APPENDIX

NOT FOR PUBLICATION

FILED

APR 9 2020

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. JOSE ANTONIO ACEVEDO-LEMUS, Defendant-Appellant.	No. 18-50324 D.C. No. 8:15-cr-00137-CJC-1 MEMORANDUM*

Appeal from the United States District Court
for the Central District of California
Cormac J. Carney, District Judge, Presiding

Submitted April 1, 2020**
Pasadena, California

Before: WARDLAW, MURGUIA, and MILLER, Circuit Judges.

Jose Antonio Acevedo-Lemus was sentenced to sixty months imprisonment and a lifetime term of supervised release following a conditional guilty plea for possession of child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B), 2252A(b)(2).

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

** The panel unanimously concludes this case is suitable for decision without oral argument. *See* Fed. R. App. P. 34(a)(2).

In January 2015, the Federal Bureau of Investigation ("FBI") seized the servers of "Playpen," an online child pornography bulletin board hosted on servers located in North Carolina, and began operating the website after moving the servers to FBI facilities in Newington, Virginia. Then, in February 2015, the FBI obtained a warrant from a magistrate judge in the Eastern District of Virginia authorizing use of a Network Investigative Technique ("NIT") to identify users of Playpen (the "NIT Warrant"). Using the information gathered from the NIT Warrant, agents then obtained a local warrant to search Acevedo-Lemus's residence. Acevedo-Lemus challenges the district court's denial of his motion to suppress evidence, arguing that the NIT Warrant was issued in violation of Federal Rule of Criminal Procedure 41(b), and that the local warrant was not supported by probable cause. We have jurisdiction under 28 U.S.C. § 1291 and we affirm.

1. Acevedo-Lemus acknowledges that his challenge to the NIT Warrant is foreclosed by our decision in *United States v. Henderson*, 906 F.3d 1109 (9th Cir. 2018). Indeed, *Henderson* addressed the precise warrant at issue here. In *Henderson*, we held that the NIT Warrant violated Federal Rule of Criminal Procedure 41(b), but that suppression was not required under the good-faith exception to the exclusionary rule. *Id. at* 1113–15. We see no reason to depart from that holding here.

2. Acevedo-Lemus does not establish good cause for his failure to

challenge the local warrant in the district court and therefore waived his right to challenge it on appeal. Under Federal Rule of Criminal Procedure 12, a "'theory for suppression not advanced in district court cannot be raised for the first time on appeal' absent a showing of good cause." *United States v. Guerrero*, 921 F.3d 895, 897–98 (9th Cir. 2019) (quoting *United States v. Keesee*, 358 F.3d 1217, 1220 (9th Cir. 2004)); *see also United States v. Restrepo-Rua*, 815 F.2d 1327, 1329 (9th Cir. 1987) (per curiam). Contrary to Acevedo-Lemus's contention, the suppression motion's passing reference to the local warrant in a section of the motion entitled "The NIT Warrant Violated the Warrant Clause's Particularity Requirement" did not adequately raise the issue. *See George v. Morris*, 736 F.3d 829, 837 (9th Cir. 2013) ("Although no bright line rule exists to determine whether a matter [has] been properly raised below, an issue will generally be deemed waived on appeal if the argument was not raised sufficiently for the trial court to rule on it." (quoting *In re Mercury Interactive Corp. Sec. Litig.*, 618 F.3d 988, 992 (9th Cir. 2010))). "[J]ust as a failure to file a timely motion to suppress evidence constitutes a waiver, so too does a failure to raise a particular ground in support of a motion to suppress." *United States v. Wright*, 215 F.3d 1020, 1026 (9th Cir. 2000) (quoting *Restrepo-Rua*, 815 F.2d at 1329).

3. But even if Acevedo-Lemus's challenge to the local warrant were reviewable, substantial evidence supports a finding of probable cause. The local

warrant established that Acevedo-Lemus: (1) became a registered member of Playpen, which is accessible only if the user knows the exact web address and installs appropriate software to connect to the network; (2) accessed Playpen for over eight hours; (3) viewed at least 175 threads on the website, two of which contained images of child pornography; and (4) accessed an additional post entitled "Mona" in the forum "Toddlers," which contained two embedded contact sheets with thumbnail images of a naked baby. Furthermore, the affidavit supporting the local warrant established that users had to take "numerous affirmative steps" to access Playpen, "making it extremely unlikely that any user could have simply stumbled upon [Playpen] without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography." Because probable cause "requires only a probability or substantial chance of criminal activity, *not an actual showing of such activity*," *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018) (emphasis added) (quoting *Illinois v. Gates*, 462 U.S. 213, 243–44 n.13 (1983)), we conclude that probable cause supported the local warrant.

AFFIRMED.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOSE ANTONIO ACEVEDO-LEMUS,

Defendant.

Case No.: SACR 15-00137-CJC

ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS

I. INTRODUCTION AND BACKGROUND

In December 2014, a foreign law enforcement agency advised the FBI that a known child pornography website called "Playpen" appeared to be associated with a

United States-based IP address.[1] (Dkt. 32 Ex. A at 6–37 ["Macfarlane Aff."] ¶ 28.) An ensuing investigation confirmed that Playpen was hosted by a server located in North Carolina. (*Id.*) The FBI obtained a search warrant for the location of the server in January 2015, seized the server, and found a copy of Playpen on it. (*Id.*)

Playpen operated as a "hidden service" located on an anonymity network known as "The Onion Router," or "Tor." (Macfarlane Aff. ¶¶ 6–7.) Ordinarily, public websites log the IP addresses of all visiting users. It is therefore an easy task for law enforcement to discover who has visited a certain website—or, alternatively, which websites a computer with a particular IP address has visited. The Tor network does not operate this way. Instead, to even access the network, a user must first download and install particular software, which subsequently shields the user's IP address by relaying it among "nodes"—computers run by volunteers all over the world. (*Id.* ¶ 8.) When a user visits a website located on the Tor network—like Playpen, for example—his actual IP address is not shown. Instead, Playpen can only see the IP address of the Tor "exit node"—the final relay computer which sent the user's communication to Playpen. (*Id.*) This deliberate concealment of IP addresses makes it exceptionally difficult for law enforcement to determine who has visited a website or hidden service located on the Tor network, as there is no practical way to trace a user's IP address back through the Tor nodes. (*Id.*)

Once on the Tor network, a user must know a website's particular web address to visit it. (He may not, as on the traditional or "open" Internet, simply perform an Internet search for certain material, since websites on the Tor network are not indexed like websites on the open Internet.) (Macfarlane Aff. ¶ 10.) Tor users must obtain web

[1] "An IP address is a number that an Internet Service Provider assigns to devices that are connected to the Internet. . . . The Internet Service Provider to which an internet user subscribes can correlate the user's IP address to the user's true identity." *Third Degree Films, Inc. v. John Does 1 through 4*, No. 12-CV-1849 BEN (BSG), 2013 WL 3762625, at *1 (S.D. Cal. July 16, 2013).

addresses from each other, or by viewing Internet postings describing the content available on certain websites. (*Id.*) The Tor network contains a "hidden service" page that is dedicated to pedophilia and child pornography, and Playpen's web address is listed on that page. (*Id.*) It would be highly unusual for a user to stumble upon Playpen. He would first have to elect to download Tor software and access the "dark web," where Tor websites are hosted, and then he would be required to affirmatively locate Playpen's web address before reaching Playpen.

