

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

_____)	
UNITED STATES OF AMERICA)	
)	
V.)	Crim. No. 15-cr-10271-WGY
)	
ALEX LEVIN)	<u>FILED UNDER SEAL</u>
_____)	

DEFENDANT’S MOTION TO SUPPRESS EVIDENCE

The defendant, Alex Levin, moves this Court pursuant to Fed. R. Crim. P. 12(b)(3)(c) to suppress all evidence obtained from the Government’s illegal search of his computer through the deployment of a “Network Investigative Technique,” in violation of 28 U.S.C. § 636(a) and Fed. R. Crim. P. 41. This includes all evidence, including computers and digital images, seized from the defendant on August 12, 2015 pursuant to a search warrant based on information derived from an earlier unlawful search.

STATEMENT OF FACTS

On August 12, 2015, FBI agents executed a search warrant at the home of the defendant, Alex Levin, in Norwood, Massachusetts. The search was conducted pursuant to Search Warrant #15-MJ-2187, issued by Magistrate Judge Marianne B. Bowler of the District of Massachusetts on August 11, 2015. The warrant application was based upon the affidavit of Detective Michael Sullivan of the Boston Police Department, who was a

member of the FBI Child Exploitation Task Force. The search warrant and affidavit are attached hereto as Exhibit 1 (hereinafter "the Residential Warrant").

The affidavit in support of the Residential Warrant primarily relied upon information derived from an investigation into a Website referred to in the affidavit as "Website A." See Exh. 1 at ¶ 9. The affiant described Website A as "a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children." *Id.* Government investigators seized the computer server hosting Website A in North Carolina on February 20, 2015, and brought it to Virginia. *Id.* The FBI assumed administrative control over the website and continued to operate it from a government facility in Virginia.¹ See Application for an Order Authorizing Interception of Electronic Communications, dated February 20, 2015, at ¶ 52 (hereinafter, the "Title III Order")(attached hereto as Exhibit 2). The website was in operation until March 4, 2015. Exh. 1 at ¶ 9. It is apparent

¹ The affidavit in support of the Residential Warrant states only that "[t]he website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time 'Website A' ceased to operate." Exh. 1 at ¶ 9. The affidavit does not mention that it was, in fact, the FBI itself who was operating the website during this thirteen-day period.

that during this time, the FBI was making child pornography available for download to an unknown number of potential users.

Investigators discovered that the website encouraged users to register anonymously using a false email address. *Id.* at ¶ 10-12. After registering, users could then access different sections of the website, including forums and sub-forums relating to sexual exploitation of children. *Id.* at ¶ 13. According to the affidavit in support of the Residential Warrant, a majority of these forums contained images of child pornography and child erotica. *Id.* at ¶ 16. The website also allowed users to upload child pornography and included discussion boards relating to the perpetration of child sexual abuse. *Id.* at ¶ 18, 19.

On February 20, 2015, the same day it seized the server, the government obtained a Title III search warrant (Exhibit 2) from a District Court Judge in the United States District Court for the Eastern District of Virginia. Exh. 1 at ¶ 9; Exh. 2. The order permitted investigators to intercept electronic communications on the site's private chat and messaging services between unknown "target subjects" or "unidentified administrators and users." Exh. 2 at ¶ 3.

Website A utilized network software that concealed users' true Internet Protocol address ("IP address"). Exh. 1 at ¶ 7-8, 21. Specifically, the website operated on an anonymous network

known as "The Onion Router" or "TOR" which prevented law enforcement from obtaining the a user's IP address without the use of a "Network Investigative Technique." ("NIT"). See Affidavit in Support of Application for Search Warrant dated February 20, 2015 at ¶ 7. (hereinafter, the "NIT warrant") (attached as Exhibit 3). Because Website A utilized the TOR network, logs of member activity contained on the seized server could not be used to locate and identify users. Exh 2. at ¶ 39.

Simultaneously with obtaining the Title III order, the Government obtained a search warrant (Exh. 3) authorizing the deployment of a Network Investigative Technique (NIT). This search warrant was issued by a Magistrate Judge of the Eastern District of Virginia. The NIT would "send one or more communications" to Website A's users that would cause the receiving computers to deliver data identifying the computer and its user to the government-controlled server in Virginia. Exh. 1 at ¶ 22; Exh. 2 at ¶ 53. This data included a broad range of information about the user's computer.²

² This data includes the computer's actual IP address; the date and time that the NIT determined what that IP address was; 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 computers; the type of operating system running on the computer (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered; the computer's Host Name; the computer's active operating system username; and the computer's MAC address. Exh. 1 at ¶ 22.

The Government states that during the time it operated Website A, a user of the site named "Manakaralupa" accessed posts on the site that contained links to illegal images. *Id.* at ¶¶ 24, 25, 26. On February 23, 2015, the FBI deployed an NIT to a computer believed to be connected with "Manakaralupa" and extracted its IP address. *Id.* at ¶ 27. The NIT also provided investigators with the host and log-on names for the computer, alleged to be "Alex-PC" and "Alex." *Id.* at ¶ 28. Investigators used this information to issue an administrative subpoena to Verizon for information related to the "Manakaralupa" IP address that had been seized through use of the NIT. *Id.* at ¶ 27, 29. Verizon identified the defendant as the subscriber for the IP address. Exh. 1 at ¶ 29.

Investigators obtained the defendant's home address and applied for a search warrant. *Id.* at ¶ 30-34. The Court issued the Residential Warrant on August 11, 2015. Investigators executed the warrant the next day at his home. Agents arrested him and seized his personal computers and other digital devices which allegedly contain child pornography. The defendant is charged with one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2).

ARGUMENT

The Government's search of the defendant's computer, along with those of individuals across the country, was in violation

of the jurisdictional requirement for searches under Fed. R. Crim. P. 41 and 28 U.S.C. § 636(a). This requirement authorizes a magistrate judge to issue a search warrant *only* for a location within the judicial district itself, with minor exceptions not applicable to the present scenario. This restriction is not a ministerial technicality. Rather, Rule 41 and § 636(a) serve as a critical line of protection against the nationwide searches that occurred in this case. Suppression of the seized evidence is mandated because a search warrant that the magistrate judge was not permitted by rule and statute to issue is "no warrant at all," *United States v. Krueger*, 809 F.3d 1109, 1126 (10th Cir. 2015) (Gorsuch, J., concurring), and is "per se harmful," i.e., prejudicial, to the defendant. *See id.* at 1122.

A. The Warrant Violated Rule 41

The searches of the defendant's home and computer devices on August 12, 2015 were the direct result of the illegal search of his computer—and countless others³—through the use of an NIT. The NIT Warrant issued by a magistrate judge of the Eastern District of Virginia violated the clearly established jurisdictional limits set forth in Fed. R. Crim. P. 41. It allowed government agents to conduct a borderless dragnet search

³ See Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, January 5, 2015, available at: <http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers>.

with no geographic limitation. Rule 41 simply does not permit a magistrate judge in Virginia to authorize the search of the defendant's computer located in Massachusetts.

Rule 41(b) provides a magistrate judge with authority to issue a warrant in five unambiguous circumstances:

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

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

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

(3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant *to install within the district a tracking device*; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, *but within any of the following*:

(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.

(emphasis added). The warrant in this case is not authorized under any of these sections and is therefore plainly unlawful.

1. The Warrant is Not Authorized Under Rule 41(b)(1).

Rule 41(b)(1) allows a magistrate judge to issue a warrant for people or property located within that judge's district. The NIT Warrant inaccurately states that the evidence sought is "located in the Eastern District of Virginia." Attachment A to the NIT Warrant indicates that the computer server, located in Virginia, is the place to be searched. Exh. 3, Attachment A. Yet the server for the "Target Website" was already under FBI control in the district. The actual "place to be searched" was the myriad of "activating computers – wherever located" that would unknowingly download the NIT, thereby forcing the transmission of their internal data back to the FBI in Virginia. See Exh. 3 at ¶ 46. The NIT Warrant authorized these searches even though there was no basis from which to conclude that these computers would be located in the Eastern District of Virginia.

Rule 41(b)(1) cannot be the basis for the search of the defendant's computer in Massachusetts.

Lest there be any doubt about whether it was the defendant's computer that was searched rather than the Virginia server, the Government explained the need for the NIT on the basis that possession of the server alone would not allow the Government to identify the site's users. Exh. 2 at ¶ 58. In order to do so, it was necessary to deploy the NIT so that the defendant's computer would download the NIT and allow the Government to seize this information in Massachusetts before sending it to Virginia. Thus, although the NIT was first deployed from the server in Virginia, it is clear that the actual search occurred when the NIT was installed on the defendant's computer and extracted its data. This situation is no different from agents claiming that a search took place in Virginia because they traveled to Massachusetts, copied data from a computer, and returned to Virginia before examining the contents. The fact that the Government is now capable of seizing data on a computer without physically traveling to its location does not alter this analysis.

In a similar case, *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. 2016), the court found the argument that the crimes were committed "'within' the location of Website A, Eastern District of Virginia, rather than on the personal computers

located in other places under circumstances where users may have deliberately concealed their locations" to be "unpersuasive." 2016 WL 337263 at *6. As is the case here, "because the object of the search and seizure was [the defendant's] computer, not located in the Eastern District of Virginia, this argument fails." *Id.*

The Court reached a similar conclusion in denying an application to issue a search warrant in *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) ("*In re Warrant*"). There, the location of the target computer was unknown but the Government relied on Rule 41(b)(1) by reasoning that the "information obtained from the Target Computer will first be examined in this judicial district." *Id.* at 756. In rejecting the application, the court explained that the search and seizure of data occurs "not in the airy nothing of cyberspace, but in physical space with a local habitation and a name." *Id.* The same is true here. The NIT search did not occur in Eastern Virginia or in cyberspace. It was a physical search of the defendant's computer located in Massachusetts.

2. The Warrant is Not Authorized Under Any of the Other Subsections of Rule 41(b).

The other subsections of Rule 41(b) are inapplicable to this case.

Rule 41(b)(2)—which allows an extraterritorial search or seizure of moveable property if it is located within the district when the warrant is issued but might move or be moved before the warrant is executed—fails to provide authorization because the defendant’s computer was never physically within the Eastern District of Virginia. See *Michaud*, 2016 WL 337263 at *6 (finding “unconvincing” the argument that Rule 41(b)(2) applies “given the interconnected nature of communications between Website A and those who accessed it.”). Importantly, the court in *In re Warrant* noted:

That (b)(2) does not authorize a warrant in the converse situation—that is, for property outside the district when the warrant is issued, but brought back inside the district before the warrant is executed. A moment’s reflection reveals why this is so. If such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found.

958 F. Supp. 2d at 757.

Rule 41(b)(3) cannot serve as a basis because this case does not involve terrorism.

Rule 41(b)(4) allows for tracking devices to be installed within the issuing district on an object that may travel to outside the district. The NIT here was installed on the defendant’s computer in Massachusetts, which was never physically located within the Eastern District of Virginia. See *Michaud*, 2016 WL 337263 at *6. Even if the installation were

deemed to have occurred on the server in Virginia, section (b)(4) is inapplicable because the defendant "never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district." *See id.*

Rule 41(b)(5) does not apply because the defendant's computer was not located within any of the specified areas covered by this subsection.

3. The Warrant Also Violated 28 U.S.C. § 636(a).

The search warrant issued by the magistrate judge in the Eastern District of Virginia also was in violation of the Federal Magistrates Act. *See Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring) (emphasizing that a violation of Rule 41(b)'s territorial limitations also implicates a statutory limitation). Section 636(a) provides three geographic areas in which a magistrate judge's powers are effective, none of which applies here. *See id.*⁴ Thus, the NIT Warrant not only violated Rule 41, but also Section 636(a) of the Federal Magistrates Act.

⁴"Each United States Magistrate judge ... shall have [1] within the district in which sessions are held by the [district] court that appointed the magistrate judge, [2] at other places where that [district] court may function, and [3] elsewhere as authorized by law ... all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure. . . ." *Id.*

B. The Violation of Rule 41 Requires Suppression.

Suppression is required because the Rule 41 violation also implicates Section 636(a). See 28 U.S.C. 636(a). The issuing magistrate judge lacked statutory authority to issue the NIT warrant in the first place. See *Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring). Importantly, "Section 636(a)'s territorial restrictions are *jurisdictional* limitations on the power of magistrate judges and the Supreme Court has long taught that the violation of a statutory jurisdictional limitation—quite unlike the violation of a more prosaic rule or statute—is *per se* harmful." *Id.* at 1122 (emphasis in original).

Our whole legal system is predicated on the notion that good borders make for good government, that dividing government into separate pieces bounded both in their powers and geographic reach is of irreplaceable value when it comes to securing the liberty of the people.

Id. at 1125, citing *Bond v. United States*, 564 U.S. 211 (2011); The Federalist Nos. 28, 32 (Alexander Hamilton), Nos. 46, 51 (James Madison).

The magistrate judge was never authorized to issue the NIT warrant and therefore its use constitutes Government hacking of the defendant's computer. Indeed, "a warrant issued in defiance of positive law's jurisdictional limitations on a magistrate judge's powers . . . for Fourth Amendment purposes. . . . is no warrant at all." See *Krueger*, 809 F.3d at 1126 (Gorsuch, J., concurring). This violation of a jurisdictional statute mandates

suppression to preserve judicial integrity and proper separation of powers under the United States Constitution. See *id.* at 1123 (noting that § 636 is entitled "Jurisdiction, powers, and temporary assignment").

