

1 STEVEN G. KALAR
Federal Public Defender
2 HANNI M. FAKHOURY
Assistant Federal Public Defender
3 1301 Clay Street, Suite 1350N
Oakland, CA 94612
4 (510) 637-3500
hanni_fakhoury@fd.org
5

6 Attorneys for DUMAKA HAMMOND
7

8 UNITED STATES DISTRICT COURT
9 FOR THE NORTHERN DISTRICT OF CALIFORNIA
10 OAKLAND DIVISION

11 UNITED STATES OF AMERICA,) CR 16-102-JD
12)
Plaintiff,)
13 v.) MOTION TO SUPPRESS NIT SEARCH
WARRANT FOR VIOLATING THE
FOURTH AMENDMENT
14 DUMAKA HAMMOND,)
15 Defendant.) Date: September 8, 2016
Time: 10:30 a.m.
16)

17 **TO: BRIAN STRETCH, UNITED STATES ATTORNEY; AND**
18 **THOMAS R. GREEN, ASSISTANT UNITED STATES ATTORNEY:**

19 PLEASE TAKE NOTICE that the defendant DUAMAKA HAMMOND hereby moves this
20 Court for an order suppressing the Network Investigative Technique (“NIT”) search warrant for
21 violating the Fourth Amendment to the United States Constitution. This motion will be heard on
22 September 8, 2016 at 10:30 a.m. in Courtroom 11, on the 19th Floor of the San Francisco Courthouse.

23 This motion is based on this notice and motion, the attached memorandum of points and
24 authorities and accompanying exhibits, including previously filed exhibits, the Fourth Amendment
25 to the United States Constitution, all other applicable constitutional, statutory and case authority and
26 such evidence and argument that may be presented at the motion hearing.
27
28

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION 1

STATEMENT OF FACTS 1

ARGUMENT 6

 A. Each Deployment of the NIT Resulted in a Series of Invasive Searches and Seizures. 6

 1. The Presence of the NIT on Mr. Hammond’s Computer Was a Seizure and Search. 7

 2. Operating the NIT on Mr. Hammond’s Computer Was a Search. 7

 3. Copying Data From Mr. Hammond’s Computer Was a Seizure..... 9

 B. The NIT Warrant Was an Unconstitutional General Warrant. 9

 1. The Government Chose Not to Provide Additional Information in the Warrant. 10

 2. The Warrant Failed to Particularly Describe What Was Being Searched and Where Those Searches Would Occur. 11

 3. The Warrant Vested Too Much Discretion in the Executing Officers. 13

CONCLUSION 15

TABLE OF AUTHORITIES

Cases

1

2

3 *Arizona v. Evans*, 514 U.S. 1 (1995) 1

4 *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) 12

5 *Boyd v. United States*, 116 U.S. 616 (1886) 8

6 *Coolidge v. New Hampshire*, 403 U.S. 443 (1971) 9, 14

7 *Go-Bart Importing Co. v. United States*, 282 U.S. 344 (1931) 10

8 *Greenstreet v. Cnty. of San Bernardino*, 41 F.3d 1306 (9th Cir. 1994) 12

9 *Groh v. Ramirez*, 540 U.S. 551 (2004) 11, 14

10 *In re Warrant to Search A Certain Email Account*, 2016 WL 377056 (2d Cir. Jul. 14, 2016) 13

11 *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008) 13

12 *Katz v. United States*, 389 U.S. 347 (1967) 6, 7, 14

13 *LeClair v. Hart*, 800 F.2d 692 (7th Cir. 1986) 9

14 *Marron v. United States*, 275 U.S. 192 (1927) 13

15 *Maryland v. Garrison*, 480 U.S. 79 (1987) 10

16 *Maryland v. King*, 133 S. Ct. 1958 (2013) 11

17 *Rakas v. Illinois*, 439 U.S. 128 (1978) 8

18 *Riley v. California*, 134 S. Ct. 2473 (2014) 7, 8

19 *Stanford v. Texas*, 379 U.S. 476 (1965) 13

20 *Steagald v. United States*, 451 U.S. 204 (1981) 11

21 *United States v. Bridges*, 344 F.3d 1010 (9th Cir. 2003) 13, 14

22 *United States v. Bright*, 630 F.2d 804 (5th Cir. 1980) 10

23 *United States v. Cardwell*, 680 F.2d 75 (9th Cir. 1982) 10

24 *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) 9, 14

25 *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc) 1, 8

26 *United States v. Crawford*, 372 F.3d 1048 (9th Cir. 2004) (en banc) 14

27 *United States v. Duran-Orozco*, 192 F.3d 1277 (9th Cir. 1999) 15

1 *United States v. Ganoë*, 538 F.3d 1117 (9th Cir. 2008) 8

2 *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006)..... 12

3 *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006)..... 11

4 *United States v. Jacobsen*, 466 U.S. 109 (1984) 6, 7, 9

5 *United States v. Jefferson*, 571 F. Supp. 2d 696 (E.D. Va. 2008) 9

6 *United States v. Jones*, 132 S. Ct. 945 (2012) 6, 7

7 *United States v. Payton*, 573 F.3d 859 (9th Cir. 2009) 8

8 *United States v. Spilotro*, 800 F.2d 959 (9th Cir. 1986)..... 11

9 *Walter v. United States*, 447 U.S. 649 (1980) 12

10 *Wong Sun v. United States*, 371 U.S. 471 (1963)..... 14

11 **Constitutional Provisions**

12 U.S. CONST. AMEND. IV *passim*

13 **Federal Statutes**

14 18 U.S.C. § 2252(a)(4)(B)..... 5

15 **Federal Rules**

16 Fed. R. Crim. P. 41(b) 13

17 **News Articles**

18 Andy Greenberg, “Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds,” *Wired*
 19 (Dec. 30, 2014), *available at* [https://www.wired.com/2014/12/80-percent-dark-web-visits-](https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/)
 20 [relate-pedophilia-study-finds/](https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/)..... 12