Users who entered Playpen's web address arrived at a main page which contained images of two partially clothed prepubescent females with their legs spread apart, along with text stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." (Macfarlane Aff. ¶ 12.) This text apparently referred to a ban on posting material from other message boards, an indication of which file compression method was preferable, and instructions on what to include with posted materials. (*Id.*) Adjacent to the text were fields for users to enter login credentials, and a hyperlink for new users to "register an account with Playpen." (*Id.*) Upon clicking the "register an account" hyperlink, users were taken to additional text which explained that Playpen required an email address but that rather than entering their real email address, users should simply enter a made-up address: "something that matches the xxx@yyy.zzz pattern." (*Id.* ¶ 13.) Users who successfully registered for the service by entering a false email address were then taken to a page containing Playpen's forums and subforums. (*Id.* ¶ 14.)

Playpen was entirely devoted to the publication and exchange of child pornography. Its forums, where Playpen users could post materials, bore titles such as "Jailbait Videos"[2] (of both "Girls" and Boys"), "Pre-teen Videos," "Pre-teen Photos," and

[2] "Jailbait" refers to underage but post-pubescent minors.

"Webcams" (again, divided by gender), "Family Playpen – Incest," and "Toddlers." (Macfarlane Aff. ¶ 14.) Playpen also maintained a "Kinky Fetish" forum that included subforums like "Bondage," "Peeing," "Scat," "Spanking," "Voyeur," and "Zoo." (*Id.*) In addition to these forums and subforums, Playpen included three other important features. The first, called "Playpen Image Hosting," allowed Playpen users to upload links to images of child pornography. (*Id.* ¶ 23.) The links were then available to all registered Playpen users. (*Id.*) The second, "Playpen File Hosting," similarly allowed users to upload videos of child pornography, which were then available to Playpen registered users. (*Id.* ¶ 24.) The third, "Playpen Chat," permitted users to post links to child pornography for other users who were logged into Playpen Chat at the same time. (*Id.* ¶ 25.) The link to Playpen Chat was on Playpen's main index page. (*Id.*)

The FBI's review of Playpen's forums and subforums, as well as its Playpen Image Hosting, Playpen File Hosting, and Playpen Chat features, revealed links to numerous depictions of what appeared to be child pornography. A representative sampling of those depictions is as follows:

- An image of a prepubescent or early pubescent female being orally penetrated by the penis of a naked male. (Macfarlane Aff. ¶ 18.)
- A video of a prepubescent female, naked from the waist down, being anally penetrated by the penis of a naked adult male. (*Id.* ¶ 18.)
- Images focused on the nude genitals of a prepubescent female. (*Id.* ¶ 23.)
- A video of an adult male masturbating and ejaculating into the mouth of a nude prepubescent female. (*Id.* ¶ 24.)
- An image of two prepubescent females lying on a bed with their genitals exposed. (*Id.* ¶ 25.)
- An image of four females, including at least two prepubescent females, performing oral sex on one another. (*Id.* ¶ 25.)

A8

The FBI seized a copy of the server hosting Playpen in January 2015. (Macfarlane Aff. ¶ 28.) The nature of the Tor network, however, prevented the FBI from identifying Playpen users, since Playpen's "logs of member activity . . . contain[ed] only the IP addresses of Tor 'exit nodes' utilized by board users." (*Id.* ¶ 29.) Accordingly, on February 19, 2015, the FBI executed a court-authorized search at the Naples, Florida residence of the suspected administrator of Playpen. (*Id.* ¶ 30.) The administrator was apprehended, and the FBI managed to assume administrative control of Playpen. (*Id.*) The FBI then devised a plan to determine the identities of Playpen users: it would, while running Playpen from a server in Virginia, reconfigure the website to deploy a network investigative technique ("NIT") any time a user downloaded content from Playpen. (*Id.* ¶ 33.) As Douglas Macfarlane, an FBI Special Agent, subsequently explained,

> In the normal course of operations, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. [Upon deployment of the NIT, Playpen,] which will be located in Newington, Virginia, . . . would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from [Playpen], 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.

(Macfarlane Aff. ¶ 33.) Specifically, the NIT would reveal to the government seven items:

1. The activating computer's IP address, and the date and time that the NIT determined what that IP address was;
2. A unique identifier generated by the NIT to distinguish the data from that of other activating computers;
3. The type of operating system running on the computer;
4. Information about whether the NIT had already been delivered to the computer;

5. The activating computer's host name;
6. The activating computer's operating system username; and
7. The activating computer's Media Access Control ("MAC") address.

(*Id.* ¶ 34.)

On February 20, 2015, the FBI sought a warrant to deploy the NIT for thirty days. (Dkt. 32 Ex. A [the "NIT Warrant"].) The warrant application explained the nature of Playpen, the investigative difficulties presented by Playpen users' use of the Tor network, the operation of the NIT, and the fact that the NIT could cause activating computers—"wherever located"—to disclose the seven pieces of information noted above. (*See generally* Macfarlane Aff.; *see also id.* ¶ 48.) The warrant was signed by Theresa Carroll Buchanan, a United States Magistrate Judge for the Eastern District of Virginia. (NIT Warrant at 1.)