Moreover, violations of Rule 41 require suppression when a defendant is prejudiced by the lack of compliance. See *United States v. Bonner*, 808 F.2d 864, 869 (1st Cir. 1986). "Prejudice means being 'subjected to a search that might not have occurred or would not have been so abrasive' had the rules been followed." *United States v. Burgos-Montes*, 786 F.3d 92, 109 (1st Cir. 2015), quoting *Bonner*, 808 F.2d at 869.

In the instant case, the defendant was prejudiced because the search authorized by the Residential Warrant would never have occurred but for information derived from the improperly issued NIT Warrant. Investigators discovered the defendant's alleged IP address through the use of the NIT. See Exh. 1 at ¶ 27. They then used this information to obtain the subscriber information for the IP address from Verizon, which ultimately led them to obtain the Residential Warrant. *Id.* at ¶ 29. The sole reason that investigators were able to identify the defendant as a suspect is because they had already used the NIT Warrant to search his computer and obtain his IP address. Thus, if not for the NIT Warrant, there would have been no probable cause to support the Residential Warrant. Exh. 2 at ¶ 58

("deployment of a NIT to attempt to identify actual IP addresses used by TARGET SUBJECTS . . . is *the only available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the identity of the TARGET SUBJECTS.*") (emphasis added). The search of the defendant's property conducted on August 12, 2015 would therefore never have occurred.

The unrestrained expansion of judicial authority to issue search warrants without geographic limitation is not a mere technicality. This violation of Rule 41(b) is not the type of "ministerial" violation for which courts have declined to require suppression. *See e.g., United States v. Dauphinee*, 538 F.2d 1, 3 (1st Cir. 1976) (steps required by Rule 41(d) are basically ministerial). The Court exceeded its authority by issuing a warrant for property located outside of its jurisdiction.

The Court of Appeals for the District of Columbia considered a similar issue in *United States v. Glover*, 736 F.3d 509, 510-516 (D.C. Cir. 2014) where it suppressed the fruits of a Title III wiretap because the court had authorized the installation of a listening device outside of the District. The Court held that Rule 41(b), which partially implements Title III, is "crystal clear" and that "a jurisdictional flaw in the warrant" cannot be excused as a "technical defect." *Id.* at 515.

The same logic applies with even greater force here. The agents in *Glover* could have simply obtained the warrant from a magistrate judge in Maryland or Virginia whereas in this case there is no magistrate judge with authority to issue the nationwide warrant.

Moreover, the court in *Glover* found a "blatant disregard of a district judge's jurisdictional limitation" where the warrant expressly authorized agents to enter the vehicle regardless of whether it was located in D.C., Maryland, or Virginia. 736 F.3d at 510, 515. In the instant case, the Government failed to comply with the Fourth Amendment's particularity requirements. *U.S. Const. Amend. IV* ("no warrants shall issue, but upon probable cause, . . . and particularly describing the place to be searched. . ."). The "manifest purpose of the particularity requirement of the Fourth Amendment is to prevent wide-ranging general searches by the police." *Bonner*, 808 F.2d at 866. Had the government particularly described the place to be searched, i.e., a computer in Massachusetts, no warrant could have issued. Instead, the search warrant erroneously described the place to be searched as the server, located in Virginia. See Exh. 3 Attachment A. Similarly, it described the information to be seized as data from the activating computers while overlooking the fact that such information could only be obtained by first

searching and seizing the data from those computers. See Exh. 3 Attachment B.

"The test for determining the adequacy of the description of the location to be searched is whether . . . 'there is any reasonable probability that another premise might be mistakenly searched.'" *Bonner*, 808 F.2d at 866. Because the magistrate in Virginia could not authorize a search of a computer in Massachusetts, its occurrence demonstrates that the description was insufficient to prevent a reasonable probability of mistake. The fact that countless other computers were also searched only bolsters this conclusion. When it comes to a constitutional concern such as the particularity requirement, the Government cannot be rewarded for vagueness. To do so would invite further violations and undermine the core requirement set forth in the Fourth Amendment. See *In re Warrant*, 958 F. Supp. 2d at 758 ("This particularity requirement arose out of the Founders' experience with abusive general warrants").

Finally, the officers acted in intentional and deliberate disregard of Rule 41. Even where no prejudice occurs, suppression is appropriate where the government was not acting in good faith. See *United States v. Leon*, 468 U.S. 897, 922 (1984); *Krawiec*, 627 F.2d at 582; *Dauphinee*, 538 F.2d at 3. Particularly where the Government moved Website A's server from North Carolina to Virginia, there can be no credible argument

that officers reasonably believed that none of the 214,898 members of Website A were located outside of Virginia. See Exh. 3 Attachment A ("The activating computers are those of *any user or administrator* who logs into the TARGET WEBSITE.") (emphasis added); Exh. 2 at ¶ 71 ("It is not presently known with any certainty where any of the remaining TARGET SUBJECTS reside.").

It is evident from the plain language of Rule 41(b) that no interpretation would allow the search of potentially thousands of computers located outside the authorizing district. In *In re Warrant*, the court stated that where the location of the Target Computer is unknown, "the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)." 958 F. Supp. 2d at 757. It is unlikely that the Government was unaware of this opinion when it filed its application.

In any event, the Government was clearly aware that the NIT Warrant was not authorized when it made its application in February, 2015. A memorandum addressed to the Committee on Rule of Practice and Procedure dated May 5, 2014, introduces a proposed amendment to Rule 41(b) that would authorize the use of the NIT Warrant. See Reena Raggi, *Report of the Advisory Committee on Criminal Rules*, May 5, 2014, at 319.⁵ Specifically, proposed Rule 41(b)(6) "would authorize a court to issue a

⁵ Available at: <http://www.fpd-ohn.org/sites/default/files/Preliminary%20Draft%20of%20Proposed%20Fed%20Rule%20Amendments%2015Aug2014.pdf>.

warrant to use remote access to search electronic storage media and seize electronically stored information inside or outside of the district: (1) when a suspect has used technology to conceal the location of the media to be searched." Rebecca A.

Womeldorft, *Transmittal of Proposed Amendments to the Federal Rules*, Oct. 9, 2015, at 8.⁶ Where the memorandum introducing the proposal states that the change "had its origins in a letter from Acting Assistant Attorney General Mythili Raman," it is not feasible that the Government was unaware that such searches were not authorized under Rule 41(b). See *Report of the Advisory Committee on Criminal Rules*, at 324. Perhaps most telling, the memorandum states that the reason for the proposal is that the territorial venue provisions create "special difficulties" for the Government when investigating crimes involving electronic information. *Id.* at 325 (explaining that "a warrant for a remote access search when a computer's location is not known would enable investigators to send an email, remotely install software on the device receiving the email, and determine the true IP address or identifying information for that device."). The fact that the proposal requires an entirely new subsection to Rule 41(b), rather than a clarification to an existing subsection, demonstrates that there is no reasonable interpretation of any provision in Rule 41(b) that would permit such a search.

⁶ Available at: <http://www.uscourts.gov/file/18641/download>.

Rule 41(b) provides explicit geographic limits on the magistrate judge's authority to issue search warrants and, under the circumstances presented here, precluded her from issuing a warrant authorizing the search of property outside the district. The rule is clear. It is not for this Court to rewrite it to keep up with new technological developments. It is for the United States Congress⁷ to address any shortcomings in the Rule. Until that occurs, searches like the one in this case violate Rule 41(b) and must result in suppression.

CONCLUSION

WHEREFORE, the defendant moves that the Court suppress all evidence obtained as a result of the search and seizure authorized by Search Warrant #15-MJ-2187.

ALEX LEVIN
By his attorneys,
CARNEY & ASSOCIATES

J. W. Carney, Jr.

J. W. Carney, Jr.
B.B.O. # 074760

Nathaniel Dolcort-Silver
B.B.O. # 693968
20 Park Plaza, Suite 1405
Boston, MA 02116
617-933-0350
jcarney@CARNEYdefense.com

⁷See generally *Krueger*, 809 F.3d at 1119-21 (Gorsuch, J., concurring)(need for Congressional approval).

February 18, 2016

Certificate of Service

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on or before the above date.

J. W. Carney, Jr.

J. W. Carney, Jr.

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

_____)	
UNITED STATES OF AMERICA)	
)	
V.)	Crim. No. 15-cr-10271-WGY
)	
ALEX LEVIN)	
_____)	

AFFIDAVIT SUPPORTING
DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

I, J. W. Carney, Jr., state that the facts contained in the attached motion are true to the best of my information and belief.

Signed under the penalties of perjury.

J. W. Carney, Jr.
J. W. Carney, Jr.

February 18, 2016

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Massachusetts

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

The Residence at 64 Plymouth Drive, Apartment C,
Norwood, Massachusetts, as More Fully Described in
Attachment A, Which is Incorporated by Reference

Case No. 15-MJ-2187-MBB

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):

The Residence at 64 Plymouth Drive, Apartment C, Norwood, Massachusetts, as More Fully Described in Attachment
A, Which is Incorporated by Reference

located in the District of Massachusetts, there is now concealed (identify the
person or describe the property to be seized):

See Attachment B, which is incorporated by reference, for a list property to be seized.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- checked evidence of a crime;
checked contraband, fruits of crime, or other items illegally possessed;
checked property designed for use, intended for use, or used in committing a crime;
unchecked a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

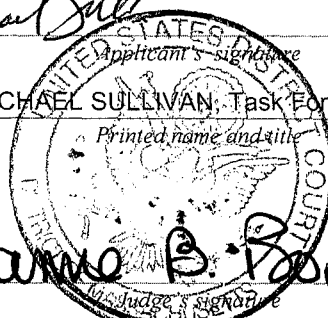
Table with 2 columns: Code Section, Offense Description. Row 1: 8 U.S.C. § 2252A(a)(2)(A) and (b)(1), receipt of child pornography. Row 2: 18 U.S.C. § 2252A(a)(5)(B), possession of child pornography.

The application is based on these facts:

See the attached Affidavit of Federal Bureau of Investigation Task Force Officer Michael Sullivan, which is
incorporated by reference.

- checked Continued on the attached sheet.
unchecked Delayed notice of days (give exact ending date if more than 30 days:) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Handwritten signature of Michael Sullivan
MICHAEL SULLIVAN, Task Force Officer
Printed name and title



Sworn to before me and signed in my presence.

Date: 08/11/2015

Handwritten signature of Marianne B. Bowler, U.S. Magistrate Judge

City and state: Boston, Massachusetts

HON. MARIANNE B. BOWLER, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

INTRODUCTION

I, Michael Sullivan, having been first duly sworn, do hereby depose and state as follows:

1. I am employed as a Detective with the City of Boston (Massachusetts) Police Department. I am also a sworn Special Deputy United States Marshal. I have been employed by the Boston Police Department approximately the past nine years and am currently assigned as a Task Force Officer to the FBI Boston Division, Child Exploitation Task Force. While employed by the Boston Police Department, I have investigated state and federal criminal violations related to, among other things, the on-line 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.
2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of or access with intent to view child pornography), are located within 64 Plymouth Drive, Apartment C, in Norwood Massachusetts (hereinafter the "SUBJECT PREMISES"). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachment A, incorporated herein by reference. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

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, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Detective with the Boston Police Department. Because this affidavit is submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

4. A user of the Internet account at the Subject Premises has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as “Website A.”¹ There is probable cause to believe that a user of the Internet account at the Subject Premises knowingly received and distributed child pornography on “Website A.”

¹ The actual name of “Website A” is known to law enforcement. Disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members 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 and the website will be identified as “Website A.”

The Network²

5. “Website A” operated on a network (“the Network”) available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user’s existing web browser, downloading free software available from the Network’s administrators, or downloading a publicly-available third-party application.³ Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user’s physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

6. Websites that are accessible only to users within the Network can be set up within the Network and “Website A” was one such website. Accordingly, “Website A” could not generally be accessed through the traditional Internet.⁴ Only a user who had installed the appropriate software on the user’s computer could access “Website A.” Even after connecting to the Network, however, a user had to know the exact web address of “Website A” in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike

² The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members 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 and the network will be identified as “the Network.”

³ Users may also access the Network through so-called “gateways” on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

⁴ Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact

on the traditional Internet, a user could not simply perform a Google search for the name of “Website A,” obtain the web address for “Website A,” and click on a link to navigate to “Website A.” Rather, a user had to have obtained the web address for “Website A” directly from another source, such as other users of “Website A,” or from online postings describing both the sort of content available on “Website A” and its location. Accessing “Website A” therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon “Website A” without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

7. The Network’s 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.

8. The Network 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 Network itself, entire websites can be set up which 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 Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

IP address of the computer server that hosted Website A, which information was not publicly available. As of on or

Description of "Website A" and its Content

9. "Website A" was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting "Website A" was seized from a web-hosting facility in Lenoir, North Carolina. The website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time "Website A" ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of "Website A." Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A," which are described below.

10. According to statistics posted on the site, "Website A" contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent girls 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 "Website A;" and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two

about February 20, 2015, Website A was no longer accessible through the traditional Internet.

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 "[Website A]." 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."

11. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user "[F]or your security you should not post information here that can be used to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.

12. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.

13. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and

experience, I know that “jailbait” refers to underage but post-pubescent minors; the abbreviation “HC” means hardcore (i.e., depictions of penetrative sexually explicit conduct); and “scat” refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a 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.

14. 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 of a particular topic included the date and time of the most recent posting to that thread 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 in 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.

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

16. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. Examples of these are as follows:

(a) On February 3, 2015, a user posted a topic entitled “Buratino-06” in the forum “Pre-

teen – Videos - Girls HC” that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these images depicted the girl being orally penetrated by the penis of a naked male;

(b) On January 30, 2015, a user posted a topic entitled “Sammy” in the forum “Pre-teen – Photos – Girls” that contained hundreds of images depicting child pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis of a male; and

(c) On September 16, 2014, a user posted a topic entitled “9yo Niece - Horse.mpg” in the “Pre-teen Videos - Girls HC” forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. 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.