21 Joseph Cox, “FBI’s Mass Hack Hit 50 Computers in Austria,” *Motherboard* (Jul. 28, 2016),
 22 *available at* [https://motherboard.vice.com/read/fbis-mass-hack-playpen-operation-pacifier-](https://motherboard.vice.com/read/fbis-mass-hack-playpen-operation-pacifier-hit-50-computers-in-austria)
 23 [hit-50-computers-in-austria](https://motherboard.vice.com/read/fbis-mass-hack-playpen-operation-pacifier-hit-50-computers-in-austria) 13

24 Joseph Cox, “New Case Suggests the FBI Shared Data from Its Mass Hacking Campaign with the
 25 UK,” *Motherboard* (Feb. 10, 2016), *available at* [https://motherboard.vice.com/read/new-](https://motherboard.vice.com/read/new-case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk)
 26 [case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk](https://motherboard.vice.com/read/new-case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk) 13

INTRODUCTION

1
2 The Ninth Circuit recently explained that “legitimate concerns about child pornography do
3 not justify unfettered crime-fighting searches or an unregulated assault on citizens’ private
4 information.” *United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013) (en banc). The nature
5 of the child pornography crime under investigation here, specifically the Playpen website, led the
6 government to seek and a court to approve a warrant that deployed an expansive and unprecedented
7 tool to hunt down users of the site: a piece of computer code called a Network Investigative
8 Technique (“NIT”) that was sent to the computers of individual users and reported information about
9 those computers back to the FBI. The government, however, did not seek to deploy this tool in the
10 targeted, particular way required by the Fourth Amendment of the U.S. Constitution. Instead the FBI
11 was permitted to deploy the NIT aggressively and expansively, sending it to hundreds of thousands
12 of computers across the United States and abroad. These numerous searches and seizures were
13 authorized by a single search warrant issued by a single magistrate judge in the Eastern District of
14 Virginia.

15 It did not have to be this way; once the government had seized the Playpen site, it could have
16 more narrowly deployed the NIT to specific users based on particularized and specific showings of
17 probable cause. Law enforcement cannot rely on new surveillance techniques “blindly,” and “[w]ith
18 the benefits of more efficient law enforcement mechanisms comes the burden of corresponding
19 constitutional responsibilities.” *Arizona v. Evans*, 514 U.S. 1, 17-18 (1995) (O’Connor, J.,
20 concurring). With appropriate tailoring and sufficient specificity, a valid warrant could issue for the
21 deployment of the NIT. But here, the government consciously chose to cast its net as broadly as
22 possible, neglecting its constitutional responsibilities. Ultimately, that means the NIT warrant
23 violated the Fourth Amendment’s particularity requirement and must be suppressed.

24 **STATEMENT OF FACTS**

25 Beginning in September 2014, FBI agents began investigating a child pornography website
26 called “Playpen” which was accessed on the Tor computer network. The Tor network consists of a
27 computer network and software that provide Internet users with online anonymity. Tor was initially
28

1 developed by the United States Naval Research Lab in the 1990s and is now run as an independent
2 non-profit organization. Tor works by obscuring how and where users access the Internet. Users
3 first download Tor software onto their computers. The software allows users to connect to the Tor
4 network, which is a network of computers—known as “nodes” or “relays”—operated by volunteers.
5 When a user connects to the Tor network, their Internet traffic does not go directly to the website
6 they are seeking. Instead, a Tor user’s Internet traffic connects to a volunteer node or relay, which
7 passes the user’s Internet traffic on to another volunteer node or relay, and then to another node or
8 relay (and perhaps many other nodes or relays) until it exits through an “exit node” and connects to
9 the site. This allows users to mask their true location when they visit a site. Specifically, the site
10 will only know the IP address of the exit node’s computer, and not the original computer that sought
11 to access the site.¹

12 Tor also provides users with other services, including an anonymous web hosting service
13 known as a “hidden service.” A Tor hidden service is a website hosted on the Tor network which
14 does not reveal its location. For example, rather than displaying a URL like www.cand.uscourts.gov,
15 the site’s location would be replaced with a Tor based web address such as dboevtdpvsuthpw.onion.
16 Tor hidden service websites end in .onion and can only be accessed through the Tor network. As a
17 result, a Tor user can connect to a Tor hidden service site without knowing the site’s location and
18 without the site knowing the visitor’s location.²

19 Playpen operated as a Tor hidden service that could only be accessed through the Tor
20 network. In order to access the site, a visitor was required to login with a username and password.
21 *See* Exhibit A, Eastern District of Virginia Search Warrant 15-SW-89 (“NIT Warrant”) at ¶ 12. Once
22 logged in, a visitor could view the content on the site, which included discussion forums, private
23 messaging services, and images of child pornography. *Id.* at ¶¶ 12-14.

24 In December 2014, a foreign law enforcement agency informed the FBI that it had a suspected
25 United States based IP address for the site. *Id.* at ¶ 28. The FBI investigated the IP address and

27 ¹ *See generally* <https://www.torproject.org/about/overview.html.en>.

28 ² *See generally* <https://www.torproject.org/docs/hidden-services.html.en>.

1 determined that the website was hosted on a server in Lenoir, North Carolina. *Id.* In January 2015,
2 the FBI obtained and executed a search warrant in the Western District of North Carolina, and seized
3 the server that hosted the Playpen website. *Id.* Once the government had control of the website, it
4 had a window into the activity of the site’s users. *Id.* at ¶¶ 14-27. For example, it could see specific
5 posts by specific users and could tell how frequently users posted to the site. *Id.* at ¶¶ 16-19. The
6 government could view the site’s users by the number of posts they made and thus determine which
7 users aggressively used the site. *See* Exh. B, Declaration of Madeline Larsen at ¶ 5. For example,
8 by the time the site was shut down on March 4, 2015, the user who had posted the most on the
9 Playpen site had made a total of 1,309 posts. *Id.* The vast majority of users of the site, however, did
10 not post onto the site at all. *Id.* at ¶ 6 (only 11,460 of the approximately 214,980 users of the site as
11 of March 4, 2015, had posted on the site).

