25 (1984). Palaniappan contends that this was error.

As Palaniappan recognizes, his appeal is governed largely by *United States v. Eldred*, where we affirmed a district court's denial of a motion to suppress evidence that was gathered under the same NIT Warrant at issue in this case. *See* 933 F.3d 110 (2d Cir. 2019). Palaniappan concedes that *Eldred* specifically rejected two of the arguments that he presses on appeal, namely, that the Government: (1) procured the NIT Warrant in bad faith; and (2) could not have relied on the NIT Warrant in good faith

because the Warrant did not authorize a search in New York.

See id. at 118–121. Palaniappan accordingly asks us to conclude that Eldred was "wrongly decided." Appellant's Br. 16. But "a panel of this Court is bound by the decisions of prior panels until such time as they are overruled either by an en banc panel of our Court or by the Supreme Court." *Johnson v. United States*, 779 F.3d 125, 128 (2d Cir. 2015) (quotation marks omitted).

Palaniappan's remaining argument on appeal is that the officers who searched his computer "could not have relied on the [NIT Warrant] in good faith because it did not particularly describe the place to be searched." Appellant's Br. 23 (quotation marks omitted). But the remedy of suppression is available only when the warrant is "so facially deficient" that an officer could not "reasonably presume it to be valid." Leon, 468 U.S. at 923.

Here, the NIT Warrant contained "no obvious deficiency," and in fact specified "the place to be searched as all activating computers, defined in relevant part as any user . . . who log[ged] into Playpen." *Eldred*, 933 F.3d at 119 (quotation marks omitted). We therefore reject Palaniappan's argument that the NIT Warrant was insufficiently particularized as to preclude the officers who relied upon it from reasonably presuming its validity.

We have considered Palaniappan's remaining arguments and conclude that they are without merit. For the foregoing reasons, the judgment of the District Court is AFFIRMED.

FOR THE COURT:
Catherine O'Hagan Wolfe, Clerk of Court

[SEAL]

/s/ Catherine O'Hagan Wolfe, Clerk of Court