17. 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. In total, “Website A” contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

18. “Website A” also included a feature referred to as “[Website A] Image Hosting.” This feature of “Website A” allowed users of “Website A” to upload links to images of child pornography

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

19. Text sections of "Website A" provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse.

- a. On January 8, 2015, a user posted a topic entitled "should i proceed?" in the forum "Stories - Non-Fiction" that contained a detailed accounting of an alleged encounter between the user and a 5 year old girl. The user wrote "...it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms..." The user ended his post with the question, "should I try to proceed?" and further stated that the girl "seemed really interested and was smiling a lot when she felt my cock." A different user replied to the post and stated, "...let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful..."

Court Authorized Use of Network Investigative Technique

20. Websites generally have Internet Protocol ("IP") address logs that can be used to locate and identify the site's users. In such cases, after the seizure of a website whose users were engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of "Website A" to access the site. A publicly available lookup could then be

performed to determine what Internet Service Provider (“ISP”) owned the target IP address. A subpoena could then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.

21. However, because of the Network software utilized by “Website A,” any such logs of user activity would contain only the IP addresses of the last computer through which the communications of “Website A” users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Network to that actual user. Such IP address logs therefore could not be used to locate and identify users of “Website A.”

22. Accordingly, on February 20, 2015, the same date “Website A” was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique (“NIT”) on “Website A” in an attempt to identify the actual IP addresses and other identifying information of computers used to access “Website A.” Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into “Website A” by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user’s computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information about the computer, and the user of the computer accessing “Website A.” That data included: the computer’s actual IP address, and the date and time that the NIT determined what that IP address was; 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 computers; 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); information about whether the NIT had already been delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

"Manakaralupa" on "Website A"

23. According to data obtained from logs on "Website A," monitoring by law enforcement and the deployment of a NIT, a user with the user name "Manakaralupa" engaged in the following activity on "Website A."

24. The profile page of user "Manakaralupa" indicated this user originally registered an account on "Website A" on February 10, 2015. Profile information on "Website A" may include contact information and other information that is supplied by the user. It also contains information about that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts. According to the user "Manakaralupa's" profile, this user was a normal member of "Website A." Further, according to the statistics section of this user's profile, the user "Manakaralupa" had been actively logged into the website for a total of 2 hours, 19 minutes and 35 seconds between the dates of February 10, 2015 and March 4, 2015. In addition the user added the personal text of "watch out Playpen newbie here".

25. On March 4, 2015, the user "Manakaralupa" with IP address 108.20.181.106 accessed a forum entitled, "Strawberry Shortcake Reuped on 03/04/2015". Among other things, this post contained a link to an image (.jpg file) of a picture collage that depicted a pre-pubescent female, about five to seven years old, posed in a variety of poses that the focal point of the picture was the child's vagina, anus, and one that had a penis placed against her mouth.

26. On March 4, 2015, "Manakaralupa" accessed a file entitled "Estefy (Latina Anal) Deep anal creampie - asi se mama linda.3gp". The file contained 1 image that contained a collage of images of a prepubescent female performing oral sex and anal sex with an adult male.

IP Address and Identification of User "Manakaralupa" on "Website A"

27. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on February 23, 2015, the user "Manakaralupa" accessed "Website A" from IP address 108.20.181.106.

28. Using publicly available websites, FBI Special Agents were able to determine that the above IP Address was operated by the Internet Service Provider ("ISP") Verizon. Deployment of the NIT also allowed the FBI to gather identifying information on the user's computer. The information for "Manakaralupa" computer included host and log on names, "Alex-PC" and "Alex."

29. In March 2015, the FBI served an administrative subpoena to Verizon requesting information related to the user who was assigned IP address 108.20.181.106 as of February 23, 2015. According to the information received from Verizon, the subscriber, Alex Levin, is receiving Internet service at the address of the SUBJECT PREMISES with an account creation date of November 14, 2011.

30. The FBI conducted a database search of public records for the SUBJECT PREMISES, 64 Plymouth Drive, Apartment C, in Norwood, Massachusetts. The search listed Alex Levin, DOB 07/01/1961 as a resident of 64 Plymouth Drive, Apartment C, in Norwood, Massachusetts. A check of the MA Registry of Motor Vehicles ("RMV") showed Alex Levin listed at 64 Plymouth Drive, Apartment C, Norwood, Massachusetts as a mailing address and did not report any home address.

31. On or about August 10, 2015 representatives of the United States Postal Inspection Service (USPIS) reported that Alex Levin is only person known to them currently receiving mail

at 64 Plymouth Drive, Apartment C (Suite C), Norwood, Massachusetts.

32. On July 14, 2015, I observed a mailbox in the front lobby of 64 Plymouth Drive that was labeled "LEVIN" and "C".

33. On July 14, 2015, I observed a black Jeep Wrangler, MA registration 9270CF, parked in the parking lot behind SUBJECT PREMISES. A check with the MA RMV showed the vehicle as registered to Alex Levin.

34. On August 5, 2015, I conducted a search of the available wireless networks in the area of the SUBJECT PREMISES which showed the following:

<u>Network</u>	<u>Status</u>
97RH5	Locked
belin.0da	Locked
Cisco68290	Locked
HOME-57C6-2.4	Locked
HOME-57C6-5	Locked
HP-Print-16-Officej...	Locked
WIN-6KQ3080VBN...	Locked
xfinitywifi	Unlocked
XKMHJ	Locked
YY5F9	Locked
ZUCG5	Locked

Based upon my training and experience, I know that xfinitywifi, the only wireless network in the area of the SUBJECT PREMISES, as of August 5, 2015, that showed an unlocked status, is an xfinity hotspot that is available to users of Comcast and not Verizon, the ISP that operates the subject IP address.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT
TO VIEW AND POSSESS, COLLECT, RECEIVE, OR DISTRIBUTE CHILD
PORNOGRAPHY**

35. Based on my previous investigative experience related to child pornography investigations,

and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web based bulletin boards to access with intent to view and possess, collect, receive or distribute images of child pornography:

a. Individuals who access with intent to view and possess, collect, receive or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who access with intent to view and possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who access with intent to view and possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and

videotapes for many years.

d. Likewise, individuals who access with intent to view and possess, collect, receive or distribute child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals who access with intent to view and possess, collect, receive or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, Internet Relay Chat or chat rooms, have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who access with intent to view and possess, collect, receive or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the

investigation of child pornography throughout the world.

34. Based upon the foregoing, I believe that a user of the Internet account at SUBJECT PREMISES likely displays characteristics common to individuals who access with the intent to view and possess, collect, receive, or distribute child pornography.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

35. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

36. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

37. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically

changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

38. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

39. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

40. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online

storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

41. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

42. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment.

This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to

examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

43. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

44. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

45. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;
- b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;
- c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth

herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- e. surveying various file directories and the individual files they contain;
- f. opening files in order to determine their contents;
- g. scanning storage areas;
- h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and
- i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

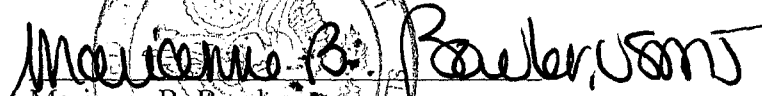
CONCLUSION

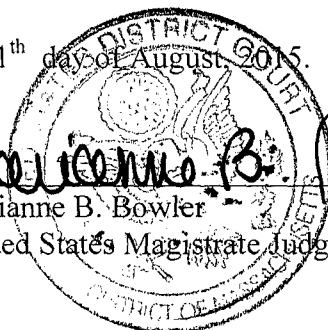
46. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this

Court issue a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.



Task Force Officer Michael Sullivan
Federal Bureau of Investigation

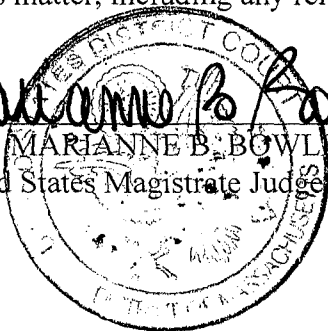
Sworn and subscribed to before me this 11th day of August, 2015.


Marianne B. Bowler
United States Magistrate Judge



I have reviewed the images referenced in paragraphs 25 and 26 above, and I find probable cause to believe that the images constitute child pornography. The Affiant shall continue to preserve the image files and screen capture images provided to the Court, for the duration of the pendency of this matter, including any relevant appeal process.

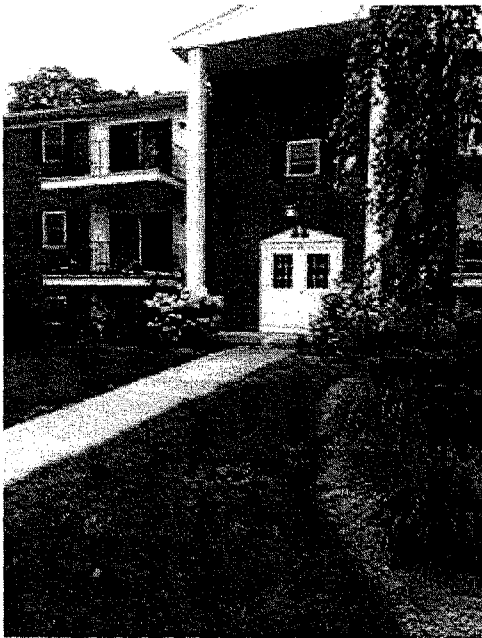

HON. MARIANNE B. BOWLER
United States Magistrate Judge



ATTACHMENT A

DESCRIPTION OF THE LOCATION TO BE SEARCHED

The SUBJECT PREMISES is located at 64 Plymouth Drive, Apartment C, Norwood, Massachusetts. The location 64 Plymouth Drive is a three story brick apartment building with white trim with a white front door and the number "64" clearly displayed above the door. The rear door of 64 Plymouth Drive is also clearly marked with the number "64." Apartment C is located on the ground level and most easily accessed by entering through the rear door down a series of stairs. At the bottom of these stairs, Apartment C is the first door on the left. The front door to Apartment C is blue and engraved on the door knocker is the letter "C."



ATTACHMENT B

Information to be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - m. contextual information necessary to understand the evidence described in this attachment.
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
 - 4. Child pornography and child erotica.
 - 5. Records, information, and items relating to violations of the statutes described above including
 - a. Records, information, and items relating to the occupancy or ownership of 64 Plymouth Drive, Apartment C, Norwood, Massachusetts including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes; and
 - b. Records and information relating to sexual exploitation of children, including correspondence and communications between users of "Website A."

As used above, the terms "records" and "information" includes all forms of creation or

storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

FILED

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

2015 FEB 20 A 8:39

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING THE
INTERCEPTION OF ELECTRONIC
COMMUNICATIONS

CASE NO. 15-10271-1
CLERK U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA
UNDER SEAL

APPLICATION FOR AN ORDER AUTHORIZING INTERCEPTION OF
ELECTRONIC COMMUNICATIONS

The United States of America, by and through Assistant United States Attorney Whitney Dougherty Russell and Trial Attorney Michael Grant (hereinafter "the prosecutors"), hereby applies to the Court pursuant to Section 2518 of Title 18, United States Code, for an Order authorizing the interception of electronic communications. In support of this application, counsel states the following:

1. The prosecutors are investigative or law enforcement officers of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, attorneys authorized by law to prosecute or participate in the prosecution of offenses enumerated in Section 2516(1)(c) of Title 18, United States Code.

2. A copy of the memorandum of an official specially designated by the Attorney General of the United States authorizing this application is attached to this application as Exhibit A.

3. This application is for an order pursuant to Section 2518 of Title 18, United States Code, authorizing the interception of electronic communications of Steven W. Chase, and other unidentified administrators and users ("TARGET SUBJECTS") of the child pornography website upf45jv3bziuctml.onion ("TARGET WEBSITE") occurring

over the private message function ("TARGET FACILITY 1") and private chat function ("TARGET FACILITY 2"), of the TARGET WEBSITE, concerning offenses enumerated in Section 2516 of Title 18, United States Code.

4. The prosecutors have discussed the circumstances of the above offenses with Special Agent Caliope Bletsis of the Federal Bureau of Investigation, who has participated in the conduct of this investigation, and have examined the affidavit of Special Agent Bletsis, which is attached as Exhibit B to this application and is incorporated herein by reference. Based upon that affidavit, your applicants state upon information and belief that:

a. there is probable cause to believe that the TARGET SUBJECTS have committed, are committing, and will continue to commit violations of the following offenses:

- i. 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise;
- ii. 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography;
- iii. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution and Conspiracy to Receive and Distribute Child Pornography;
- iv. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography; and

b. there is probable cause that the TARGET SUBJECTS, during the period of interception authorized by this Order, will use TARGET FACILITY 1 and TARGET FACILITY 2 (together referred to as the "TARGET FACILITIES"), in furtherance of the offenses described above;

c. There is probable cause to believe that the interception of electronic

communications of the TARGET SUBJECTS over the TARGET FACILITIES will reveal: (1) the nature, extent and methods of operation of the TARGET SUBJECTS' unlawful activities; (2) the identity of the TARGET SUBJECTS and their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities, or information that may be useful in establishing the identity of their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (3) the advertising, receipt, and distribution of child pornography related to those activities; (4) the existence and locations of records relating to those activities; and (5) the location and identity of computers used to further the target offenses; in addition, these electronic communications are expected to constitute admissible evidence of the commission of the above-described offenses. It is expected that monitoring of the electronic communications of the TARGET SUBJECTS over the TARGET FACILITIES, if authorized, will provide valuable evidence against the TARGET SUBJECTS and others currently unknown to law enforcement involved in illegal activities that cannot reasonably be obtained by other means; and

d. It has been established as detailed in the attached Affidavit that normal investigative procedures have been tried and have failed, reasonably appear unlikely to succeed if tried, or are too dangerous to employ.