12 Once it seized the server hosting Playpen rather than shut down the site, the FBI instead
13 placed a copy of the seized server and website, including the child pornography contained on the
14 Playpen site, onto a government controlled server in Newington, Virginia. *Id.* On February 20,
15 2015, prosecutors in the Eastern District of Virginia (“EDVA”) submitted an application and
16 affidavit for a search warrant to U.S. Magistrate Judge Theresa Carroll Buchanan in Alexandria,
17 Virginia. In the affidavit, the government explained that it wanted to continue operating the Playpen
18 site from a “government-controlled computer server in Newington, Virginia, on which a copy of
19 TARGET WEBSITE currently resides.” Exh. A at ¶ 30. It explained it wanted to operate the site
20 for 30 days in order to locate and identify visitors to the site. *Id.* at ¶¶ 29-30. The warrant affidavit
21 explained that in order to identify the users of Playpen, it would need to deploy an additional
22 investigative tool to work around the fact that the Tor network was obfuscating the visitor’s IP
23 address. The government thus requested authorization to deploy a Network Investigative Technique
24 (“NIT”) which it believed had a “reasonable likelihood” to locate administrators and users of the site.
25 *Id.* at ¶ 31; *see also* ¶¶ 32-37.

26 The NIT was simply computer software that the government inserted into the Playpen site.
27 More specifically, the NIT was “malware”—a term used to refer to malicious software that is
28

1 designed to disrupt or damage computer operations, as well as gather sensitive information or gain
2 unauthorized access to a computer.³ The NIT was a form of malware known as a remote access tool,
3 which is software that takes advantage of unpatched flaws in computer software in order to control
4 a device and extract information from the computer without the user's knowledge or consent.⁴

5 According to the search warrant affidavit, the government would deploy the NIT—that is,
6 send it to the user's computer—anytime a visitor to Playpen entered a username and password to
7 access the site. Once a visitor to the site entered their username and password, the FBI controlled
8 server would use the NIT to force the user's computer to collect information directly from the user's
9 computer and then transmit that information back to the FBI. Exh. A at ¶ 36. The specific
10 information collected by the NIT were:

- 11 • The “activating” computer's actual IP address and the date and time the NIT
12 determined what that IP address was;
- 13 • A unique identifier generated by the NIT to distinguish the different data obtained
14 from other “activating” computers;
- 15 • The type of operating system running on the “activating” computer, including
16 type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
- 17 • Information about whether the NIT has already been delivered to the “activating”
18 computer;
- 19 • The “activating” computer's “host name,” which is the name assigned to a device
20 connected to a computer network used to identify the specific device;
- 21 • The “activating” computer's active operating system username; and
- 22 • The “activating” computer's Media Access Control (“MAC”) address, which is a
23 unique identifying number associated with computers.

24 *Id.* at ¶ 34. The NIT application sought authorization to deploy the NIT to investigate “any user”
25

26 ³ See Robert Moir, Defining Malware: FAQ, Microsoft TechNet (Oct. 2003), available at
<https://technet.microsoft.com/en-us/library/dd632948.aspx>.

27 ⁴ See Roger A. Grimes, Danger: Remote Access Trojans, Microsoft TechNet (Sept. 2002), available
28 at <https://technet.microsoft.com/en-us/library/dd632947.aspx>.

1 who logged into the site with a username and password, regardless of their physical location, whether
2 or not they were using the site’s chat features, or viewing child pornography. *Id.* at ¶ 32 fn. 8. But
3 the government also noted that it could deploy the NIT in other ways, explaining “in order to ensure
4 technical feasibility and avoid detection of the technique by subjects of investigation, the FBI may
5 deploy the NIT more discretely against particular users.” *Id.* The warrant affidavit, however, did
6 not elaborate on what that meant, how the government would decide which users merited that
7 different treatment or what deploying the NIT “more discretely” meant. The magistrate judge signed
8 the warrant that same day and authorized the government to deploy the NIT for 30 days.

9 Equipped with the NIT warrant and a wiretap order signed by a district judge authorizing the
10 real time interception of communications on the site, the government began deploying the NIT on
11 February 20, 2015. *See* Doc. 19, Motion to Suppress NIT Warrant, Exhibit B, Eastern District of
12 Virginia Wiretap Order 15-ES-4. Although the government was authorized to deploy the NIT for 30
13 days, on March 4, 2015, it abruptly stopped deploying the NIT and took the Playpen website offline.
14 Based on information obtained by the NIT, the government identified numerous IP addresses that
15 visited the Playpen site during the time it was operated by the government.

16 One of those IP address was associated with 678 7th Street in Richmond, California, which
17 was ultimately determined to be Mr. Hammond’s residence.⁵ On July 16, 2015, FBI Special Agent
18 Robert Basanez submitted an application and affidavit for a search warrant to Northern District of
19 California Magistrate Judge Maria-Elena James, seeking authorization to search Mr. Hammond’s
20 apartment in Richmond. *See* Doc. 19, Motion to Suppress NIT Warrant, Exhibit C, Northern District
21 of California Search Warrant 15-70905. Judge James signed the warrant that same day. *Id.* at p. 5-7.

22 The next day, the FBI executed the search warrant in Richmond. Eight months later, a one
23 count indictment was filed on March 10, 2016, charging Mr. Hammond with possession of child
24 pornography in violation of 18 U.S.C. § 2252(a)(4)(B).

25
26
27 ⁵ After filing the motion to suppress the NIT warrant (Doc. 19), counsel for Mr. Hammond realized
28 that the motion incorrectly identified Mr. Hammond’s address as 678 8th Street; it should be 678 7th
Street.

1 **ARGUMENT**

2 The Fourth Amendment to the U.S. Constitution states “The right of the people to be secure
3 in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be
4 violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and
5 particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST.
6 AMEND. IV.

7 Here, the NIT both searched Mr. Hammond’s computer and seized data from it. While the
8 government obtained a search warrant to deploy the NIT, the warrant failed to comply with one of
9 the pillars of the Fourth Amendment: it was not particularized but instead a 21st century version of
10 a general warrant. Thus, the NIT warrant and all of its fruits must be suppressed.