Deployment of the NIT Warrant revealed that a Playpen user with the username "DarkYogi" viewed at least 175 threads on Playpen during the deployment of the NIT, including at least two threads containing files that appeared to the government to be child pornography. (Dkt. 32 Ex. C at 1–30 ["Wrathall Aff."] ¶ 26.) The first file depicts a nude white prepubescent girl with her mouth open and her hand on an adult male erect penis that appears to be ejaculating into the girl's mouth. (*Id.*) The second file contains a visual depiction of a female white toddler with no pants on being vaginally penetrated by the erect penis of an adult male. (*Id.*) The NIT acquired the IP address of the user's computer, which—a search of publicly available websites revealed—was operated by Time Warner Cable. (*Id.* ¶¶ 27–28.) In March 2015, the government served an administrative subpoena on Time Warner, who indicated that the IP address in question was assigned to Defendant Jose Acevedo at a residence in Anaheim, California. (*Id.* ¶ 29.) The FBI confirmed that Defendant indeed lived at the Anaheim address and then

obtained a search warrant authorizing the search of Defendant's home for evidence of child pornography. (*Id.* ¶¶ 30–33; *see generally id.*) The FBI executed the search, interviewed Defendant, and seized a Hewlett Packard computer with a Western Digital hard drive and a SanDisk Cruzer thumb/flash drive. The hard drive and flash drive were found to contain 210 videos of child pornography and 31 still images of child pornography. A grand jury subsequently returned an indictment against Defendant for two counts of knowingly possessing child pornography. (*See* Dkt. 1.)

Defendant now moves for the suppression of all evidence stemming from the NIT Warrant. He argues that that warrant (1) violated the Fourth Amendment and (2) exceeded the magistrate's authority under Federal Rule of Criminal Procedure 41(b). (Dkt. 28.) The Court concludes that the FBI's acquisition of the key piece of information here—Defendant's IP address—was not a search under the meaning of the Fourth Amendment, and therefore did not require a warrant. The Court also concludes that in any event, suppression would not be an appropriate remedy for a Fourth Amendment violation in these circumstances. Accordingly, Defendant's motion is DENIED.

II. DISCUSSION

A. The NIT's Acquisition of Defendant's IP Address Was Not a Search

The Fourth Amendment to the U.S. Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." "As a prerequisite to establishing the illegality of a search under the Fourth Amendment, a defendant must show that he had a reasonable expectation of privacy in the place searched." *United States v. Heckencamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). A defendant may do so by demonstrating a "subjective expectation that his activities would be private [and that] his expectation was

one that society is prepared to recognize as reasonable." *United States v. Bautista*, 362 F.3d 584, 589 (9th Cir. 2004). Defendant can do neither here.

1. Defendant Lacked a Subjective Expectation of Privacy in His IP Address Because He Routinely Disclosed It to Others

First, Defendant could not have had a subjective expectation that his IP address[3] would remain private because he routinely disclosed it to third parties, including Time Warner, the Tor network, and websites he visited on the open Internet. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz v. United States*, 389 U.S. 347, 351 (1967). Applying this principle, the Ninth Circuit has on a number of occasions concluded that Internet users do not have reasonable expectations of privacy in their own IP addresses or the IP addresses of the websites they visit. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007) ("Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing information."); *Heckencamp*, 482 F.3d 1142, 1148 (holding that a defendant had "no reasonable expectation of privacy" in "network logs" that contained his computer's IP address); *United States v. Martinez*, 588 Fed. Appx. 741 (Mem.) (9th Cir. 2014) (unpublished) ("The use by law enforcement of proprietary forensic software packages that revealed information, such as hash values and IP addresses, did not make the search unlawful, as there was no reasonable expectation of privacy in this information[.] It was available to others, even though they may not have known how to view it."). Multiple

[3] Although the NIT seized seven pieces of information, the parties apparently agree that the crucial piece of information was Defendant's IP address. The warrant to search Defendant's home makes clear that it was this information, not anything else identified by the NIT, that led the FBI to Defendant. (Wrathall Aff. ¶¶ 7; 27–33.) The search warrant did not rely on any of the other six pieces of information, and the Court will limit its analysis to the fruits of the IP address.

district courts who have entertained motions to suppress evidence stemming from the NIT Warrant are in accord. *United States v. Matish*, --- F. Supp. 3d. ----, 2016 WL 3545776, at *21 (E.D. Va. June 23, 2016) (holding that the FBI "did not need to obtain a warrant before deploying the NIT" because the defendant had "no reasonable expectation of privacy in his IP address"); *United States v. Werdene*, --- F. Supp. 3d ----, 2016 WL 3002376, at III.B (E.D. Pa. May 18, 2016) (holding that because the defendant "did not have a reasonable expectation of privacy in his IP address, the NIT cannot be considered a 'search' within the meaning of the Fourth Amendment"); *United States v. Michaud*, Case No. 3:15-cr-05351-RJB, 2016 WL 337263, at *7 (W.D. Wash. Jan. 28, 2016) ("[The defendant] has no reasonable expectation of privacy of [sic] the most significant information gathered by deployment of the NIT, [his] assigned IP address[.]"); *but see United States v. Darby*, --- F. Supp. 3d ----, 2016 WL 3189703, at *6 (E.D. Va. June 3, 2016) (concluding that the NIT constituted a search, but noting that the government did not argue otherwise); *United States v. Arterbury*, Case No. 15-CR-182-JHP (N.D. Okla. Apr. 25, 2016) (report and recommendation) (concluding that the defendant had a reasonable expectation of privacy in his IP address because the government obtained the information from his computer, and not from a third party).

Two peculiar facts in this case—first, that the FBI obtained Defendant's IP address from his computer, not from a third party, and second, that Defendant *attempted* to obscure his IP address by using the Tor network—do not alter this conclusion.

First, it does not matter that the government procured Defendant's IP address from his computer as opposed to getting it from a third party because an IP address is not a private physical feature of a computer, but a commonly disclosed digital one assigned by a third party. When a consumer purchases a computer, takes it home, opens it up, and turns it on, that computer does not have an IP address. Instead, it is assigned an IP address by an internet service provider (like Time Warner) when it connects to a

particular network, and that IP address may change if the computer connects to a different network. *See Matish*, 2016 WL 3545776, at *21 ("[The defendant's] IP address was not located on his computer, indeed, it appears that computers can have various IP addresses depending on the networks to which they connect."). It is not completely accurate to say that the government accessed Defendant's computer to retrieve his IP address, as the IP address is not a physical component of the computer. Instead, when Defendant downloaded content from Playpen, the government sent along some code that directed Defendant's computer to disclose to the government a feature of Defendant's connection—his IP address. *Cf. id.* at *21 ("[The defendant's] IP address was revealed in transit when the NIT instructed his computer to send other information to the FBI."). And—crucially—the FBI was only able to deploy the NIT to Defendant's computer *after Defendant sought Playpen out*. The FBI did not come looking for Defendant. Instead, it waited until he came to them and engaged in illicit activity by downloading content from Playpen. The government allowed him to download that content but also sent him home with an unexpected souvenir: code that would reveal his IP address.