5. There are no previous applications which are known to have been made to any judge of competent jurisdiction for approval of the interception of the oral, wire or electronic communications of any of the same individuals, facilities, or premises specified in this Application, except as set forth in the affidavit.

6. This Court has territorial jurisdiction to issue the requested order under 18 U.S.C. § 2518(3) because the computer server intercepting all communications and on which the TARGET WEBSITE, including the TARGET FACILITIES, are located will be in Newington, VA, in the Eastern District of Virginia during the period of interception.

WHEREFORE, there is probable cause to believe that the TARGET SUBJECTS are engaged in the commission of offenses involving violations of Title 18, United States Code, Sections 2251 and 2252A, and that during the period of interception applied for herein, the TARGET SUBJECTS will use the TARGET FACILITIES to communicate with each other and with others as yet unknown, in connection with the commission of the above-described offenses. The prosecutors also believe that, if the interception herein applied for is authorized by this Court, electronic communications of the TARGET SUBJECTS concerning those offenses will be intercepted.

7. On the basis of the allegations contained in this application, which in turn is based on the attached affidavit of Special Agent Bletsis:

IT IS HEREBY REQUESTED that this Court issue an order pursuant to the power conferred upon it by Section 2518 of Title 18, United States Code, authorizing FBI and/or individuals employed by or operating under a contract with the government and acting under the supervision of the FBI, to intercept electronic communications of the TARGET SUBJECTS, occurring over the TARGET FACILITIES, until such electronic communications are intercepted that fully reveal: (1) the nature, extent and methods of operation of the TARGET SUBJECTS' unlawful activities; (2) the identity of the TARGET SUBJECTS and their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities, or information that may be useful in establishing

the identity of their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (3) the receipt and distribution of child pornography related to those activities; (4) the existence and locations of records relating to those activities; (5) the location and identity of computers used to further the target offenses; and (6) admissible evidence of the commission of the above-described offenses - or for a period of thirty (30) days, to be measured from the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the Order or 10 days after the Order is entered, whichever is earlier from the date of this authorization.

IT IS FURTHER REQUESTED that this Court direct that its Order be executed as soon as practicable after it is signed and that all monitoring of electronic communications shall be conducted in accordance with Chapter 119 of Title 18, United States Code, as outlined in Agent Bletsis's affidavit. That is, the computer server intercepting all communications and on which the TARGET FACILITIES are located will be in Newington, VA, in the Eastern District of Virginia during the period of interception. A copy of intercepted communications will be sent to a facility in Linthicum, MD, where certain FBI personnel will be stationed while the TARGET WEBSITE remains operating. Each private message and private chat will be reviewed over a secure system, and based on the identities of the sender and recipient and the content of the private message or private chat, monitoring personnel will determine as soon as practicable after interception whether the private message or private chat appears to be relevant to the investigation or otherwise criminal in nature. If the private message or private chat is not criminal in nature, the private message or private chat will be marked "minimized" and not accessed

by other members of the investigative team. If the private message or private chat appears to be privileged, it will be marked "privileged" and secured from access by other members of the investigative team. If a private message or private chat appears to be relevant to the investigation or otherwise criminal in nature, it will be marked "non-minimized" and may be shared with the other agents and monitors involved in the investigation. If a private message or private chat is marked "minimized" or "privileged," it will not be disseminated to members of the investigative team. All intercepted private messages and private chats will be sealed with the court upon the expiration of the court's order authorizing the interception. It is anticipated that the monitoring location will be staffed at all times, at which time intercepted communications will be monitored and read. The monitoring location will be kept secured with access limited to only authorized monitoring personnel and their supervising agents.

IT IS FURTHER REQUESTED that the prosecutors or any other Assistant United States Attorney or Department of Justice Trial Attorney familiar with the facts of this case, shall cause to be provided to the Court a report on or about the fifteenth and thirtieth day following the date of the Order or the date interception begins, whichever is later, showing the progress that has been made toward achievement of the authorized objectives and the need for continued interception, although if the Order is renewed for a further period of interception, the application for renewal may serve as the report on or about the thirtieth day. If any of the above-ordered reports should become due on a weekend or holiday, such report shall become due on the next business day thereafter.

IT IS FURTHER REQUESTED that the Court direct that the Court's Order, as well as the supporting Application, Affidavit (along with its attachments), proposed

Orders, and all interim reports filed with the Court, be sealed until further order of this Court, except that copies of the Order, in full or redacted form, may be served on FBI agents as necessary to effectuate the Court's Order. Moreover, the Government hereby requests authorization to disclose the existence of the Interception Order and the contents of pertinent collected electronic communications, pursuant to Title 18, United States Code, Sections 2517(2) and (3), as appropriate for the purposes of providing relevant facts to a Court in support of any complaints, arrest warrants or search warrants. In addition, the Government requests authorization to disclose facts, pursuant to Title 18, United States Code, Sections 2517(2) and (3), as necessary to provide relevant testimony at any preliminary hearings, detention hearings, grand jury proceedings and other proceedings pertaining to the TARGET SUBJECTS and others as yet unknown. The Government also requests authorization to disclose facts to foreign investigative or law enforcement officers, pursuant to Title 18, United States Code, Section 2517(7), as necessary to the proper performance of the official duties of the officer making or receiving such disclosure, and that foreign investigative or law enforcement officers may use or disclose such facts or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

IT IS FURTHER REQUESTED that no inventory or return of the results of the foregoing interception need be made, other than the above required reports, before 90 days from the date of the expiration of the Order, or any extension of the Order, or at such time as the Court in its discretion may require.

IT IS FURTHER REQUESTED that, upon an ex parte showing of good cause to a judge of competent jurisdiction, the service of the above inventory or return may be

postponed for a further reasonable period of time.

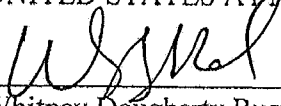
I declare under penalty of perjury that the foregoing is true and correct.

EXECUTED in Alexandria, Virginia, on February 20, 2015.

Respectfully submitted,

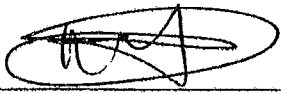
DANA J. BOENTE
UNITED STATES ATTORNEY

By:


Whitney Dougherty Russell
Assistant United States Attorney

DAMON KING
ACTING CHIEF
Child Exploitation and Obscenity Section
Criminal Division
U.S. Department of Justice

By:


Michael Grant
Trial Attorney

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

ALEXANDRIA DIVISION

IN THE MATTER OF THE APPLICATION	:	
OF THE UNITED STATES OF AMERICA	:	CASE NO. 1:15-ES-4
FOR AN ORDER AUTHORIZING THE	:	
INTERCEPTION OF ELECTRONIC	:	UNDER SEAL
COMMUNICATIONS	:	

EXHIBIT A



Office of the Attorney General
Washington, D.C.

ORDER NO. 3055-2009

SPECIAL DESIGNATION OF CERTAIN OFFICIALS OF THE CRIMINAL DIVISION AND
NATIONAL SECURITY DIVISION TO AUTHORIZE APPLICATIONS FOR COURT
ORDERS FOR INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS

By virtue of the authority vested in me as the Attorney General, including 28 U.S.C. § 510, 5 U.S.C. § 301, and 18 U.S.C. § 2516(1), and in order to preclude any contention that the designations by the prior Attorney General have lapsed, the following officials are hereby specially designated to exercise the power conferred by section 2516(1) of title 18, United States Code, to authorize applications to a Federal judge of competent jurisdiction for orders authorizing or approving the interception of wire and oral communications by the Federal Bureau of Investigation or a Federal agency having responsibility for the investigation of the offense(s) as to which such application is made, when such interception may provide evidence of any of the offenses specified in section 2516 of title 18, United States Code:

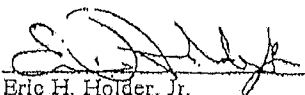
1. The Assistant Attorney General in charge of the Criminal Division, any Acting Assistant Attorney General in charge of the Criminal Division, any Deputy Assistant Attorney General of the Criminal Division, and any Acting Deputy Assistant Attorney General of the Criminal Division;

2. The Assistant Attorney General for National Security, any Acting Assistant Attorney General for National Security, any Deputy Assistant Attorney General for National Security, and any Acting Deputy Assistant Attorney General for National Security, with respect to those matters delegated to the supervision and responsibility of the Assistant Attorney General for National Security. These officials of the National Security Division shall exercise this authority through, and in full coordination with, the Office of Enforcement Operations within the Criminal Division.

Attorney General Order No. 2943-2008 of January 22, 2008, is revoked effective at 11:59 p.m. of the day following the date of this order.

Date

2-26-09


Eric H. Holder, Jr.
Attorney General



U.S. Department of Justice

Criminal Division

Washington, D.C. 20530

The Honorable Dana J. Boente
United States Attorney
Eastern District of Virginia
Alexandria, Virginia

FEB 18 2015

Attention: Keith Becker and Michael Grant,
Trial Attorneys, U.S. Department of Justice,
Criminal Division, Child Exploitation and
Obscenity Section

Dear Mr. Boente:

An appropriate official hereby approves an application to be made to a federal judge of competent jurisdiction for an order under Section 2518 of Title 18, United States Code, authorizing, for a thirty (30) day period, the interception of electronic communications occurring over the private message function and private chat function of the website "upf45jv3bziuctml.onion," in connection with an investigation into possible violations of federal felonies by Steven W. Chase, and others as yet unknown.


The above-described application may be made by you or any other attorney on your staff who is an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code.

Sincerely,

Leslie R. Caldwell
Assistant Attorney General
Criminal Division

FEB 18 2015

Date


KENNETH A. BLANCO
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

FILED

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

2015 FEB 20 A 8:42

ALEXANDRIA DIVISION

IN THE MATTER OF THE APPLICATION :
OF THE UNITED STATES OF AMERICA :
FOR AN ORDER AUTHORIZING THE :
INTERCEPTION OF ELECTRONIC :
COMMUNICATIONS :

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA
CASE NO. 1:15-ES-4

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR AN ORDER
AUTHORIZING INTERCEPTION OF ELECTRONIC COMMUNICATIONS**

I, Caliope Bletsis, being duly sworn, state the following:

INTRODUCTION

1. I have been employed as a Special Agent (“SA”) with the Federal Bureau of Investigation (FBI) since December 2004, 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. This affidavit is submitted in support of the Government's Application for an Order under Title 18, United States Code, Section 2518, authorizing the interception, for a period of up to thirty days, of the electronic communications of Steven W. Chase, and other unidentified administrators and users ("TARGET SUBJECTS") of a child pornography website upf45jv3bziuctml.onion, hereinafter the "TARGET WEBSITE,"¹ occurring over the private message function ("TARGET FACILITY 1") and private chat function ("TARGET FACILITY 2"), of the TARGET WEBSITE.

3. As a result of my personal participation in this investigation, through information obtained from other federal and foreign law enforcement agents and witnesses, including physical surveillance and the review of documents, and on the basis of other information that I have reviewed and determined to be reliable, I allege facts to show that:

- a. There is probable cause to believe that the TARGET SUBJECTS have committed, are committing, and will continue to commit offenses specified in Title 18, United States Code, § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography, and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), Knowing Possession of, Access or Attempted Access With Intent to View

¹ The actual name of TARGET WEBSITE is known to law enforcement. The site remains active and disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site, potentially provoking members to notify other members 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 and the website will be identified as "TARGET WEBSITE".

Child Pornography (collectively, the "TARGET OFFENSES").

- b. There is probable cause to believe that particular electronic communications of TARGET SUBJECTS concerning the TARGET OFFENSES will be obtained through interception of electronic communications occurring over TARGET FACILITY 1 and TARGET FACILITY 2 (together referred to as the "TARGET FACILITIES"). In particular, these communications are expected to lead to the revelation of evidence concerning the TARGET OFFENSES, including the content of communications between and among the TARGET SUBJECTS. In addition, these electronic communications are expected to constitute admissible evidence of the commission of the TARGET OFFENSES.

4. The requested Order is sought for a period of time until the interception fully reveals the manner in which the TARGET SUBJECTS and their confederates participate in the TARGET OFFENSES, or for a period of thirty (30) days, whichever occurs first, pursuant to Title 18, United States Code, Section 2518(5). Pursuant to Section 2518(5) of Title 18, United States Code, it is further requested that the 30-day period be measured from the earlier of the date on which investigative or law enforcement officers begin to conduct interception under this Court's Order or 10 days from the date of this Court's Order.

5. 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 administrative subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/employees/computer

forensic professionals; and my experience, training and background as a Special Agent with the FBI.

6. Because this affidavit is being submitted for the limited purpose of securing authorization for the collection of electronic communications, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for an order authorizing the interception of electronic communications occurring over the Internet via communications occurring over TARGET FACILITY 1 and TARGET FACILITY 2.

RELEVANT STATUTES

7. This investigation concerns alleged violations of: Title 18, United States Code, § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and 18 U.S.C. §§2252A(a)(5)(B) and (b)(2), Knowing Possession of, Access or Attempted Access With Intent to View Child Pornography.

- a. 18 U.S.C. § 2252A(g) prohibits a person from engaging in 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)(1) 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)(1) 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.

DESCRIPTION OF TARGET FACILITIES

- 8. TARGET FACILITY 1: The private message function of the TARGET WEBSITE is similar to e-mail messages and allows the TARGET SUBJECTS to send and

receive communications with other users and/or administrator(s) of the TARGET WEBSITE, such that the private message is only accessible to the user who sent or received such a message and the site administrator(s).