11 **A. Each Deployment of the NIT Resulted in a Series of Invasive Searches and Seizures.**

12 A Fourth Amendment seizure occurs when “there is some meaningful interference with an
13 individual’s possessory interests” in property. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).
14 A Fourth Amendment search occurs when the government either “physically occupie[s] private
15 property for the purpose of obtaining information,” *United States v. Jones*, 132 S. Ct. 945, 949
16 (2012), or infringes on an individual’s “reasonable expectation of privacy.” *Katz v. United States*,
17 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).

18 The NIT warrant glosses over the significant Fourth Amendment events that occurred every
19 time the government deployed its malware, but each NIT deployment caused three separate Fourth
20 Amendment events to occur: (1) a seizure of Mr. Hammond’s computer; (2) a search of the private
21 areas of that computer; and (3) a seizure of private information from the computer. That two seizures
22 and a search occurred when the NIT was deployed is evidence of the NIT warrant’s sweeping
23 breadth. The NIT warrant was not limited to a single search or seizure; nor was it limited to all three
24 for a specific user. Rather, the NIT warrant ultimately authorized the FBI to repeatedly execute these
25 searches and seizures—upwards of hundreds of thousands of times—on thousands of computers.

1 **1. The Presence of the NIT on Mr. Hammond’s Computer Was a Seizure and**
2 **Search.**

3 When the government sent the NIT to Mr. Hammond’s computer, that malware exploited an
4 otherwise unknown or obscure software vulnerability, turning the software against the user—and
5 into a law enforcement investigative tool. As a result, the presence of the NIT on Mr. Hammond’s
6 computer (even if unnoticed by Mr. Hammond), and the manipulation of the software running on his
7 computer, constitutes a Fourth Amendment seizure and search.

8 Mr. Hammond undeniably had a possessory interest in his personal property—the computer
9 and the software operating on those computers. The government “interfere[d]” with that possessory
10 interest by surreptitiously placing the NIT code on his computer. Indeed, by exploiting a
11 vulnerability in the software running on his computer, the government exercised “dominion and
12 control” over the exploited software and thus seized Mr. Hammond’s computer. *Jacobsen*, 466 U.S.
13 at 120-21, n.18. Similarly, even if the malware did not affect the normal operation of the software,
14 it added a new—and unwanted—“feature:” it became a law enforcement tool for identifying Tor
15 users. That exercise of “dominion and control,” even if limited, was a Fourth Amendment seizure.
16 *Id.*

17 The installation and presence of the NIT onto Mr. Hammond’s computer was also a Fourth
18 Amendment search since the government entered into Mr. Hammond’s computer in order to obtain
19 information about him. *See Jones*, 132 S. Ct. at 949 (finding Fourth Amendment search occurred
20 where “government physically occupied” individual’s property by attaching GPS tracker to it).

21 **2. Operating the NIT on Mr. Hammond’s Computer Was a Search.**

22 When the NIT operated on Mr. Hammond’s computer, the malware sought out certain
23 information stored on the computer. This was a Fourth Amendment search since it intruded upon a
24 reasonable expectation of privacy. *Katz*, 389 U.S. at 360-61.

25 There can be no real dispute that individuals have a reasonable expectation of privacy in their
26 computers and the information stored therein. As the Supreme Court recently recognized in *Riley v.*
27 *California*, 134 S. Ct. 2473 (2014), due to the wealth of information that electronic devices “contain
28

1 and all they may reveal, they hold for many Americans “the privacies of life.” 134 S. Ct. at 2494-95
2 (citing *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Computers “are simultaneously offices
3 and personal diaries” and “contain the most intimate details of our lives.” *Cotterman*, 709 F.3d at
4 964. It is no surprise that the Ninth Circuit has repeatedly recognized the need for a warrant prior to
5 searching a computer. *See, e.g., United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009)
6 (“Searches of computers . . . often involve a degree of intrusiveness much greater in quantity, if not
7 different in kind, from searches of other containers.”); *United States v. Ganoë*, 538 F.3d 1117, 1127
8 (9th Cir. 2008) (“as a general matter an individual has an objectively reasonable expectation of
9 privacy in his personal computer”).

10 In this case, a search occurred because the NIT operated directly on Mr. Hammond’s
11 computer—a private area subject to a reasonable expectation of privacy. *Ganoë*, 538 F.3d at 1127.
12 That is all that is required to give rise to a Fourth Amendment interest. *See Rakas v. Illinois*, 439
13 U.S. 128, 143 (1978) (Fourth Amendment protection depends on “a legitimate expectation of privacy
14 in the invaded place”).⁶ The malware operated by “searching” the computer and its memory for the
15 following information: the computer’s IP address; the type of operating system running on the
16 computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x
17 86); the computer’s “Host Name”; the computer’s “active operating system username”; and
18 “media access control (“MAC”) address.” Doc. 19, Exh. A at ¶ 34.⁷ Just as a search would have
19 occurred if the FBI manually reviewed Mr. Hammond’s computer to locate this information, a search

20
21 ⁶ While some of the information obtained in the search might, in other contexts, be provided to third
22 parties, the government did not obtain the information here from any third party. Rather, it directly
23 searched private areas on Mr. Hammond’s computer. Thus, the so-called third party doctrine—
24 which holds there is no Fourth Amendment expectation of privacy in information voluntarily given
25 to a third party when the government seeks to *obtain it from the third party directly*—has no
26 applicability here. *See Riley*, 134 S. Ct. at 2492-93 (third party doctrine did not apply when police
27 directly search cell phone’s call log as opposed to records of phone calls obtained from the phone
28 company); *see also* Doc. 19 at p. 14-15.

⁷ Mr. Hammond is not aware of precisely how the malware operated on his computer and is awaiting
additional discovery from the government on the specifics of the NIT computer code. Those
specifics could affect the analysis of the invasiveness of the search—how much information the
malware accessed and what specific areas of the computer were searched—which could be a separate
basis for a motion to suppress. Even without those specifics, as explained above, this Court can
conclude that a Fourth Amendment search and seizure occurred.