In that sense this case is very much like *United States v. Knotts*, 460 U.S. 276 (1983). There, the government—with a storeowner's consent—installed a "beeper" in a drum of chloroform subsequently purchased by an individual whom the government suspected of drug production. *Id.* at 277. After the drum was purchased and placed in the trunk of a vehicle, agents followed the vehicle, both maintaining visual contact and monitoring electronic signals from the beeper. *Id.* at 278. Eventually, the vehicle made "evasive maneuvers," and both visual and electronic contact were lost. *Id.* A helicopter with another monitor later picked up the signal, however, and tracked it to a cabin. *Id.* After performing additional surveillance of the cabin, the government obtained a residential search warrant, based on part on the electronic tracking of the chloroform drum. *Id.* The search revealed a drug lab, and the defendant moved to suppress, arguing that the tracking of the beeper was an unreasonable search.

The Supreme Court refused to suppress the evidence. It explained that the government had made "limited use" of the beeper, acquiring only information that the driver of the vehicle had "voluntarily conveyed" to the public—namely, the location of the vehicle and its ultimate destination. *Id.* at 281. (Nothing in the record indicated that the government had received or relied upon beeper signals after concluding that the "drum containing the chloroform had ended its automotive journey," *id.* at 284–85.) True, the "failure of visual surveillance" meant that the beeper gave law enforcement officials information they could not have acquired otherwise. *Id.* at 285. The crucial fact in the Supreme Court's view, however, was that the information law enforcement *did* acquire was ordinarily public, and "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them." *Id.* at 282. And although the *Knotts* Court warned that "dragnet type law enforcement practices" involving the use of beepers may present a more difficult constitutional question, it concluded that the government's monitoring of the beeper constituted neither a search nor a seizure under the meaning of the Fourth Amendment. *Id.* at 285.

Knotts was recently distinguished by *United States v. Jones*, where the Supreme Court ruled that the warrantless installation of a GPS tracker on a suspect's car was a search. 132 S. Ct. 945 (2012). That case was different from *Knotts*, the Supreme Court explained, in two ways. First, the beeper in *Knotts* was installed in the drum of chloroform *before* the drum came into the defendant's possession. In *Jones*, by contrast, the GPS device was installed on a car already owned and possessed by the defendant's wife. *Jones*, 132 S. Ct. at 952 (reasoning that "Jones, who possessed the Jeep at the time the Government trespassorily inserted the information-gathering device, [wa]s on much different footing" from the defendants in *Knotts* and another beeper case, *United States v. Karo*, 468 U.S. 705 (1984).) Second, the *Jones* Court noted the *Knotts* Court's emphasis on the "limited use" of the beeper, as well as its reservation of the constitutionality of

warrantless "dragnet type law enforcement practices," *see Knotts*, 460 U.S. at 284. *Jones*, the Supreme Court said, involved a long-term, "dragnet-style" search and was therefore not a "limited use" case like *Knotts*. *Jones*, 132 S. Ct. at 952 n.6.

These two distinctions illustrate why *Knotts*, not *Jones*, is the correct analogue in this case. First, as in *Knotts*, the information-gathering technique used here was originally installed on something controlled by the government—Playpen content—and only then transferred to Defendant's computer, *at Defendant's request*. Defendant is therefore "on much different footing" than the defendant in *Jones*, 132 S. Ct. at 952, and instead is like the defendant in *Knotts* who unknowingly purchased the bugged chloroform. And second, the NIT obtained *very* limited information from Defendant's computer. It did not, for example, search for files containing child pornography or otherwise inspect the computer's contents. Indeed, its crucial operation was only to acquire a piece of information, normally public and often disclosed to third parties, that Defendant had managed to successfully obscure from the FBI: his IP address.

It also does not matter that Defendant tried to shield his IP address from the government, since he nonetheless disclosed that information to the initial Tor "entry node." As the *Werdene* court explained, "a necessary aspect of Tor is the initial transmission of a user's IP address to a third-party"—the operator of the initial Tor node—and the fact that a user's IP address is "subsequently bounced from node to node within the Tor network to mask his identity does not alter the analysis of whether he had an actual expectation of privacy in that IP address," which he had initially disclosed to a stranger. *Werdene*, 2016 WL 3002376, at III.A; *see also United States v. Farrell*, No. CR15-029RAJ, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016) (holding that a defendant had no expectation of privacy in his IP address, which he concealed through Tor, because "in order for a prospective user to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes").

Here again, *Knotts* is on point. Just as the Supreme Court would not countenance the possibility that the *Knotts* defendant's "evasive" driving maneuvers could permit him to escape law enforcement's technological tools, so too Defendant may not escape responsibility here merely because he managed to disclose his IP address to Tor but not to the government. That result was unacceptable more than thirty years ago in *Knotts*, and it is unacceptable today. Mere disclosure by a computer of its IP address—a hallmark of Internet communication—does not become a Fourth Amendment search when the government happens to be the party to whom disclosure occurs. Simply put, Defendant could not have had a subjective expectation of privacy in his IP address.

2. Society Does Not Recognize Defendant's Expectation as Reasonable

Defendant also cannot demonstrate that any subjective expectation of privacy he may have had in his IP address is an expectation that "society is prepared to recognize as 'reasonable,'" *Katz*, 389 U.S. at 361. Defendant opened his computer, got on the Internet, and went searching for child pornography. In an attempt to evade detection by law enforcement, he used Tor, hoping to mask his IP address from government investigators. American society abhors child pornography, and it does not view Defendant's deceptive efforts to conceal his viewing of child pornography as establishing a reasonable expectation of privacy. *Werdene*, 2016 WL 3002376, at III.B (noting that the defendant's "use of Tor to view and share child pornography is not only an activity that society rejects, but one that it seeks to sanction"); *Matish*, 2016 WL 3545776, at *24 ("Society thus is unprepared to recognize any privacy interests [the defendant] attempts to claim as reasonable in his search for pornographic material."); *cf. Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) ("[A] burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate.'"). Contrary to his assertions, Defendant cannot conceal his deviant behavior through Internet tricks. *Werdene*, 2016 WL 3002376, at

III.B (rejecting the defendant's attempt to "serendipitously receive Fourth Amendment protection because he used Tor in an effort to evade detection"); *Matish*, 2016 WL 3545776, at *24 ("[The defendant] should not be rewarded for allegedly obtaining contraband through his virtual travel through interstate commerce on a Tor hidden service."). Indeed, this Court agrees with the *Matish* court that the government "should be able to use the most advanced technological means to overcome criminal activity that is conducted in secret." *Matish*, 2016 WL 3545776, at *24. Law enforcement cannot afford to be hamstrung by technologically creative criminals, especially when what is at risk is the sexual exploitation and sadistic abuse of children.