9. TARGET FACILITY 2: The private chat function of the TARGET WEBSITE allows the TARGET SUBJECTS to communicate in real-time directly with each other and the communications are only visible and accessible to the users engaged in the private chat and the administrator(s).

10. Other than TARGET FACILITY 1 and TARGET FACILITY 2, described above, there are no other private areas of the TARGET WEBSITE where communications are only visible to some, but not all, registered users.

TARGET SUBJECTS

11. Steven W. Chase (“Chase”) – As described in further detail below, Chase has been identified as the primary administrator (“Administrator-1”) of the TARGET WEBSITE. Other than Chase, all other current users and administrators of the TARGET WEBSITE remain unidentified.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

12. 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. 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 site 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)(1) 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 alphanumeric 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 process 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. A “Proxy Server” is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. Proxy

servers can facilitate access to content on the World Wide Web and prove anonymity.

- p. 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, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- q. “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).
- r. “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).
- s. “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”).

SUMMARY OF PROBABLE CAUSE

13. The TARGET SUBJECTS are the administrators and users of the TARGET WEBSITE who regularly send and receive illegal child pornography via the TARGET WEBSITE which operates as a “hidden services” located on the Tor network, further described below. This 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 the TARGET OFFENSES. As of February 12, 2015, a law enforcement agent visited the TARGET WEBSITE, in an undercover capacity, and confirmed that the site remains active, accessible and substantially the same as described herein.

The Tor Network

14. 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.²

² 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

15. 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 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.

16. 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 in the same manner 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 "asdlk8fs9df1ku7f" 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

network.

hosts the website through those public lookups.

Finding and Accessing the TARGET WEBSITE

17. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of the TARGET WEBSITE 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 TARGET WEBSITE as well as the site'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, including the TARGET WEBSITE. Accessing the TARGET WEBSITE therefore requires numerous affirmative steps by a user, making it extremely unlikely that any user could simply stumble upon the 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 TARGET WEBSITE Content and Criminal Use of the TARGET

FACILITIES

18. Between September 16, 2014 and February 3, 2015, FBI Special Agents, acting in an undercover capacity, connected to the Internet via the Tor Browser and accessed TARGET WEBSITE.³ The TARGET WEBSITE is a message board website whose primary purpose is the

³ As of February 18, 2015, the URL of the TARGET WEBSITE had changed from muff7i44irws3mwu.onion to upf45jv3bzuctml.onion. I am aware from my training and experience that it is possible for a website to be moved

advertisement and distribution of child pornography. According to statistics posted on the site, TARGET WEBSITE contained a total of 95,148 posts, 9,333 total topics, and 158,094 total members. Based on the earliest known post, the website appeared to have been operating since approximately August 19, 2014.

19. 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 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]." 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."

20. 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.

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 periodically changes the location and URL of the TARGET WEBSITE in order to avoid law enforcement detection. An FBI agent accessed the TARGET WEBSITE in an undercover capacity on February 18, 2015, at its new URL, and determined that its content has not changed.

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 turn 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 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."

21. After accepting the above terms, registration to the message board then requires a user to enter a username, 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:

<u>Section – Forum</u>	<u>Topics</u>	<u>Posts</u>
General Category		
[TARGET WEBSITE] information and rules	25	236
How to	133	863
Security & Technology discussion	281	2,035
Request	650	2,487
General Discussion	1,390	13,918
The INDEXES	10	119
Trash Pen	87	1,273

[TARGET WEBSITE] Chan		
Jailbait ⁴ – Boy	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 ⁵	1,427	20,992
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	31	135
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

⁴ Based on my training and experience, I know that “jailbait” refers to underage but post-pubescent minors.

⁵ 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.

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
Pycecknn – Russian	8	239
Stories		
Fiction	99	505
Non-fiction	122	675

22. 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. Another service available to users was the ability to send private chat messages between users.

23. 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.

24. A review of the various topics within 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.

25. A review of topics within the remaining forums revealed the majority contained discussions, as well as numerous images that appeared to depict child pornography 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 a prepubescent or early pubescent female engaged in sexually explicit conduct. 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 a prepubescent female engaged in sexually explicit conduct. One of these images depicted the female being orally penetrated by the penis of a male.

On September 16, 2014, the user "tutu01" posted a topic entitled "9yo Niece - Horse.mpg" in the "Pre-teen Videos - Girls HC" forum that contained four images depicting a prepubescent female engaged in sexually explicit conduct 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.

26. 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 on average over 1,500 unique users visited the website daily and over 11,000 unique users visited the website over the course of a week. A private message feature, TARGET FACILITY 1, 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....”

27. Further review revealed numerous additional posts referencing private messages or PMs regarding posts 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.”

28. Additionally, law enforcement agents reviewed hundreds of private messages occurring over TARGET FACILITY 1 that were in furtherance of the TARGET OFFENSES and/or provided information on the identities of the TARGET SUBJECTS. These private messages were collected over the server for the TARGET WEBSITE, and law enforcement was able to access these messages through the server copy that was obtained from the search warrant for the TARGET WEBSITE in January 2015. Examples of these messages, which law enforcement believes discusses the sexual abuse of minors, are as follows:

- a. On January 10, 2015, the user “kinderkutje” sent a private message to the user “LittleGirlLover369” stating: “Hi, thnx! She is cute and tasty indeed...She's around 1,5yo on that photo....I play with her everytime I have her alone, started from around 3/4 mo...She's now 3,5. I also have another niece, also 3,5 but they are not sisters, and as tasty as the other one ;-) Never had them together at once unfortunately! I only tried anal once with the niece in my avatar when she was 2,5, almost got the head of my cock inside.... Never penetrated their pussies (except with my tongue) and

never cummed inside their asses or pussies directly (all too dangerous) For the rest, I did everything...Even thought a couple of times to show them on my webcam, naked etc, but never got to do that..."

- b. On January 6, 2015, user Cyclopz sent a private message to "drprlvinguy" that contained the following: "My personal feelings are that were you to have a consensual sexual relationship with a child that she enjoyed, two things might make her regret it in her late teens and early twenties. One is the knowledge that her sexual partner was her father and two, the sex was recorded. My name Cyclopz alludes to my 1080p HD hidden camera glasses I have for recording purposes although I plan to use them with another little girl in my life, a 5 year old brunette pixie not related to me by blood. POV porn is another favorite of mine. ;)."
- c. On December 16, 2014, the user "elizza" sent a private message to the user "Cadvan123" stating the following: "but contact me only if you are ready to rape your sisters. when you think they are too good for you then don't waste my time!"

29. 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 TARGET WEBSITE site, described above as TARGET FACILITY 1, 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 TARGET SUBJECTS.

30. The TARGET WEBSITE also includes a feature referred to as "[TARGET WEBSITE] Image Hosting." This feature of the TARGET WEBSITE allows users of the TARGET WEBSITE to upload images of child pornography that are in turn, only accessible to users of the TARGET WEBSITE. On February 12, 2015, an FBI agent operating in an

undercover capacity 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 "[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.

31. The TARGET WEBSITE also includes a feature referred to as "[TARGET WEBSITE] File Hosting." This feature of TARGET WEBSITE allows users of TARGET WEBSITE to upload videos of child pornography that are in turn, only accessible to users of TARGET WEBSITE. On February 12, 2015, an FBI Agent operating in an undercover capacity 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 "[TARGET WEBSITE] File Hosting." The video depicted an adult male masturbating and ejaculating into the mouth of a nude, prepubescent female.

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

- a. 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.

- b. User "Rusty" posted a link to an image that depicted a prepubescent female with an amber colored object inserted into her vagina.
- c. 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 genitals.
- d. Other images that appeared to depict child pornography were also observed.

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

34. Messages posted in [TARGET WEBSITE] Chat are generally public and available for all users to see. A review of [TARGET WEBSITE] Chat showed that it also contained a feature allowing users of [TARGET WEBSITE] Chat to send messages privately, over TARGET FACILITY 2, which are only visible to the sender and intended recipient(s). Examples of messages sent using TARGET FACILITY 2 were collected over the server for the TARGET WEBSITE, and law enforcement was able to access these messages through the server copy that was obtained from the search warrant for the TARGET WEBSITE in January 2015. Examples of these messages, which law enforcement believes discusses the sexual abuse of minors, are as follows:

- a. On January 14, 2015, the user "pedoman88" sent a private chat message to "hornyuncle" stating "made it easier when daughter comes over...sis still calls me when she gets drunk...of course shes 20 now....still a good fuck ;)."
- b. On January 14, 2015, the user "hornyuncle" sent a private chat message to "CuteGirlLover" that stated "mmmm I want to cover that in cum." Prior to this message, "CuteGirlLover" had sent "hornyuncle" multiple private chat messages that contained links to images located on hidden services with the path

“gh/girls_sc/src/1420407661151-5.jpg” after the address. The links were no longer active, but based on my training and experience, I know members of sites such as the TARGET WEBSITE often send links to images of child pornography. The links often expire after a certain amount of time or the original uploader deletes the file.

- c. On January 14, 2015, the user “honyuncle” sent two private chat messages to “pedoman88” that stated “gotta love the internet meet like minded folks” and “alone man but another pedo helped me get started with her.”

35. Based on my training and experience and the review of the site by law enforcement agents, I believe that the private chat function of the site, described above as the TARGET FACILITY 2, 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 TARGET SUBJECTS.

36. A review of message threads also revealed that users discussed traveling to foreign countries with the intent to sexually abuse children in a foreign country. One example of this type of discussion is where user “luvazngrls” posted a thread on October 8, 2014, titled “Travel Advice in Asia, SE Asia, and Australia,” and asked “I need to take a vacation soon somewhere in Asia or Southeast Asia (though possibly as far as Australia). Can anyone give me some tips for the best places to go to find accessible girls (10-13) in the region?...Whatever I need to know to find some girls for a few days...Pay to play is fine.” Another user, “youssef,” responded on October 8, 2014, and stated, “[Y]ou can try phillippines, don’t go to Indonesia.” A second user, “Global,” responded on October 11, 2014, and stated “[Y]ou will find that in most countries child brothels are in the small villages and towns, not in cities...Most brothels will let the very young do BJs, but no fucking which is left with the older girls. In Asian countries, a

child brothel is quite easy to find, just ask around...Best is to arrange a girl to be delivered to your hotel.”

Target Website Sub-Forums

37. 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 textual descriptions of sexually abusing children: (a) Pre-teen Videos - Girls HC; (b) Pre-teen Videos - Boys HC; (c) Pre-teen Photos - Girls HC; (d) Pre-teen Photos - Boys HC; (e) Potpourri – Toddlers; (f) Potpourri - Family Play Pen – Incest; (g) Spanking; (h) Kinky Fetish – Bondage; (I) Peeing; (j) Scat⁶; (k) Stories - Non-Fiction; (l) Zoo; (m) Webcams – Girls; and (n) Webcams – Boys.

Identification and Seizure of the Computer Server Hosting the TARGET WEBSITE

38. 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 provided information that the IP Address 192.198.81.106 was owned by Centrilogic, a server hosting company headquartered at 801 Main Street NW, Lenoir, NC 28645-3907. Through further investigation, FBI verified that TARGET WEBSITE was hosted from the previously referenced IP address. Due to a misconfiguration of the server hosting the TARGET WEBSITE, the TARGET WEBSITE was available for access on the regular Internet to users who knew the true IP address of the server. After receiving the tip from the foreign law enforcement agency, an FBI Agent, acting in an undercover capacity, accessed IP Address 192.198.81.106 on the regular Internet and resolved to the TARGET WEBSITE. 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

⁶ Based on my training and experience, “scat” refers to sexually explicit activity involving defecation and/or feces.

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 is currently located on a computer server at a government facility in Newington, VA, in the Eastern District of Virginia.

39. 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 TARGET WEBSITE will remain unknown. 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 TARGET WEBSITE, the logs of member activity will contain only the IP addresses of Tor "exit nodes" utilized by board users. Those IP address logs cannot be used to locate and identify the administrators and users of TARGET WEBSITE.

Primary Administrator

40. Further investigation has identified a suspected administrator ("Administrator-1") of TARGET WEBSITE, who has administrative control over the computer server in Lenoir, NC, that hosts the TARGET WEBSITE, as Steven W. Chase, a resident of Naples, FL.

41. As mentioned previously in this affidavit, a review of TARGET WEBSITE showed that TARGET WEBSITE had been misconfigured and was accessible through the regular Internet, if a user knew the true IP Address of the site. The primary administrator of TARGET WEBSITE, referred to herein as "Administrator-1," has been trying to fix the problem. FBI agents know this by reading his private messages from the copy of the TARGET WEBSITE

that was seized pursuant to the aforementioned search warrant. With this in mind, despite being a hidden service, FBI learned that the main admin account on the message board (Administrator-1) was logged into directly from an IP address assigned to Steven Chase's Florida residence, 3570 15th Ave SW, Naples, Florida 34117, in September 2014 and November 2014.

42. A review of the log files showed that the server had also been accessed remotely from IP Address 67.251.7.149 on more than 10 days between December 21, 2014 and January 18, 2015. The server was accessed remotely using Secure Shell ("SSH") and File Transfer Protocol ("FTP"). Based upon my training and experience, I know that both SSH and FTP require usernames and passwords that must be created by the administrator of a server. Without the proper username and password, an individual would not be able to connect to a server with SSH or FTP. Taking this into consideration, I believe that the individual who accessed the server at IP Address 192.198.81.106 from IP Address 67.251.7.149 is the, or one of the, administrators of TARGET WEBSITE. The connections to the Target Server were generally between the hours of 8PM Eastern and 3AM Eastern Standard Time ("EST"). Some connections were made outside of this general time frame.