1 also occurred when the government employed technological means to interact with the computer
2 directly and obtain the same information.

3 **3. Copying Data From Mr. Hammond’s Computer Was a Seizure.**

4 When the NIT copied information from software running on the users’ computers, the
5 copying of that data was a second seizure. Again, a seizure occurs when the government
6 “meaningfully interfere[s]” with an individual’s possessory interest in property. *Jacobsen*, 466 U.S.
7 at 113. Courts recognize that individuals have possessory interests in information and that copying
8 information interferes with that interest. *See LeClair v. Hart*, 800 F.2d 692, 695, 696 n.5 (7th Cir.
9 1986) (recognizing it “is the information and not the paper and ink itself” that is actually seized)
10 (quoting *Jacobsen*, 466 U.S. at 113).

11 “[W]hile copying the contents of a person’s documents . . . does not interfere with a person’s
12 possession of those documents, it does interfere with the person’s *sole* possession of the information
13 contained in those documents.” *United States v. Jefferson*, 571 F. Supp. 2d 696, 703 (E.D. Va. 2008)
14 (emphasis added). This is because “the Fourth Amendment protects an individual’s possessory
15 interest in information itself, and not simply in the medium in which it exists.” *Id.* at 702; *see also*
16 *United States v. Comprehensive Drug Testing, Inc.* (“CDT”), 621 F.3d 1162, 1168-71 (9th Cir. 2010)
17 (en banc) (per curiam) (referring to copying of data as a “seizure”).

18 Since the government both searched and seized data from Mr. Hammond’s computer, it was
19 required to obtain a search warrant before deploying the NIT. Although the government did in fact
20 obtain a warrant, that warrant failed to satisfy a crucial Fourth Amendment prerequisite: that it be
21 particularized.

22 **B. The NIT Warrant Was an Unconstitutional General Warrant.**

23 One of the “distinct constitutional protections served by the warrant requirement” is that
24 “those searches deemed necessary should be as limited as possible.” *Coolidge v. New Hampshire*,
25 403 U.S. 443, 467 (1971). The Fourth Amendment was intended to eliminate “the ‘general warrant’
26 abhorred by the colonists” which was “a general, explanatory rummaging in a person’s belongings.”
27 *Id.* Thus, the Fourth Amendment requires a warrant be particular and limits searches and seizures to
28

1 “specific areas and things for which there is probable cause to search.” *Maryland v. Garrison*, 480
2 U.S. 79, 84 (1987). That ensures “the search will be carefully tailored to its justifications, and will
3 not take on the character of the wide-ranging explanatory searches the Framers intended to prohibit.”
4 *Id.* Particularity also ensures that warrants are not issued on the basis of “vague or doubtful bases of
5 fact.” *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931).

6 As described above, each time the malware was deployed, a series of significant searches and
7 seizures took place. Given the significance and invasiveness of those events, particularity was
8 critical. But the NIT warrant failed this elementary Fourth Amendment requirement.

9 **1. The Government Chose Not to Provide Additional Information in the Warrant.**

10 The obstacles to investigation posed by Tor did not justify a warrant as sweeping as the one
11 obtained by the government here. The particularity requirement is context-dependent, and the
12 specificity required in a warrant will vary based on the amount of information available and the scope
13 of the search to be executed. Thus, in assessing the validity of warrants, “[o]ne of the crucial factors
14 to be considered is the information available to the government.” *United States v. Cardwell*, 680
15 F.2d 75, 78 (9th Cir. 1982); *see also Garrison*, 480 U.S. at 85-86 (officers who know they do not
16 have probable cause to search a place are “plainly” obligated to exclude it from a warrant request).
17 “Generic classification in a warrant are acceptable only when a more precise description is not
18 possible.” *Cardwell*, 680 F.2d at 78 (quoting *United States v. Bright*, 630 F.2d 804, 812 (5th Cir.
19 1980)).

20 Here, far more precision was possible, and thus necessary. The FBI was in possession of the
21 server that hosted the site and had a clear window into the site’s user activity. Based on this user
22 activity, the government could track: (1) which users were posting and the specific information they
23 could access; (2) the frequency with which those users were doing so; and (3) the nature of the
24 information that was posted or accessed. In other words, the government knew which *specific*
25 Playpen users were administrators of the site and could tell which users used the site regularly and
26 aggressively. *See* Exh. A at ¶¶ 14-27; Exh. B at ¶¶ 5-6. Law enforcement could have done more
27 still—such as reviewing site activity for evidence of a user’s location or actual identity, issuing
28

1 subpoenas for email addresses associated with user accounts, or using the site’s chat feature to engage
 2 individual users in conversations to learn more about their location or identity.⁸ The government
 3 could have thus obtained a specific NIT warrant based on specific facts and tied to specific users,
 4 authorizing NIT searches and seizures against those specific, named users and their specific
 5 computers. *See United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) (validity of warrant
 6 depends on “whether the government was able to describe the items more particularly in light of
 7 the information available to it at the time the warrant issued”).⁹

8 **2. The Warrant Failed to Particularly Describe What Was Being Searched and**
 9 **Where Those Searches Would Occur.**

10 The NIT warrant failed to meet the requirements of particularity in myriad ways. Warrants
 11 require identification of a particular individual and the particular place to be searched. *See Maryland*
 12 *v. King*, 133 S. Ct. 1958, 1980 (2013) (warrant lacks particularity if “not grounded upon a sworn
 13 oath of a specific infraction by a *particular* individual, and thus not limited in scope and application”)
 14 (emphasis added). For example, an arrest warrant for a specific individual is not sufficiently
 15 particularized to give officers the “authority to enter the homes of third parties” when it “specifies
 16 only the object of a search . . . and leaves to the unfettered discretion of the police the decision as to
 17 which particular homes should be searched.” *Steagald v. United States*, 451 U.S. 204, 220 (1981).
 18 Any additional person or place to be searched requires a specific description in the warrant and an