B. Suppression is Unwarranted in Any Event

Suppression would not be the proper remedy regardless of whether the FBI's deployment of the NIT was a search. "[S]uppression is not an automatic consequence of a Fourth Amendment violation. Instead, the question turns on the culpability of the police and the potential of exclusion to deter wrongful police conduct." *Herring v. United States*, 555 U.S. 135, 137 (2009). Defendant argues that the evidence stemming from the NIT Warrant must be suppressed because the NIT Warrant inappropriately authorized an out-of-district search of his computer.[4] *See* Fed. R. Crim. P. 41(b) ("[A]

[4] Defendant's alternative argument—that the NIT Warrant failed the Fourth Amendment's particularity requirement—is without merit. That argument has been rejected, as near as the Court can tell, by every federal court to consider it. *See, e.g.*, *Matish*, 2016 WL 3545776, at *14 (finding that "the NIT Warrant did not violate the Fourth Amendment's particularity requirement" because "there existed a fair probability that anyone accessing Playpen possessed the intent to view and trade child pornography"); *Michaud*, 2016 WL 337263, at *5 ("Although the FBI may have anticipated tens of thousands of potential suspects as a result of deploying the NIT, that does not negate particularity, because it would be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor network."); *United States v. Epich*, Case No. 15-CR-163-PP, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016) (concluding that the NIT Warrant satisfied the particularity requirement because it "explained who was subject to the search, what information the NIT would obtain, the time period during which the NIT would be used, and how it would be used, as well as bearing attachments describing the place to be searched and the information to be seized").

magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district."). He is incorrect.

1. Any Rule 41 Violation Does Not Require Suppression

In the Ninth Circuit, suppression is only available for Rule 41 violations if "1) the violation rises to a constitutional magnitude; 2) the defendant was prejudiced, in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule; or 3) officers acted in intentional and deliberate disregard of a provision in the Rule." *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005). For reasons the Court has already explained, no violation of "constitutional magnitude" has occurred here because Defendant had no reasonable expectation of privacy in his IP address. *See Werdene*, 2016 WL 3002376, at III.B ("Since [the defendant] did not have a reasonable expectation of privacy in his IP address, . . . the violation [of Rule 41] is therefore not constitutional."). Nor was Defendant prejudiced by any potential Rule 41 violation. After all, the FBI *could* have installed copies of Playpen in every judicial district in the country (there are 94) and then secured a corresponding number of Rule 41 warrants. It only chose not to do so because of the enormous burden and expense of such an undertaking. But the fact remains that the issuance of a modified NIT Warrant that fully complied with even a narrow reading of Rule 41 was entirely possible. Defendant's argument that he was prejudiced by this search boils down to an assertion that his consumption of child pornography was totally immunized by his use of Tor, and there was nothing the government could do about it. Not so.

Finally, there is no reason to believe that the FBI intentionally and deliberately violated Rule 41 by seeking the NIT Warrant. As an initial matter, there are credible arguments to be made that Rule 41 was never violated at all, casting doubt on Defendant's assertion that the FBI was knowingly flouting the Rule. Rule 41(b)(4), for

example, provides that a magistrate judge may "issue a warrant to install within the district a tracking device" and that 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[.]" It is not a stretch to say that the NIT functioned as a permissible "tracking device" attached to child pornography that was subsequently downloaded by Defendant when his computer sent a request to the Playpen server. Indeed, at least two district courts have agreed with this position. *See Matish*, 2016 WL 3545776, at *18 ("[T]he NIT Warrant authorized the FBI to install a tracking device on each user's computer when that computer entered the Eastern District of Virginia . . . [w]hen that computer left Virginia—when the user logged out of Playpen—the NIT worked to determined its location . . . all relevant events occurred in Virginia."); *United States v. Darby*, --- F. Supp. 3d ----, 2016 WL 3189703, at *12 (E.D. Va. June 3, 2016) (holding that Rule 41(b)(4) authorized the NIT Warrant because "[u]sers of Playpen digitally touched down in the Eastern District of Virginia" and the FBI was then entitled to install a tracking device); *but see Michaud*, 2016 WL 337263, at *6 (rejecting the argument that Rule 41(b)(4) permitted the NIT Warrant); *United States v. Levin*, --- F. Supp. 3d ----, 2016 WL 2596010, at *6 (D. Mass. May 5, 2016) (same). The fact that courts are presently divided over whether the NIT Warrant even violated Rule 41 is compelling evidence that the FBI did not intentionally and deliberately violate that Rule by seeking the warrant in the first instance.

Moreover, as the government points out, the Supreme Court has recently recommended that Rule 41 be modified to explicitly permit magistrate judges to "issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media is located has been concealed through technological means." (Dkt. 38 Ex. B at 6.) Defendant takes this proposed amendment to mean that the FBI knew it was operating outside Rule 41. But the amendment actually cuts the other way. It would be

strange indeed for the Court to suppress the evidence in this case in the face of a strong signal from the Supreme Court that Rule 41 should explicitly permit the issuance of warrants like the NIT Warrant. The severe penalty of suppression should not be levied against the government (and society generally) merely because the government had the good sense to seek an amendment to Rule 41.

2. The Good Faith Exception Applies

Even in the presence of a violation, the good faith exception to the exclusionary rule would bar suppression here.[5] Application of the exclusionary rule is only appropriate in those "unusual cases" where suppression will "deter police misconduct." *United States v. Leon*, 468 U.S. 897, 916, 918 (1984). When police officers "acting with objective good faith ha[ve] obtained a search warrant from a judge or magistrate and acted within its scope," there is "no police illegality and thus nothing to deter." *Id.* at 920–21.

Here, Defendant's technical sophistication meant that to adequately prosecute the child pornography laws, FBI agents were required to design a tool that was up to the task. The NIT was the solution. FBI agents were, at every juncture, up front with the magistrate judge about how the NIT worked, what it would seize from "activating computers," and where "activating computers" could be located. (Macfarlane Aff. ¶ 48.) That Rule 41 may not yet be a perfect fit for our technological world does not mean that the FBI agents here acted in bad faith.

[5] Traditional limitations on the exclusionary rule, like the good faith exception and the balancing of the costs of suppression against any violation, still apply in the Rule 41 context, since the suppression provisions of Rule 41 are "no broader than the constitutional rule," *Alderman v. United States*, 394 U.S. 165, 173 n.6 (1969).

The costs of suppression also weigh against that remedy in this case. Defendant proposes that he and other viewers and distributors of child pornography can escape capture and continue their viewing and distribution so long as they use Tor, while society and the children victimized by their behavior continue to suffer. That would be repugnant to justice and the purpose of law. As the Supreme Court has explained,

> The [good faith] analysis must also account for the substantial social costs generated by the [exclusionary] rule. Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. Our cases hold that society must swallow this bitter pill when necessary, but only as a last resort. For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.