43. A publicly available website provided information that IP Address 67.251.7.149 was owned by Time Warner Cable. Time Warner Cable provided information in response to a subpoena indicating that IP Address 67.251.7.149 was assigned to Louise Chase, 3119 Carrabassett Drive, Carrabassett Valley, ME 04947 on January 9, 2015 at 17:26:25 EST. According to information provided by Centrilogic, the billing account associated with the server hosting TARGET WEBSITE was accessed from IP Address 67.251.7.149 on this date and time. SSH and FTP connections were also observed between IP Address 67.251.7.149 and the Target Server on January 9, 2015.

44. Surveillance conducted by FBI Agents and local law enforcement officers at 3119 Carrabassett Drive, Carrabassett Valley, ME 04947 revealed a White Dodge Charger in the driveway on January 30, 2015. A local law enforcement officer provided information that the vehicle had been in two accidents in the Carrabassett Valley area in December 2014. The driver of the vehicle was Steven William Chase, son of Louise Chase. Steven Chase told the responding officers at the time of his accidents that he was visiting his mother. Steven Chase had a Florida Driver's license which listed his address as 3570 15th Ave SW, Naples, Florida 34117. The license plate listed for Steven Chase's vehicle on the accident report was a Florida license plate.

45. On December 14, 2014, Administrator-1 sent a private message on TARGET WEBSITE that read, "I am still on my winter vacation for another four months or so."

46. On January 26, 2015, a Pen Register / Trap Trace ("PRTT") order was served on Time Warner Cable for the Internet account at - 3119 Carrabassett Valley Drive, Carrabassett Valley, ME 04947. The FBI began receiving data and monitoring the PRTT on January 27, 2015. Analysis of the PRTT showed Internet activity consistent with an individual accessing "TARGET WEBSITE" typically between the hours of 6PM Eastern and 1AM Eastern. Some pertinent activity was also observed outside of this time frame. The activity was observed on several days between January 28, 2015 and February 2, 2015.

47. On February 3, 2015 the PRTT stopped receiving data. Time Warner Cable was contacted and advised that the cable modem at the residence had been disconnected. A public Facebook profile for Steven Chase provided information that Steven Chase departed Maine on February 3, 2015, and returned to Florida on February 5, 2015.

48. On February 6, 2015, a PRTT order was served on Comcast for the Internet

account at Chase's residence at 3570 15th Ave SW, Naples, Florida 34117. Comcast had previously provided information in response to a subpoena indicating that the Internet account at the residence was registered in the name Barbara Chase. A records search indicated that Barbara Chase was the deceased wife of Steven William Chase.

49. FBI began monitoring of the Comcast PRTT on February 12, 2015. Analysis of the PRTT data showed a significant amount of activity over an encrypted Virtual Private Network ("VPN") service between 6PM Eastern Time on February 12, 2015 and 1AM Eastern Time on February 13, 2015. On February 13, 2015, an undercover FBI Agent accessed TARGET WEBSITE and observed that Administrator-1 had been logged in to TARGET WEBSITE during this time frame. Based on my training and experience, I know that individuals who wish to conceal illegal activity on the Internet will often use encrypted VPN services to do so. This particular VPN service is based in a foreign country that does not respond to United States legal process. A description of the VPN service available on the service's public Internet website contains the following description: "We are committed to your privacy and do not collect or log traffic data or browsing activity from individual users connected to our VPN" and "We are a privacy-focused service and have a strict no logging policy! We do not track or monitor user activities while connected...."

50. According to information provided by Centrilogic, the server hosting TARGET WEBSITE was paid for with a PayPal account associated with email address miket46589@yahoo.com. In response to a subpoena, PayPal provided information that the PayPal account was accessed from IP Address 50.188.218.61 on November 10, 2014 at 13:37:37 Pacific Time. A publicly available website provided information that IP Address 50.188.218.61 was owned by Comcast. Comcast provided information in response to a subpoena indicating

that IP Address 50.188.218.61 was assigned to Steven William Chase's residence, 3570 15th Ave SW, Naples, Florida 34117, on the provided date and time.

51. Based on the information provided in the preceding paragraphs, your affiant believes that Steven William Chase is Administrator-1 of "TARGET WEBSITE", that he administered the website from his Florida residence in November 2014, continued to administer the website from his mother's Maine residence in December 2014, January 2015, and February 2015, and that he has continued to administer the website since returning to his Florida residence in February 2015.⁷

52. Accordingly, on February 19, 2015, FBI personnel executed a court-authorized search at the Naples, 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 of TARGET 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.

DEPLOYMENT OF NETWORK INVESTIGATIVE TECHNIQUE

⁷ As explained supra, footnote 3, the administrator of the TARGET WEBSITE periodically changes its location and URL in order to avoid law enforcement detection. As of February 18, 2015, investigation has revealed the current IP address of the TARGET WEBSITE to be 199.241.188.206. As noted herein, due to a mis-configuration of the TARGET WEBSITE, the TARGET WEBSITE is accessible through the regular Internet, if a user knows the true IP Address of the site. On February 18, 2015, an FBI agent acting in an undercover capacity accessed the TARGET WEBSITE at IP address 199.241.188.206. That IP address is assigned to Centrilogic, Inc., and, according to information obtained from Centrilogic, is one of the IP addresses that Chase has contracted for his use.

53. As noted above, the TARGET WEBSITE will operate from a government facility in Newington, Virginia, within the Eastern District of Virginia, and remain online and accessible to the TARGET SUBJECTS for a limited period of time. During the period of this authorization, FBI expects to concurrently deploy a court-authorized Network Investigative Technique (“NIT”) on the TARGET WEBSITE in an attempt to identify the actual IP addresses and other identifying information for computers used by TARGET SUBJECTS to access the TARGET WEBSITE. The NIT will send one or more communications to TARGET SUBJECTS that access the TARGET WEBSITE after the date of its deployment, which communications are designed to cause the computer receiving it to deliver data that will help identify the computer, its location, other information about the computer, and the user of the computer accessing the TARGET WEBSITE. In particular, the NIT is designed to reveal to the government the computer’s actual IP address, the date and time that the NIT determines what that IP address is, a unique session identifier to distinguish the data from that of other computers and other information, and other information that may assist in identifying computers that accesses the TARGET WEBSITE and their users. Separate authorization will be sought from this Court for the execution of that search warrant and the deployment of the NIT.

TARGET SUBJECTS COMMUNICATIONS ON THE TARGET WEBSITE

54. TARGET SUBJECTS can communicate on the TARGET WEBSITE in four ways: (1) through postings or reply postings on the website, which may include videos, images, or links to videos or images, which are visible and accessible to any user who accesses the board, including law enforcement agents; (2) through the public chat feature of the website, which may also include videos, images, or links to videos or images, which are visible and accessible to any user who accesses the board, including law enforcement agents; (3) through TARGET

FACILITY 2, the private chat feature on the website, which is similar to the public chat function but is only visible and accessible to the users engaged in the private chat; and (4) through TARGET FACILITY 1, the private message function, which is similar to e-mail messages and which are only accessible to the user who sent or received such a message and the site administrator(s). Other than the private messaging function and private chat function, there are no private areas of the TARGET WEBSITE where communications are only visible to some, but not all, registered users.

55. In order to access any of the content of the TARGET WEBSITE, it is necessary to register with a username and a password. Only users of the TARGET WEBSITE who register with a username and a password have access to the private messaging and private chat functions. The private message function is not an "instant messaging" system where users communicate in real time, but rather operates similar to sending and receiving e-mails. The private chat function is similar to an "instant messaging" system where the users communicate in real time, but only with other users who are engaged in the private chat. Multiple examples of public postings on the TARGET WEBSITE where TARGET SUBJECTS discuss the use of private messaging and private chat are described herein.

56. TARGET SUBJECTS communicate anonymously on the sites, using aliases known as "screen names." TARGET SUBJECTS rarely, if ever, post any personally identifiable information that would allow law enforcement to identify the TARGET SUBJECTS or the TARGET SUBJECTS actual location on areas of the TARGET WEBSITE accessible to all users. In fact, the site specifically cautions its users not to post or share any identifying information as described in the rules of TARGET WEBSITE listed in paragraph 20 of this affidavit. Based upon my training and experience, users are more likely to send information that

is identifying or that could corroborate other identifying information in private messages or private chats exchanged only between board users. For example, I am aware of multiple investigations into Tor network child pornography websites that allowed private messages or private chats to be exchanged between members, where certain members of the site were identified in part because of personal details and open Internet online accounts shared in private messages which were intercepted pursuant to a Title III authorization. Such personal details included their actual geographic location, open Internet e-mail addresses about which data could be obtained via subpoenas or search warrants, and information about child victims which users claimed to be sexually abusing. Reviewing private messages, private chats, and postings in private areas of the TARGET WEBSITE in real time will allow agents to act upon any identifying details or details about child victims immediately upon the sending or receipt of such a message or chat, rather than waiting for the later execution of a search warrant to retrieve historical private message or private chat data. That information received in real time can be paired with information gathered via the NIT and other information available in postings to help to identify or corroborate the identity of TARGET SUBJECTS. Also based upon my training and experience, users often privately trade child pornography which is facilitated by communication via private messages or private chat. Users may directly send child pornography via private message or private chat, or exchange information that allows them to trade child pornography via other digital platforms -- for example, another e-mail account, a file hosting website, or other child pornography websites. Child pornography that is trafficked via file uploading websites is often made available only for a limited period of time, which is a security measure by the user in order to avoid detection. Where law enforcement agents are able to intercept a communication directing a user to a file sharing website or to download location, that

file can be downloaded by law enforcement and therefore preserved as evidence. Accordingly, reviewing such messages in real time may provide crucial evidence of child pornography trafficking which would not be available by reviewing historical messages. Furthermore, I am aware from training and experience as well as the review of seized data from the TARGET WEBSITE that the administrators and moderators of the website communicate with each other regarding the administration, management and facilitation of the TARGET WEBSITE via private messaging. During the period of time that the TARGET WEBSITE will operate from a government facility, those administrators and moderators may communicate via private messages or private chats regarding any changes made to the TARGET WEBSITE and the potential of law enforcement infiltration of the site. Law enforcement agents will be able, following the apprehension of Chase, to communicate as the main administrator of the TARGET WEBSITE. However, law enforcement would not be able, absent the interception of private messages, to learn in real time about communications between other administrators and moderators suggesting an awareness of changes made to the TARGET WEBSITE (to facilitate the investigative techniques discussed herein) and potential actions those administrators and moderators may take to alert others, obstruct justice or destroy evidence. While the TARGET WEBSITE is operating at a government facility for a limited period of time, FBI will have access to all users' private messages and private chats, which may include videos, images, or links to videos or images, which are visible and accessible only to certain users of the sites.

PERSONS LIKELY TO BE INTERCEPTED

57. The INTERCEPTTEES include Steven Chase and those TARGET SUBJECTS who send or receive private messages or private chats on the TARGET WEBSITE during the 30-day period of this authorization. At this time, because of the anonymous nature of the Tor

network and the choice of the TARGET SUBJECTS to utilize that functionality, the actual identities of the TARGET SUBJECTS are unknown.

NECESSITY FOR COLLECTION OF PRIVATE MESSAGES AND PRIVATE CHATS

58. Based on my training and experience as a Special Agent, as well as the experience of other law enforcement officers involved in this investigation, and based upon all of the facts set forth herein, it is my belief that the seizure of the TARGET WEBSITE in conjunction with its continued operation for a limited period of time, the deployment of a NIT to attempt to identify actual IP addresses used by the TARGET SUBJECTS, and the interception of electronic communications of the TARGET SUBJECTS occurring over the TARGET FACILITIES as applied for herein, is the only available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the identity of the TARGET SUBJECTS and that they are engaging in the TARGET OFFENSES. I believe that such combination of investigative steps are the only available technique likely to provide law enforcement with the critical information needed for this investigation, i.e., evidence of the actual identity of the TARGET SUBJECTS and that of their accomplices, aiders and abettors, co-conspirators and participants in illegal activities, who have deployed advanced technology to remain anonymous while conducting their illegal activity; the nature, extent and methods of operation of TARGET SUBJECTS' unlawful activities; the existence and locations of records relating to those activities; communications between TARGET SUBJECTS and their accomplices, aiders and abettors, co-conspirators and participants in those illegal activities; and the location and identity of computers used to further the TARGET OFFENSES.

59. The interception of private messages and private chats in real time is necessary for several reasons. TARGET SUBJECTS communicate anonymously on the sites, using aliases

known as "screen names." As described above, private messaging and private chat is only available to users who register with a username and password. TARGET SUBJECTS rarely, if ever, post any personally identifiable information that would allow law enforcement to identify the TARGET SUBJECTS or the TARGET SUBJECTS actual location on areas of the TARGET WEBSITE accessible to all users. In my training and experience, users are more likely to send information that is identifying or that could corroborate other identifying information in private messages and private chats exchanged only between board users or within private areas only accessible to certain users. For example, I am aware of multiple investigations into Tor network child pornography websites that allowed private messages and private chats to be exchanged between members, where certain members of the site were identified in part because of personal details and open Internet online accounts shared in private messages and private chats which were intercepted pursuant to a Title III authorization. Reviewing private messages and private chats in real time will allow agents to act upon any identifying details or details about child victims immediately upon the sending or receipt of such a message, rather than waiting for the later execution of a search warrant to retrieve historical private message and private chat data. That information received in real time can be paired with information gathered via the NIT and other information available in postings to help to identify or corroborate the identity of TARGET SUBJECTS.