19 _____
 20 ⁸ In the wiretap affidavit, the government claimed traditional investigative techniques were unlikely
 21 to succeed. Doc. 19, Exh. B at ¶¶ 63-76. But they never explained any of those details *in the NIT*
 22 *warrant affidavit* to the magistrate judge who authorized the expansive deployment of the NIT. Any
 23 attempt by the government to incorporate other documents into the NIT warrant affidavit had to be
 24 explicit in the NIT warrant itself. *See United States v. Hill*, 459 F.3d 966, 975-76 (9th Cir. 2006)
 25 (“We do not approve of issuing warrants authorizing blanket removal of all computer storage media
 for later examination when there is no affidavit giving a reasonable explanation...as to why a
 wholesale seizure is necessary.”); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (“We do not
 say that the Fourth Amendment prohibits a warrant from cross-referencing other documents...But in
 this case the warrant did not incorporate other documents by reference, nor did either the affidavit or
 the application (which had been placed under seal) accompany the warrant. Hence, we need not
 further explore the matter of incorporation.”).

26 ⁹ Although the government eventually did obtain a warrant specific to Mr. Hammond, that was only
 27 *after* it deployed the NIT expansively and *after* it had searched his computer and seized data from it.
 28 Regardless of what steps it could have taken *before* it deployed the NIT here, it was ultimately the
 un-particularized and unconstitutional NIT warrant that resulted in the search of Mr. Hammond’s
 computer.

1 individualized showing of probable cause. *See Greenstreet v. Cnty. of San Bernardino*, 41 F.3d
2 1306, 1309 (9th Cir. 1994); *see also Walter v. United States*, 447 U.S. 649, 656-57 (1980) (“a warrant
3 to search for a stolen refrigerator would not authorize the opening of desk drawers.”).

4 The NIT warrant here did not name any specific person. Nor did it identify any specific user
5 of the targeted website. It did not attempt to describe any series or group of particular users. Nor did
6 it identify any particular computer to be searched, or even a particular type of device. Exh. A at
7 Attachment A. Instead, the NIT warrant broadly encompassed the computer of “any user or
8 administrator” of the website, regardless of whether they were a user of the site, an academic
9 researcher,¹⁰ an undercover officer from another law enforcement agency,¹¹ or a person who only
10 logged on to legally read fictional pornographic stories.¹² Significantly, there were approximately
11 “158,094 total members” to the site at the time the government requested the NIT warrant. Exh. A
12 at ¶ 11. The NIT warrant, on its face, thus authorized the searches and seizures described earlier for
13 as many as 158,094 individuals’ computers.

14 Compounding matters, the NIT warrant failed to provide any specificity about *where* the
15 searches would be carried out—the location of the “activating computers.”¹³ Instead, the NIT
16 warrant authorized the search of “any” activating computer, no matter *where* that computer might be
17 located. Exh. A at Attachment A. Because an activating computer could conceivably be located
18 anywhere in the world, the Warrant authorized FBI searches and seizures in all 50 U.S. states, every
19

20 ¹⁰ *See* Andy Greenberg, “Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds,”
21 *Wired*, Dec. 30, 2014, available at <https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/> (reporting on University of Portsmouth study where researchers ran
22 Tor relays, visited the Tor hidden service sites visited by Tor users that used these relays and
classified each site by its content).

23 ¹¹ *See e.g., United States v. Gourde*, 440 F.3d 1065, 1067 (9th Cir. 2006) (undercover agent logged
onto child pornography site).

24 ¹² *See* Exh. A at ¶ 14 (section of Playpen website devoted to fictional stories); *see also Ashcroft v.*
25 *Free Speech Coalition*, 535 U.S. 234, 250 (2002) (First Amendment prohibits criminalization of
pornographic speech “that records no crime and creates no victims by its production.”).

26 ¹³ The NIT warrant claimed the location of the property to be searched was the government server
27 hosting the Playpen website in the Eastern District of Virginia. Doc. 19, Exh. A, Attachment A
28 (“place to be searched” is “computer server” operating the website). But as explained earlier, and in
Mr. Hammond’s previously filed motion to suppress, that is incorrect: the searches occurred on the
user’s specific computers, wherever they were located. *See* Doc. 19 at p. 8-11.

1 U.S. territory, and every country around the world.¹⁴ The fact that the searches could take place in
 2 a foreign country raises significant red flags because U.S. magistrate judges have no legal authority
 3 to issue a warrant to seize or search data located abroad. *See* Fed. R. Crim. P. 41(b) (limiting
 4 magistrate judge’s authority to authorize a search to particular U.S. districts, territories, possessions
 5 or diplomatic or consular properties located abroad); *see also In re Warrant to Search A Certain*
 6 *Email Account*, ___ F.3d ___, 2016 WL 377056, *8 (2d Cir. Jul. 14, 2016); *In re Terrorist Bombings*
 7 *of U.S. Embassies in East Africa*, 552 F.3d 157, 169 (2d Cir. 2008). Thus, the breadth of the NIT
 8 warrant was virtually unbounded.

9 “Search warrants . . . are fundamentally offensive to the underlying principles of the Fourth
 10 Amendment when they are so bountiful and expansive in their language that they constitute
 11 a virtual, all-encompassing dragnet.” *United States v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003).
 12 Such is the case here: the government obtained a single warrant, authorizing the search of upwards
 13 of 159,000 users located around the world. That is far closer to a “virtual, all-encompassing dragnet”
 14 than a specific, particularized warrant required by the Fourth Amendment. *Bridges*, 344 F.3d
 15 at 1016.

16 3. The Warrant Vested Too Much Discretion in the Executing Officers.

17 The Fourth Amendment’s particularity requirement makes general searches “impossible” by
 18 ensuring that, when it comes to what can be searched or seized, “nothing is left to the discretion of
 19 the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also*
 20 *Stanford v. Texas*, 379 U.S. 476, 481 (1965) (particularity helps eliminate the threat of “officers
 21 acting under the unbridled authority of a general warrant”).