Davis v. United States, 564 U.S. 229, 237 (2011) (internal citations and quotation marks removed). Considering the unspeakable harm caused by child pornography, and the creative and limited conduct of the FBI that was undertaken to mitigate that harm, the Court has no trouble concluding that suppression is entirely unwarranted here.

III. CONCLUSION

For the foregoing reasons, Defendant's motion to suppress is DENIED.

DATED: August 8, 2016

CORMAC J. CARNEY
UNITED STATES DISTRICT JUDGE

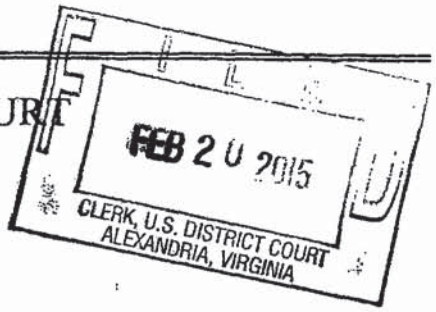
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH	)	FILED UNDER SEAL
OF COMPUTERS THAT ACCESS	)	
upf45jv3bziuctml.onion	)	Case No. 1:15-SW-89

ATTACHMENT A

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
upf45jv3bziuctml.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)*:

- ☑ 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:

Code Section	*Offense Description*
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.

- ☑ Continued on the attached sheet.
- ☑ 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

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

Honorable Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

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

Case No. 1:15-SW-89

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

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

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

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:

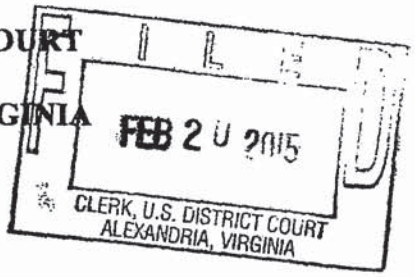
1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will 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 progress to restore it.

j. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

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

m. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the Internet Service Provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static,"

if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

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

o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

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

any person. See 18 U.S.C. § 2256(2).

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

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

PROBABLE CAUSE

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

The Tor Network

7. The TARGET WEBSITE operates on an anonymity network available to Internet users known as "The Onion Router" or "Tor" network. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of

protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.[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 "asdlk8fs9dflku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

Finding and Accessing the TARGET WEBSITE

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

purpose and content. In addition, upon arrival at the TARGET WEBSITE, the user sees images of prepubescent females partially clothed and whose legs are spread with instructions for joining the site before one can enter. Accordingly, there is probable cause to believe that, for the reasons described below, any user who successfully accesses the TARGET WEBSITE has knowingly accessed with intent to view child pornography, or attempted to do so.

Description of the TARGET WEBSITE and Its Content

11. Between September 16, 2014 and February 3, 2015, FBI Special Agents operating in the District of Maryland connected to the Internet via the Tor Browser and accessed the Tor hidden service the TARGET WEBSITE at its then-current Uniform Resource Locator ("URL") 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:

Section – Forum	Topics	Posts	
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 [redacted] posted a topic entitled [redacted] 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 [redacted] posted a topic entitled [redacted] 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 [redacted] posted a topic entitled [redacted] 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 [redacted] which was created by the TARGET WEBSITE user [redacted] 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 [redacted] which was created by the TARGET WEBSITE user [redacted] 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 '[redacted] 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 [redacted] posted a link to an image that depicted a prepubescent female with an amber colored object inserted into her vagina.

User [redacted] posted a link to an image that depicted two prepubescent females laying on a bed with their legs in the air exposing their nude genitals.

Other images that appeared to depict child pornography were also observed.

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

THE TARGET WEBSITE SUB-FORUMS

27. While the entirety of the TARGET WEBSITE is dedicated to child pornography, the following sub-forums of the TARGET WEBSITE were reviewed and determined to contain the most egregious examples of child pornography and/or dedicated to retellings of real world

hands on sexual abuse of children.

- Pre-teen Videos - Girls HC
- Pre-teen Videos - Boys HC
- Pre-teen Photos - Girls HC
- Pre-teen Photos - Boys HC
- Potpourri - Toddlers
- Potpourri - Family Play Pen - Incest
- Spanking
- Kinky Fetish - Bondage
- Peeing
- Scat[6]
- 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 [redacted] a server hosting company headquartered at [redacted] 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 [redacted] 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 [redacted] 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.

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* OF COMPUTERS THAT ACCESS upf45jv3bziuctml.onion	)	Case No. 1:15-SW-89 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

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

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

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
1:15-SW-89	Between 2/20/15 and 3/4/15	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

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: March 31, 2015

Executing officer's signature

Special Agent FBI Daniel I. Alfin

Printed name and title

UNDER SEAL

UNITED STATES DISTRICT COURT

for the

Central District of California

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

[redacted]
Anaheim, California 92805

Case No. SA15-386M

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 Central District of California, 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)*:

- ☑ 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:

Code Section	*Offense Description*
Title 18 U.S.C. §§ 2252A(a)(5)(B), (b)(2)	See attached Affidavit

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ 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.

/s/
Applicant's signature

FBI SA STEVEN WRATHALL
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/21/2015

DOUGLAS F. McCORMICK
Judge's signature

City and state: Santa Ana, CA

HON. DOUGLAS F. McCORMICK U.S. Magistrate Judge
Printed name and title

AUSA: J. Wafer

LODGED
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
2015 JUL 21 PM 2:03

AFFIDAVIT

I, Steven Wrathall, being duly sworn, do hereby state:

I.

INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and I have been so employed since February 2009. I am currently assigned to the Los Angeles Office, Orange County Resident Agency. As part of the Child Exploitation Task Force ("CETF"), I investigate, among other things, federal child pornography and child sexual exploitation crimes in the Central District of California. I received training in the investigation of crimes against children during my attendance at the FBI Academy in Quantico, Virginia. In addition, I have received hours of additional related classroom training and have participated in numerous investigations of criminal activity, including the investigation of crimes against children, violent crimes, and cybercrimes.

II.

PURPOSE OF AFFIDAVIT

2. This affidavit is submitted in support of an application for a warrant to search [redacted] Anaheim, California 92805 (the "SUBJECT PREMISES"), more fully described below in paragraph 4 and in Attachment A, to seize evidence, fruits, and instrumentalities, as specified in paragraph 5 and in Attachment B, of violations of 18 U.S.C. §§ 2252A(a)(5)(B), (b)(2) (access, or attempt to access, with intent to view child pornography).

3. The facts set forth in this affidavit are based in part on my personal observations, training, and experience investigating child pornography crimes. The facts set forth in this affidavit related to the investigation of Website A and activity on Website A related to the user

DarkYogi were provided to me by Special Agents of the FBI in the Violent Crimes Against Children Unit, Criminal Investigations Division, in Washington, D.C. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

III.