60. Interception of private messages and private chats is also necessary for the identification and protection of potential victims of child sexual abuse. There are postings to the TARGET WEBSITE by at least two members who contend to have access to children, one of which has posted images that the user contends are of sexual abuse the user has committed against children. That individual ("CD-1") was identified through other investigative means and

admitted to producing images of child pornography subsequent to his arrest in February 2015. In the event that a user shares information about child sexual abuse and/or the production of child pornography in a private message or private chat that is being monitored in real time, agents can, in conjunction with the deployment of the NIT and any other available evidence, immediately take action to locate and identify that user in an attempt to prevent further abuse of that child. In that scenario, reviewing such private messages and private chats only after the execution of a search warrant would waste crucial time.

61. Moreover, in order for the NIT to have a chance to work, members need to continue to access the TARGET WEBSITE after the NIT is deployed. In order to ensure that users continue to access the TARGET WEBSITE, it is necessary that there be as minimal an interruption as possible in the operation of the TARGET WEBSITE, so as not to create suspicion among the TARGET SUBJECTS that a law enforcement action is taking place on the board. In my training and experience and in reviewing messages posted on the TARGET WEBSITE, and other child pornography and exploitation websites operating on the Tor network, interruptions in service for more than a minimal time period is a tip-off to board users that law enforcement infiltration may be going on and may result in users not accessing the board for a period of time. Law enforcement will review historical private messages and private chats for any identifying information shared by TARGET SUBJECTS, however, that review takes time. Review of the seized copy of TARGET WEBSITE has included scraping message board postings and private messages for personally identifying information such as e-mail addresses and user names for other Internet services. Analysis of that data is ongoing and efforts are being made to determine which, if any, of the identified e-mail addresses and usernames are real and can be utilized to obtain a true identity for any users of TARGET WEBSITE. Other than Chase, and CD 1, none of

the other administrators or users have been identified. Waiting for such a review to be complete before deploying a NIT and monitoring private messages and private chats on the TARGET WEBSITE in real time would deprive law enforcement of potentially crucial information at a critical phase in the investigation.

NORMAL INVESTIGATIVE PROCEDURES

62. Based upon your affiant's training and experience, as well as the experience of other FBI agents and law enforcement officers with whom I have investigated this case, and based upon all of the facts set forth herein, it is your affiant's belief that the seizure of the TARGET WEBSITE in conjunction with its continued operation for a limited period of time, the deployment of a NIT to attempt to identify actual IP addresses used by the TARGET SUBJECTS, and the interception of electronic communications of the TARGET SUBJECTS occurring over the TARGET FACILITIES is the only available technique with a reasonable likelihood of securing the evidence necessary to prove that the TARGET SUBJECTS are engaging in the SUBJECT OFFENSES beyond a reasonable doubt. Due to the unique nature of the information sought, numerous investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed, reasonably appear to be unlikely to succeed if they are tried, or are too dangerous to employ for the reasons discussed below.

UNAVAILABILITY OF ALTERNATIVE INVESTIGATIVE TECHNIQUES

63. Your affiant and other investigators in criminal investigations of violations of Title 18, United States Code, Sections 2251 and 2252A, et seq., customarily use the following investigative techniques: (a) physical surveillance; (b) use of Grand Jury Subpoenas; (c) interview of subjects or associates; (d) search warrants; (e) infiltration by undercover officers; and (f) use of cooperating individuals.

64. Over the past three years, investigators have also explored various means and methods of investigating Tor based websites and offenders using Tor. As set forth below these techniques are insufficient to accomplish the objectives of the investigation.

Physical Surveillance

65. Physical Surveillance is unavailable because the TARGET SUBJECTS, other than Chase, are unidentified and communicating in a way that provides for their anonymity.

Grand Jury Subpoenas

66. Grand Jury subpoenas are unavailable because all of the TARGET SUBJECTS, other than Chase, are unidentified and communicating in a way that provides for their anonymity.

Interview of Subject or Associates

67. Interviewing TARGET SUBJECTS or any associates is impossible because all of the TARGET SUBJECTS (but for Steven Chase and CD-1) are unidentified and communicating in a way that provides for their anonymity.

68. CD-1, a member of TARGET WEBSITE previously referenced in this affidavit, who was arrested in February 2015, was interviewed subsequent to his arrest. He did not provide any information that could be used by law enforcement to identify other users of TARGET WEBSITE.

Search Warrants

69. Search warrants are being used actively in this investigation. For example, FBI expects to execute search warrants to deploy a NIT to attempt to identify the TARGET SUBJECTS. As noted herein, however, the execution of the search warrant to seize a copy of the TARGET WEBSITE was insufficient to identify TARGET SUBJECTS and interdict their illegal activity. While possession of the data will provide important evidence concerning the

criminal activity that has occurred on the server and the TARGET WEBSITE, the identities of the other administrators and users of the TARGET WEBSITE will remain unknown. 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, logs of member activity, if any, will contain only the IP addresses of Tor "exit nodes" utilized by board users. Those IP address logs cannot be used to locate and identify TARGET SUBJECTS of the TARGET WEBSITE. In order to attempt to identify those users, the website needs to remain operating so that authorization may be obtained to employ a NIT on the site to identify true IP addresses of TARGET SUBJECTS. The execution of a search warrant to seize the TARGET WEBSITE alone would not provide such authority.

70. Agents could execute another search warrant at a later date to again review historical private messages and private chats by TARGET SUBJECTS. Reviewing only historical private messages, private chats, and postings, however, is not sufficient for the reasons stated above. A search warrant will not provide real-time information about TARGET SUBJECTS or communications between and among the TARGET SUBJECTS about their unlawful activities. That real-time information can be paired with other identifying data from a NIT to allow agents to quickly locate and apprehend TARGET SUBJECTS before or as soon as possible after the TARGET WEBSITE ceases operating. When the TARGET WEBSITE ceases to operate, in my training and experience, there is likely to be speculation among TARGET SUBJECTS that a law enforcement action has been taken against the TARGET WEBSITE. That may cause TARGET SUBJECTS to flee or destroy evidence before they can be apprehended. The need for real-time information that can be quickly acted upon is heightened in the event that TARGET SUBJECTS disclose information about ongoing sexual abuse of child victims. Solely reviewing historical private messages, private chats, or postings may prevent agents from

immediately acting upon evidence of ongoing abuse disclosed via private messages or private chats.

71. Search warrants for the physical premises of the TARGET SUBJECTS are unavailable because the other TARGET SUBJECTS are unidentified and communicating in a way that provides for their anonymity. It is not presently known with any certainty where any of the remaining TARGET SUBJECTS reside, or where they receive, hide, transfer, and conceal the proceeds of their crime. Once other TARGET SUBJECTS have been identified, the use of search warrants of physical premises may be a valuable tool. However, until that time, the use of search warrants of physical premises of the TARGET SUBJECTS is infeasible.

72. Agents have considered seizing the TARGET WEBSITE and removing it from existence immediately and permanently. However, at this time, no TARGET SUBJECTS besides the administrator described above have been identified. There are multiple TARGET SUBJECTS who claim that they are sexually abusing children and sharing images of that abuse with others. Removing the TARGET WEBSITE from existence immediately and permanently upon seizure would end the distribution and receipt of child pornography taking place on the TARGET WEBSITE, however, it would prevent law enforcement from attempting to locate and identify the TARGET SUBJECTS and their child victims, and attempting to rescue those child victims from ongoing abuse. Any attempt to identify TARGET SUBJECTS requires that the TARGET WEBSITE remain operating for some period of time. Accordingly, it is your affiant's belief that the seizure of the TARGET WEBSITE in conjunction with its continued operation for a limited period of time, the deployment of a NIT to attempt to identify actual IP addresses used by the TARGET SUBJECTS, and the interception and collection of private messages and private chats sent/received by TARGET SUBJECTS is appropriate in this case.

Confidential Informants, Cooperating Sources, and Undercover Agents

73. Undercover agents have been used in this investigation to access the TARGET WEBSITE and document the sites, their categories, and postings on the sites. Cooperating individuals are unavailable because the TARGET SUBJECTS are currently unidentified and therefore not available to assist with law enforcement activities. The use of undercover agents, confidential informants and cooperating sources in this investigation is unlikely to succeed, however, in terms of meeting the stated objectives of the investigation at this stage. In order to obtain personally identifying data about a TARGET SUBJECT, an undercover agent or cooperating individual would have to engage in private messaging with that TARGET SUBJECT, develop a significant and trusting relationship with the TARGET SUBJECT, and attempt to elicit personally identifying information from the TARGET SUBJECT. As noted above, postings on the TARGET WEBSITE caution its members against providing such information. In my training and experience, such information is much more likely to have been exchanged between existing TARGET SUBJECTS who have already developed such a relationship with each other and shared such information via private messages or private chats.

74. Moreover, using an “administrator” account on the TARGET WEBSITE to attempt to elicit personally identifiable information from TARGET SUBJECTS is not feasible and would immediately be viewed by TARGET SUBJECTS as suspicious and indicative of law enforcement infiltration of the board. That would likely lead unidentified TARGET SUBJECTS to flee the board and/or destroy evidence of their unlawful activity.

Pen Registers and Trap and Trace Devices

75. Pen registers and trap and trace type data have been utilized in this case to verify that the IP Address hosting the TARGET WEBSITE is sending and receiving data on the Tor network. However, at this stage of the investigation, they are inadequate investigative

techniques. Pen registers do not enable law enforcement officers to obtain the content of communications, which is necessary in order to identify the TARGET SUBJECTS. Moreover, because of the way that Tor operates, a pen register and trap and trace device deployed on the TARGET WEBSITE would reveal only the Tor "exit node" used by TARGET SUBJECTS to access the board, which cannot be used to locate and identify that user.

Electronic Interception

76. There have been no prior electronic interceptions of communications occurring on the TARGET WEBSITE.

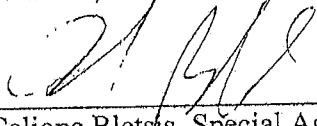
MINIMIZATION

77. Only electronic communications (i.e., private messages and private chats) will be intercepted. All intercepted communications of the TARGET SUBJECTS will be minimized in accordance with Chapter 119 of Title 18, United States Code. The computer server intercepting all communications and on which the TARGET FACILITIES are located will be in Newington, VA, in the Eastern District of Virginia during the period of interception. A copy of intercepted communications will be sent to an FBI facility in Linthicum, Maryland, where certain FBI personnel will be stationed while the TARGET WEBSITE remains operating. Each private message and private chat will be reviewed over a secure system, and based on the identities of the sender and recipient and the content of the private message or private chat, monitoring personnel will determine as soon as practicable after interception whether the private message or private chat appears to be relevant to the investigation or otherwise criminal in nature. If the private message or private chat is not criminal in nature, the private message or private chat will be marked "minimized" and not accessed by other members of the investigative team. If the private message or private chat appears to be privileged, it will be marked "privileged" and

secured from access by other members of the investigative team. If a private message or private chat appears to be relevant to the investigation or otherwise criminal in nature, it will be marked "non-minimized" and may be shared with the other agents and monitors involved in the investigation. If a private message or private chat is marked "minimized" or "privileged," it will not be disseminated to members of the investigative team. All intercepted private messages and private chats will be sealed with the court upon the expiration of the court's order authorizing the interception. It is anticipated that the monitoring location will be staffed at all times, at which time intercepted communications will be monitored and read. The monitoring location will be kept secured with access limited to only authorized monitoring personnel and their supervising agents.

78. As of February 12, 2015, a search of the Electronic Surveillance (ELSUR) Automated Records Systems for DEA, ICE and the FBI was conducted and revealed no prior applications for Court authorization to intercept the wire, oral, or electronic communications involving the same subjects, facilities, or premises specified in this affidavit.

79. IT IS REQUESTED that this Affidavit, the attached Application, the resulting Order, and all reports submitted pursuant to the Order, be sealed until further order of the court.



Caliope Bletsis, Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me
on this 20 day of February, 2015.



UNITED STATES DISTRICT JUDGE
EASTERN DISTRICT OF VIRGINIA

Anthony J. Trenga
United States District Judge

FILED

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

ALEXANDRIA DIVISION 2015 FEB 20 A 8:38

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING THE
INTERCEPTION OF ELECTRONIC
COMMUNICATIONS

CASE NO. 15-1554
U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA
UNDER SEAL

**ORDER AUTHORIZING INTERCEPTION OF ELECTRONIC
COMMUNICATIONS**

Application under oath having been made before me by Assistant United States Attorney for the Eastern District of Virginia Whitney Dougherty Russell and Department of Justice Child Exploitation and Obscenity Section Trial Attorney Michael Grant (hereinafter "the prosecutors"), who are investigative or law enforcement officers of the United States within the meaning of Section 2510(7) of Title 18, United States Code, for an order pursuant to Section 2518 of Title 18, United States Code, authorizing the interception of electronic communications, and full consideration having been given to the matters set forth therein, the Court finds:

- a. there is probable cause to believe that Steven W. Chase, and other unidentified administrators and users ("TARGET SUBJECTS") of the child pornography website upf45jv3bziuctml.onion ("TARGET WEBSITE") have committed, are committing, and will continue to commit federal felony offenses as provided for by Section 2516(3) of Title 18, United States Code, that is: 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; 18 U.S.C. §§ 2252A(a)(5)(B) and

(b)(2), and Knowing Possession of, Access or Attempted Access With Intent to View Child Pornography (“TARGET OFFENSES”);

b. there is probable cause that the TARGET SUBJECTS, during the period of interception authorized by this Order, will use the private message function (“TARGET FACILITY 1”) and private chat function (“TARGET FACILITY 2”), of the TARGET WEBSITE in furtherance of the offenses described above;

c. there is probable cause to believe that the interception of electronic communications authorized by the Order will reveal: (1) the nature, extent and methods of operation of the TARGET SUBJECTS’ unlawful activities; (2) the identity of the TARGET SUBJECTS and their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities, or information that may be useful in establishing the identity of their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (3) the advertising, receipt, and distribution of child pornography related to those activities; (4) the existence and locations of records relating to those activities; and (5) the location and identity of computers used to further the TARGET OFFENSES. In addition, these electronic communications are expected to constitute admissible evidence of the commission of the above-described offenses. It is expected that monitoring of TARGET FACILITY 1 and TARGET FACILITY 2 (together referred to as the “TARGET FACILITIES”) will provide valuable evidence against the TARGET SUBJECTS involved in illegal activities that cannot reasonably be obtained by other means; and

d. it has been established that normal investigative procedures have been tried and have failed, reasonably appear unlikely to succeed if tried, or are too dangerous to employ.