22 As a result of its breadth—authorizing the search of “any” activating computer regardless of
 23 where it was located—the NIT warrant gave executing officers total discretion to decide which users

24 _____
 25 ¹⁴ Indeed, it appears that the government did conduct overseas searches based on the NIT warrant.
 26 *See* Joseph Cox, “FBI’s Mass Hack Hit 50 Computers in Austria,” *Motherboard* (Jul. 28, 2016),
 27 *available at* <https://motherboard.vice.com/read/fbis-mass-hack-playpen-operation-pacifier-hit-50-computers-in-austria>;
 28 Joseph Cox, “New Case Suggests the FBI Shared Data from Its Mass Hacking Campaign with the UK,”
Motherboard (Feb. 10, 2016), *available at* <https://motherboard.vice.com/read/new-case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk>.

1 to target and the manner in which to accomplish the searches and seizures. It thus left to the FBI to
2 decide how the NIT would be deployed, how the NIT operated, what portions of the activating
3 computers the NIT would search, and which of the hundreds of thousands of users of the site the NIT
4 would be deployed against.

5 In fact, the warrant application explicitly sought that discretion. As the government
6 explained, “in order to ensure technical feasibility and avoid detection of the technique by subjects
7 of investigation, the FBI may deploy the NIT more discretely against particular users.” Exh. A at ¶
8 32 n. 8. Thus, the government deployed different types of malware (or the same malware, in different
9 ways) against different users without providing any explanation of how and when these distinctions
10 would be made. Thus, the NIT warrant permitted the government to conduct its searches and seizures
11 in different ways against different users—all at the FBI’s discretion.

12 Particularly absent from the warrant was some meaningful limitation on the operation of the
13 NIT. Given that the malware effectuated a search of a user’s private computer, this type of tailoring
14 was critical. *See CDT*, 621 F.3d at 1168-71. Despite its facial appeal, the FBI’s request to act at its
15 own discretion is further evidence of a constitutional violation. *See Groh*, 540 U.S. at 560-61 (“Even
16 though petitioner acted with restraint in conducting the search, the inescapable fact is that this
17 restraint was imposed by the agents themselves, not by a judicial officer.”) (citing *Katz*, 389 U.S. at
18 356). Warrants, and the particularity requirement specifically, are designed so that the searches
19 authorized are “as limited as possible.” *Coolidge*, 403 U.S. at 467. That was not the case here: the
20 government cast its net as widely as possible and, at its own election, decided who it would target
21 and in what manner. But leaving the operation of a “dragnet” to the “discretion of the State” is
22 “fundamentally offensive to the underlying principles of the Fourth Amendment.” *Bridges*, 344 F.3d
23 at 1016.

24 Thus, the NIT warrant violated the Fourth Amendment and the warrant and all other evidence
25 “obtained as a product of illegal searches and seizures”—including the identification of Mr.
26 Hammond’s IP address—must be suppressed. *United States v. Crawford*, 372 F.3d 1048, 1054 (9th
27 Cir. 2004) (en banc) (citing *Wong Sun v. United States*, 371 U.S. 471, 484-88 (1963)). That extends
28

1 to evidence seized from the Richmond search warrant, including but not limited to any evidence
2 seized from Mr. Hammond's computer, which was a "fruit" of the original illegal NIT search
3 warrant. *See United States v. Duran-Orozco*, 192 F.3d 1277, 1281 (9th Cir. 1999).

4 **CONCLUSION**

5 The government could have more specifically tailored the NIT search warrant in order to
6 narrow its scope and avoid the unprecedented expansive search that occurred here. Because the NIT
7 warrant was not particularized, it violated the Fourth Amendment and the warrant and all of its fruits
8 must be suppressed.

9
10 DATED: August 4, 2016

STEVEN G. KALAR
Federal Public Defender

11
12 /S/
HANNI M. FAKHOURY
Assistant Federal Public Defender
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 STEVEN G. KALAR
Federal Public Defender
2 HANNI M. FAKHOURY
Assistant Federal Public Defender
3 1301 Clay Street, Suite 1350N
Oakland, CA 94612
4 Telephone: (510) 637-3500
5 Attorneys for DUMAKA HAMMOND

6
7 UNITED STATES DISTRICT COURT
8 FOR THE NORTHERN DISTRICT OF CALIFORNIA
9 OAKLAND DIVISION

10 UNITED STATES OF AMERICA,) CR 16-102-JD
11)
12 Plaintiff,) DECLARATION OF HANNI M.
13 v.) FAKHOURY IN SUPPORT OF MOTION
14 DUMAKA HAMMOND,) TO SUPPRESS NIT WARRANT
15 Defendant.)
16)

17 I, HANNI M. FAKHOURY, hereby state and declare:

- 18 1. I am an attorney licensed to practice law in California. I am employed as an Assistant Federal
19 Public Defender for the Northern District of California and have been appointed to represent
20 Mr. Hammond in this case.
21 2. Attached as Exhibit A is a true and correct copy of the February 20, 2015 Eastern District of
22 Virginia Search Warrant 15-SW-89 ("NIT Warrant") produced by the government in
23 discovery.
24 3. Attached as Exhibit B is the declaration of Federal Public Defender Investigator Madeline
25 Larsen. I personally witnessed Ms. Larsen sign the declaration.

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

27 DATED: August 4, 2016


28 
HANNI M. FAKHOURY

EXHIBIT A

U.S. v. DUMAKA HAMMOND

CR-16-102-JD

MOTION TO SUPPRESS NIT SEARCH
WARRANT FOR VIOLATING THE
FOURTH AMENDMENT

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

Alexandria Division

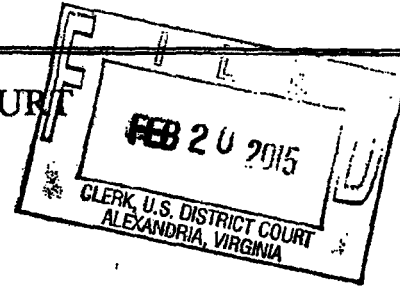
IN THE MATTER OF THE SEARCH) FILED UNDER SEAL
OF COMPUTERS THAT ACCESS)
upf45jv3bziuctml.onion) Case No. 1:15-SW-89