PREMISES TO BE SEARCHED

4. The SUBJECT PREMISES is described here and in Attachment A as follows:

a. The property located at [redacted] Anaheim, California 92805. The SUBJECT PREMISES is a single story single family residence that has greenish color stucco with white trim, a white garage door, and a brown shingled roof. The SUBJECT PREMISES is on the west side of [redacted] Street with the front door and garage door facing east. The numbers "[redacted]" are painted in black numbering on a white background on the curb in front of the SUBJECT PREMISES.

IV.

ITEMS TO BE SEIZED

5. The items to be seized as evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(5)(B), (b)(2), are described in detail in Attachment B, which is incorporated herein by reference.

V.
DEFINITIONS

6. The following definitions apply to this Affidavit and attachments hereto:

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

Instrumentality Protocol

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 Website Administrator.

b. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

d. "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.

e. "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."

f. "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.

g. "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).

h. "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.

i. "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.

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

k. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

l. "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.

m. "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.

n. 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.

o. "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 Internet Service Provider ("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.

p. "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 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.

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

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

s. 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

Instrumentality Protocol

("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).

t. "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

u. "Sexually explicit conduct" is defined in 18 U.S.C. § 2256(2).

v. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

w. "Visual depictions" is defined in 18 U.S.C. § 2256(5).

x. "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").

VI.

SUMMARY

7. A user of the Website A Internet account, with an IP address that returned to [redacted] Anaheim, California 92805 has been linked to an online community of individuals who regularly share child pornography for viewing and downloading on a website that operated on an anonymous Internet network. The website is described below and referred to

Instrumentality Protocol

herein as Website A.[1] Based on records of account activity for a user of Website A obtained by the FBI, there is probable cause to believe that a user of the Website A Internet account, with an IP address that returned to [redacted] Anaheim, California 92805, knowingly accessed with intent to view child pornography on Website A.

VII.

PROBABLE CAUSE

A. The Network

8. Website A operated on a network ("the Network") available to Internet users who are aware of its existence.[2] 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

---

[1] While the actual name of Website A is known to law enforcement, the FBI is still investigating users of Website A, including user **DarkYogi**. Disclosure of the name of Website A in this search warrant application could alert Website A's users to the existence of the Website A investigation, potentially provoking members to notify other members of the investigation, to flee, or to destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, in this affidavit I refer to Website A anonymously and describe it in generic terms.

[2] Like the actual name of Website A, 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, or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, in this affidavit I refer to the Network anonymously and describe it in generic terms.

[3] Users may also access the Network through so-called "gateways" on the open Internet,

Instrumentality Protocol

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.

9. 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 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.

---

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 have known the exact IP address of the computer server that hosted Website A, which information was not publicly available. As of on or about February 20, 2015, Website A was no longer accessible through the traditional Internet.

10. 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.

11. 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.

B. Description of Website A and its Content

12. 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

Instrumentality Protocol

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.

13. 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 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."

14. 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

Instrumentality Protocol

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.

15. 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.

16. 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.

17. 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

Instrumentality Protocol

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.

18. 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.

19. 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.

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.

20. 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.

21. 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.

22. Text sections of Website A provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse. For example, 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

Instrumentality Protocol

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..."

C. Court Authorized Use of Network Investigative Technique

23. 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.

24. 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.

25. 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

Instrumentality Protocol

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.

D. DarkYogi's Access to and Activity on Website A

26. According to data logs obtained pursuant to a search warrant on the server hosting Website A, information obtained by law enforcement monitoring Website, and information obtained through the deployment of a NIT as described above in paragraph 25—all of which was provided to me by FBI Special Agents in the Violent Crimes Against Children Unit, Criminal Investigation Division, in Washington, D.C.—a user with the user name **DarkYogi** engaged in the following activity on Website A.

a. User **DarkYogi** registered and was first active on Website A on February 1, 2015.

b. User **DarkYogi** last visited Website A on March 4, 2015.

c. Between the dates of February 1, 2015, and March 4, 2015, user **DarkYogi's** total time logged onto Website A was 8 hours, 5 minutes, 37 seconds.

d. Between February 22, 2015, and March 4, 2015, user **DarkYogi** viewed at least 175 threads on Website A. At least two of the threads viewed by user **DarkYogi** contained files that appear to contain child pornography

i. February 26, 2015, the user **DarkYogi** accessed a thread which contained images in a file entitled *114269ee389a90d87bf656147de3083b.jpg*. I have viewed this image file, a copy of which was provided to me by FBI Special Agents as indicated above, and observed that it contains a visual depiction of a nude white prepubescent girl with her mouth open and her hand on an adult male erect penis that appears to be ejaculating in her mouth.

ii. On March 3, 2015, the user **DarkYogi** accessed a thread which contained an image file entitled *24607553_18.jpg*. I have viewed this image file, a copy of which was provided to me by FBI Special Agents as indicated above, and observed that it contains a visual depiction of a female white toddler with no pants on and legs spread open. An adult white male has his erect penis in the vagina of the toddler.

E. IP Address and Identification of User analysis on Website A

27. According to data logs obtained pursuant to a search warrant on the server hosting Website A, information obtained by law enforcement monitoring Website A, and information obtained through the deployment of a NIT as described above in paragraph 25, on February 25,

Instrumentality Protocol

2015, the user **DarkYogi**, using IP address 76.89.183.187, accessed a Website A post entitled "Mona" in the forum "Toddlers." This post contained two embedded contact sheets with thumbnail images of a naked baby. Other users of Website A replied to this post, including one user who remarked about the pictures: "Nice thumbnails of the naked baby at least."

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) Time Warner Cable.

29. In March 2015, an administrative subpoena was served on Time Warner Cable requesting information related to the user who was assigned to the above IP address. According to the information received from Time Warner Cable, Jose Acevedo is receiving Internet service at [redacted] Anaheim, California 92805, with an installation date of May 30, 2014. Internet service was current as of March 6, 2015, at the aforementioned premises.

30. On or about July 20, 2015, I reviewed a National Comprehensive Report ("NCR") records check for "Jose Acevedo." NCR is a report generated by Thomson Reuters, a company that consolidates public records, including addresses, driver licenses, property deed transfers, and corporate information. From my review I learned that the current address listed for a "Jose Acevedo" is the SUBJECT PREMISES.

31. On or about July 20, 2015, I reviewed NCR records for the address [redacted] Anaheim, California 92805, i.e., the SUBJECT PREMISES, and learned that "[redacted]" and "[redacted]" are listed in NCR as residing at the SUBJECT PREMISES.