WHEREFORE, IT IS HEREBY ORDERED pursuant to Section 2518 of Title 18, United

States Code, that the FBI and/or individuals employed by or operating under a contract with the government and acting under the supervision of the FBI, are authorized to intercept electronic communications of the TARGET SUBJECTS occurring over the TARGET FACILITIES, until such electronic communications are intercepted that fully reveal: (1) the nature, extent and methods of operation of the TARGET SUBJECTS' unlawful activities; (2) the identity of the TARGET SUBJECTS and their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities, or information that may be useful in establishing the identity of their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (3) the advertising, receipt, and distribution of child pornography related to those activities; (4) the existence and locations of records relating to those activities; and (5) the location and identity of computers used to further the target offenses; and (6) admissible evidence of the commission of the above-described offenses - or for a period of thirty (30) days, to be measured from the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the Order or 10 days after the Order is entered, whichever is earlier from the date of this authorization.

IT IS FURTHER ORDERED that, pursuant to Section 2518 of Title 18, United States Code, special agents with the FBI, and other "investigative and law enforcement officers," as defined in Section 2510(7) of Title 18, United States Code, to be assisted, if necessary, by authorized translators, are authorized to intercept and to record electronic communications of the TARGET SUBJECTS over the TARGET FACILITIES, and that this Order shall be executed as soon as practicable.

IT IS FURTHER ORDERED that all monitoring of electronic communications shall

be conducted in accordance with Chapter 119 of Title 18, United States Code. That is, the computer server intercepting all communications and on which the TARGET FACILITIES are located will be in Newington, VA, in the Eastern District of Virginia during the period of interception. A copy of intercepted communications will be sent to a facility in Linthicum, MD, where certain FBI personnel will be stationed while the TARGET WEBSITES remain operating. Each private message will be reviewed over a secure system, and based on the identities of the sender and recipient and the content of the private message or private chat, monitoring personnel will determine as soon as practicable after interception whether the private message or private chat appears to be relevant to the investigation or otherwise criminal in nature. If the private message or private chat is not criminal in nature, the private message or private chat will be marked "minimized" and not accessed by other members of the investigative team. If the private message or private chat appears to be privileged, it will be marked "privileged" and secured from access by other members of the investigative team. If a private message or private chat appears to be relevant to the investigation or otherwise criminal in nature, it will be marked "non-minimized" and may be shared with the other agents and monitors involved in the investigation. If a private message or private chat is marked "minimized" or "privileged," it will not be disseminated to members of the investigative team. All intercepted private messages and private chat will be sealed with the Court upon the expiration of the court's order authorizing the interception. It is anticipated that the monitoring location will be staffed at all times, at which time intercepted communications will be monitored and read. The monitoring location will be kept secured with access limited to only authorized monitoring personnel and their supervising agents.

IT IS FURTHER ORDERED that the FBI, and any other law enforcement agency, is

permitted to intercept any electronic communications sent from, received by or occurring over the TARGET FACILITIES, including without limitation to any activity of any nature occurring within the TARGET FACILITIES, private messages and private chats sent from or received by the TARGET FACILITIES, draft private messages and private chats, and deleted private messages and private chats.

IT IS FURTHER ORDERED THAT the prosecutors or any other Special Assistant United States Attorney or Department of Justice Trial Attorney familiar with the facts of this case, shall cause to be provided to the Court a report on or about the fifteenth and thirtieth day following the date of the Order or the date interception begins, whichever is later, showing the progress that has been made toward achievement of the authorized objectives and the need for continued interception, although if the Order is renewed for a further period of interception, the application for renewal may serve as the report on or about the thirtieth day. If any of the above-ordered reports should become due on a weekend or holiday, such report shall become due on the next business day thereafter.


IT IS FURTHER ORDERED that this Order, as well as the supporting Application, Affidavit (along with its attachments), proposed Orders, and all interim reports filed with the Court, be sealed until further order of this Court, except that copies of the Order, in full or redacted form, may be served on the FBI as necessary to effectuate the Court's Order. Moreover, the United States may disclose the existence of the interception Order and the contents of pertinent intercepted communications, pursuant to Title 18, United States Code, Sections 2517(2) and (3), as appropriate for the purposes of providing relevant facts to a Court in support of any complaint, arrest warrant, and search or seizure warrant. In addition, the United States may disclose facts, pursuant to Title 18, United States Code, Sections

2517(2) and (3), to provide relevant testimony at any preliminary hearings, detention hearings, grand jury proceedings and other proceedings pertaining to the TARGET SUBJECTS and others as yet unknown. The United States may also disclose facts to foreign investigative or law enforcement officers, pursuant to Title 18, United States Code, Section 2517(7), as necessary to the proper performance of the official duties of the offer making or receiving such disclosure, and that foreign investigative or law enforcement officers may use or disclose such facts or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

IT IS FURTHER ORDERED that no inventory or return of the results of the foregoing interception need be made, other than the above required reports, before 90 days from the date of the expiration of the Order, or any extension of the Order, or at such time as the Court in its discretion may require; and

IT IS FURTHER ORDERED that, upon an ex parte showing of good cause to a judge of competent jurisdiction, the service of the above inventory or return may be postponed for a further reasonable period of time.

DATED: February 20, 2015



Anthony J. Trenga
UNITED STATES DISTRICT JUDGE

Presented by: AUSA Whitney Dougherty Russell
Trial Attorney Michael Grant

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

ALEXANDRIA DIVISION

**IN RE: REQUEST FOR PERMISSION TO
DISCLOSE SEALED DOCUMENTS TO
COMPLY WITH FEDERAL RULE OF
CRIMINAL PROCEDURE 16**

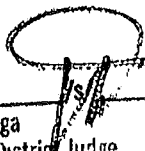
Case Nos. 1:15-ES-4
1:15-SW-89
1:15-SW-106

Filed Under Seal

ORDER

It is hereby ORDERED that the United States is permitted to disclose documents associated with the above-referenced wiretap and search warrants to counsel for charged defendants, as necessary to comply with the obligations of the United States pursuant to Federal Rule of Criminal Procedure 16. The documents remain SEALED pending further order of this Court.

It is further ORDERED that the Clerk of the Court provide a copy of this Order to the United States Attorney's Office.



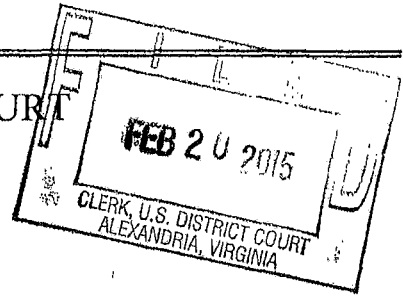
Anthony J. Trenga
United States District Judge 3/26/15

Honorable Anthony J. Trenga
UNITED STATES DISTRICT JUDGE

AO 106 (Rev. 06/09) Application for a Search Warrant

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 upf45jv3bzuctml.onion

Case No. 1:15-SW-89

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location): See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized): See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- [x] evidence of a crime; [] contraband, fruits of crime, or other items illegally possessed; [] property designed for use, intended for use, or used in committing a crime; [] a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Table with 2 columns: Code Section, Offense Description. Row 1: 18 U.S.C. §§ 2252A(g); 2251(d) (1) and/or (e); 2252A(a)(2)(A) and (b)(1); 2252A(a)(5)(B) and (b)(2) | Engaging in a Child Exploitation Enterprise, Advertising and Conspiracy to Advertise Child Pornography; Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; Knowing Access or Attempted Access With Intent to View Child Pornography

The application is based on these facts: See attached affidavit.

- [x] Continued on the attached sheet. [x] Delayed notice of 30 days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Whitney Dougherty Russell

Douglas Macfarlane Applicant's signature

Douglas Macfarlane, Special Agent, FBI Printed name and title

Sworn to before me and signed in my presence.

Date: 02/20/2015

Theresa Carroll Buchanan United States Magistrate Judge

Theresa Carroll Buchanan Judge's signature

City and state: Alexandria, Virginia

Honorable Theresa Carroll Buchanan, U.S. Magistrate Judge Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant

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)
upf45jv3bzuctml.onion)

Case No. 1:15-SW-89

UNDER SEAL

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)

at 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 (name)

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 (check the appropriate box) for 30 days (not to exceed 30).

Until, the facts justifying, the later specific date of /s/

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

Theresa Carroll Buchanan United States Magistrate Judge

City and state: Alexandria, Virginia

Honorable Theresa Carroll Buchanan, U.S. Magistrate Judge Printed name and title

Handwritten signature of Theresa Carroll Buchanan

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

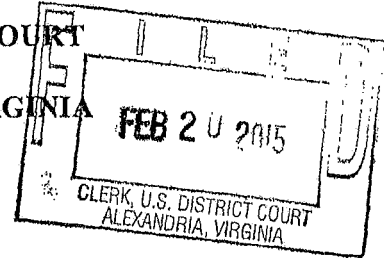
From any “activating” computer described in Attachment A:

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)(1) and or (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), 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.

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.¹

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

4. This investigation concerns alleged violations of: 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receiving and Distributing/Conspiracy to Receive and Distribute Child Pornography; and 18 U.S.C. §

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

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 in 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)(1) 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)(1) 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.

DEFINITIONS 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)(1) 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 process 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.²

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 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,"

² 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.

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 “asdlk8fs9dfkku7f” 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”) muff7i44irws3mwu.onion.³ 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 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

³ 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

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

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

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 username, 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:

<u>Section – Forum</u>	<u>Topics</u>	<u>Posts</u>
General Category		
[the TARGET WEBSITE] information and rules		25 236
How to	133	863
Security & Technology discussion	281	2,035
Request	650	2,487
General Discussion	1,390	13,918
The INDEXES	10	119
Trash Pen	87	1,273
[the TARGET WEBSITE] Chan		
Jailbait ⁴ – Boy	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

⁴ Based on my training and experience, I know that "jailbait" refers to underage but post-pubescent minors.

Pre-teen Videos		
Girls HC ⁵	1,427	20,992
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	31	135
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

⁵ 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.

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 "tutu01" 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 turn, 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
- Scat⁶
- 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 provided information that the IP Address 192.198.81.106 was owned by Centrilogic, a server hosting company headquartered at 801 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 of Naples, 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.⁷

30. Accordingly, on February 19, 2015, FBI personnel executed a court-authorized

⁶ Based on my training and experience, "scat" refers to sexually explicit activity involving defecation and/or feces.

⁷ Due to a misconfiguration of the TARGET WEBSITE that existed for an unknown period of time, the true IP Addresses of a small number of users of the TARGET WEBSITE (that amounted to less than 1% of registered users

search at the Naples, 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 of TARGET 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

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

of the TARGET WEBSITE) were captured in the log files stored on the Centrilogic server.

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.⁸

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.

34. The NIT will reveal to the government environmental variables and certain registry-

⁸ 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 1 by engaging in substantial posting activity, or in particular areas of TARGET WEBSITE, such as the TARGET WEBSITE sub-

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

forums described in Paragraph 27.

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)(1) 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)(1) 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(f)(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.⁹

⁹ The United States considers this technique to be covered by law enforcement privilege. Should the Court wish to

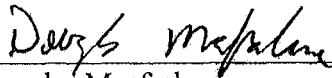
CONCLUSION

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

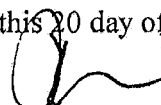
49. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of these crimes.

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.



Douglas Macfarlane
Special Agent

Sworn to and subscribed before me
this 20 day of February /s/


Theresa Carroll Buchanan
United States Magistrate Judge
Honorable Theresa Carroll Buchanan
UNITED STATES MAGISTRATE JUDGE

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.

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)(1) and or (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), 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.

AO 93 (Rev. 12/09) Search and Seizure Warrant

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)
upf45jv3bzuctml.onion)

Case No. 1:15-SW-89

UNDER SEAL

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 (name)

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 (check the appropriate box) for 30 days (not to exceed 30). until, the facts justifying, the later specific date of

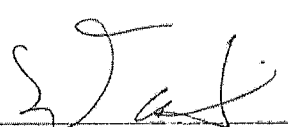
Date and time issued: 2/20/2015 11:45

Theresa Carroll Buchanan Judge's signature

City and state: Alexandria, Virginia

Honorable Theresa Carroll Buchanan, U.S. Magistrate Judge Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return		
Case No.: 1:15-SW-89	Date and time warrant executed: Between 2/20/15 and 3/4/15	Copy of warrant and inventory left with: N/A
Inventory made in the presence of: N/A		
Inventory of the property taken and name of any person(s) seized: Data from computers that accessed TARGET WEBSITE Between 2/20/15 and 3/4/15		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: <u>March 31, 2015</u>	 <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> Executing officer's signature	
	Special Agent FBI <u>Daniel I. Alfieri</u> Printed name and title	