32. On or about July 20, 2015 I reviewed a California Department of Motor Vehicles (DMV) database report for "Jose Acevedo." The query returned one record for an individual named Jose Acevedo who lists [redacted] Anaheim, California 92805 as of April 25, 2013.

33. On or about July 20, 2015, I drove by the SUBJECT PREMISES and observed a silver Toyota four door car parked in the driveway of the SUBJECT PREMISES bearing California License plate "[redacted]". I reviewed the DMV registration information for "[redacted]" and learned that the vehicle is registered to "Jose Acevedo" and lists the SUBJECT PREMISES as the current address on file.

VIII.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW AND COLLECT CHILD PORNOGRAPHY

34. Based on my experience investigating child pornography crimes, and the training and experience of other law enforcement officers with whom I have had discussions about child pornography crimes, I know there are certain characteristics common to individuals who utilize web-based bulletin boards to access with intent to view child pornography:

a. Such persons frequently maintain collections of child pornographic materials, often in a digital or electronic format, in a safe, secure and private environment, such as in their residence or on a personal computer or external digital storage media. These collections are often maintained for several years and are kept close by, usually at the person's residence or inside the person's vehicle, to enable the person to view the collection.

b. Such persons frequently correspond with others to share information and materials; rarely destroy correspondence from other child pornography distributors; conceal such correspondence; 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.

c. Such persons prefer not to be without their child pornography for any prolonged time period.

VIII.

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

Instrumentality Protocol

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.

IX.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES

42. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as

Instrumentality Protocol

modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of

text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

43. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

X.

REQUEST FOR AUTHORITY FOR NO KNOCK EXECUTION

44. The rules posted on Website A by the primary administrator state that all material shared via Website A must be encrypted. On September 16, 2014, an administrator of Website A created a topic entitled, "Windows Security Guide." The topic contained, among other information, instructions on securely deleting data and creating encrypted partitions. Specifically, the administrator instructed users to, "install and keep everything cp related, including [the Network software] and programs on the Truecrypt container." The post contained numerous additional instructions for modifying or disabling features of the operating system that may assist investigators performing forensic exams on seized computers.

45. Based upon the totality of the information in this affidavit as well as my training and experience, I believe that there is a reasonable probability that the subject under investigation uses encryption software which, if activated, may prevent law enforcement from obtaining the information stored in the computers which are subject to seizure. If, at the time agents enter to execute this search warrant, an encrypted computer is powered off or locked, then the encryption would be activated and it would be difficult or impossible to search that device without the necessary password or pass-phrase. I am aware of instances where law enforcement has encountered an encrypted device or devices during the course of a court-authorized search of a residence, and been unable to search the device(s). To avoid the scenario where agents encounter an encrypted computer or computers, agents will attempt to execute this warrant at a time when

the subject under investigation is home and computers at the subject location are up and running and being used to send or receive data over the Internet. Precautions also need to be taken to ensure that the subject under investigation does not activate encryption when agents arrive at the home to serve the warrant. Activating that encryption can be as simple as pressing a button on a computer or powering a computer down, which takes a matter of seconds. Accordingly, if the subject under investigation or others in the premises is aware of the search prior to the actual entry of the agents who are conducting the search, the encryption software can therefore be easily activated. Accordingly, in order to minimize the possibility that agents will encounter encrypted computers, your Affiant respectfully requests that this warrant be a "no knock" and "day and/or night hours" warrant, allowing agents to make a dynamic entry into the residence, in order to prevent the activation of encryption software, at any time of the day or night at which agents can determine that the subject under investigation is home and data is being sent/received via the Internet.

46. According to information I received from Special Agents of the FBI in the Violent Crimes Against Children Unit, Criminal Investigations Division, "no knock" and "day or night hours" warrants were successfully used in this investigation. For example, on February 20, 2015, the primary administrator of Website A was arrested by the FBI after the execution of a "no knock" and "day or night hours" warrant. After the administrator was detained, on-scene personnel determined that he had stored data pertaining to Website A on an encrypted device. Due to the fact that the FBI had a "no knock" and "day or night hours" warrant in that situation, the FBI successfully seized the evidence pertaining to Website A that likely otherwise would have been encrypted.

XI.

CONCLUSION

47. Based upon the foregoing, I believe that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C.§§ 2252A(a)(5)(B), (b)(2), as described above and in Attachment B of this affidavit, will be found at the SUBJECT PREMISES.

/S/

Steven Wrathall, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 21st day of July, 2015.

DOUGLAS F. McCORMICK

HON. DOUGLAS F. McCORMICK
United States Magistrate Judge

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is the property located at [redacted] Anaheim, California 92805. The SUBJECT PREMISES is a single story single family residence that has greenish color stucco with white trim, a white garage door, and a brown shingled roof. The SUBJECT PREMISES is on the west side of [redacted] with the front door and garage door facing east. The numbers "[redacted]" are painted in black numbering on a white background on the curb in front of the SUBJECT PREMISES.

ATTACHMENT B

I.

NO KNOCK AND NIGHTTIME SERVICE

The searching agents and officers need not knock and announce their presence prior to entry. The warrant may be executed at any time in the day or night.

II.

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(5)(B), (b)(2) (access, and attempted access, with intent to view child pornography), namely:

a. Records, documents, programs, applications or materials evidencing access or attempted access with intent to view Website A, as described in paragraph 3 of the affidavit supporting this search warrant.

b. Records, documents, programs, applications or materials evidencing use of the Network, as described in paragraphs 8 through 11 of the affidavit supporting this search warrant.

c. Records, documents, programs, applications or materials containing or depicting child pornography, as defined in 18 U.S.C. § 2256.

d. Records, documents, programs, applications or materials that do not constitute child pornography under 18 U.S.C. § 2256 but which evidence a sexual interest in minors, such as articles about child development, sex education, child pornography, and pedophilia; writings (whether fiction or non-fiction) describing sexual activity between adults and minors; and photographs, movies, and visual depictions of minors simulating sexual activity.

e. Records, documents, programs, applications or materials evidencing knowledge or awareness of law enforcement techniques used in investigating child pornography crimes.

f. No more than five records, documents, programs, applications or materials tending to identify the resident or resident(s) of the SUBJECT PREMISES.

g. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

h. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device 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, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, 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;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device'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.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks,

Instrumentality Protocol

memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

III.

SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use sophisticated hashing tools, such as tools for identifying child pornography, including "EnCase" and "FTK" (Forensic Tool Kit).

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest),

only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device. If the search determines that a digital device contains data falling within the list of items to be seized, the government may also retain the device itself, without further order of the Court.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Instrumentality Protocol