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 upf45jv3bzuctml.onion

Case No.1:15-SW-89

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

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

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

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

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

The search is related to a violation of:

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

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

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

Reviewed by AUSA/SAUSA:

AUSA Whitney Dougherty Russell

Douglas Macfarlane Applicant's signature

Douglas Macfarlane, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/20/2015

Theresa Carroll Buchanan United States Magistrate Judge

Judge's signature

Judge's signature

City and state: Alexandria, Virginia

Honorable Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

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

UNITED STATES DISTRICT COURT

for the Eastern District of Virginia

In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address) OF COMPUTERS THAT ACCESS upf45jv3bzlucltmi.onion

Case No. 1:15-SW-89

UNDER SEAL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia (Identify the person or describe the property to be searched and give its location): See Attachment A

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized): See Attachment B

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

YOU ARE COMMANDED to execute this warrant on or before March 6, 2015 (not to exceed 14 days)

in the daytime 6:00 a.m. to 10 p.m. at any time in the day or night as I find reasonable cause has been established.

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

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

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

Until, the facts justifying, the later specific date of

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

Theresa Carroll Buchanan United States Magistrate Judge

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

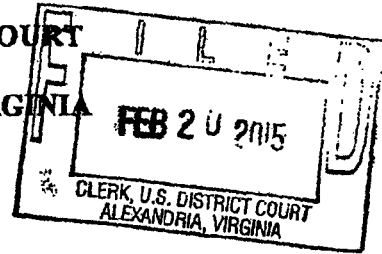
From any “activating” computer described in Attachment A:

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

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

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

INTRODUCTION

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") since April, 1996, and I am currently assigned to the FBI's Violent Crimes Against Children Section, Major Case Coordination Unit ("MCCU"). I currently investigate federal violations concerning child pornography and the sexual exploitation of children and have gained experience through training in seminars, classes, and everyday work related to these types of investigations. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information, in conjunction with criminal investigations pertaining to child pornography the sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

2. I make this affidavit in support of an application for a search warrant to use a network investigative technique (“NIT”) to investigate the users and administrators of the website upf45jv3bziuctml.onion (hereinafter “TARGET WEBSITE”) as further described in this affidavit and its attachments.¹

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

RELEVANT STATUTES

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

¹ The common name of the TARGET WEBSITE is known to law enforcement. The site remains active and disclosure of the name of the site would potentially alert users to the fact that law enforcement action is being taken against the site, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms.

2252A(a)(5)(B) and (b)(2), Knowing Possession, Access or Attempted Access With Intent to View Child Pornography.

- a. 18 U.S.C. § 2252A(g) prohibits a person from engaging in a child exploitation enterprise. A person engages in a child exploitation enterprise if the person violates, inter alia, federal child pornography crimes listed in Title 18, Chapter 110, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons;
- b. 18 U.S.C. §§ 2251(d)(1) and (e) prohibits a person from knowingly making, printing or publishing, or causing to be made, printed or published, or conspiring to make, print or publish, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;
- c. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) prohibits a person from knowingly receiving or distributing, or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

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

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

5. The following definitions apply to this Affidavit:
 - a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private

messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the bulletin board administrator.

- b. “Child erotica,” as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.
- c. “Child Pornography,” as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- d. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- e. “Computer Server” or “Server,” as used herein, is a computer that is attached to a dedicated network and serves many users. A “web server,” for example, is a

computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

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

form. It commonly includes programs to run operating systems, applications, and utilities.

- h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- j. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

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

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

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

- n. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- p. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of

any person. See 18 U.S.C. § 2256(2).

- q. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- r. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”).

PROBABLE CAUSE

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

The Tor Network

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

protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.²

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

9. Tor also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Tor network itself, entire websites can be set up as "hidden services." "Hidden services,"

² Users may also access the Tor network through so-called "gateways" on the open Internet such as "onion.to" and "tor2web.org," however, use of those gateways does not provide users with the anonymizing benefits of the Tor network.

like other websites, are hosted on computer servers that communicate through IP addresses and operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as “asdlk8fs9dfiku7f” 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, it is not possible to determine through public lookups the IP address of a computer hosting a Tor “hidden service.” Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

Finding and Accessing the TARGET WEBSITE

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

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

Description of the TARGET WEBSITE and Its Content

11. Between September 16, 2014 and February 3, 2015, FBI Special Agents operating in the District of Maryland connected to the Internet via the Tor Browser and accessed the Tor hidden service the TARGET WEBSITE at its then-current Uniform Resource Locator (“URL”) muff7i44irws3mwu.onion.³ The TARGET WEBSITE appeared to be a message board website whose primary purpose is the advertisement and distribution of child pornography. According to statistics posted on the site, the TARGET WEBSITE contained a total of 95,148 posts, 9,333 total topics, and 158,094 total members. The website appeared to have been operating since approximately August 2014 which is when the first post was made on the message board.

12. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, “No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out.” Based on my training and experience, I know that: “no cross-board reposts” refers to a prohibition against material that is posted on other websites from being “re-posted” to

³ As of February 18, 2015, the URL of the TARGET WEBSITE had changed from muff7i44irws3mwu.onion to upf45jv3bziuctml.onion. I am aware from my training and experience that it is possible for a website to be moved from one URL to another without altering its content or functionality. I am also aware from the instant investigation that the administrator of the TARGET WEBSITE occasionally changes the location and URL of the TARGET WEBSITE in an effort to, in part, avoid law enforcement detection. On February 18, 2015, I accessed the TARGET

the TARGET WEBSITE; and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' (a hyperlink to the registration page) with [TARGET WEBSITE name]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

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

"VERY IMPORTANT. READ ALL OF THIS PLEASE.

I will add to this as needed.

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

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

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

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

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

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

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

<u>Section – Forum</u>	<u>Topics</u>	<u>Posts</u>	
General Category			
[the TARGET WEBSITE] information and rules		25	236
How to	133	863	
Security & Technology discussion	281	2,035	
Request	650	2,487	
General Discussion	1,390	13,918	
The INDEXES	10	119	
Trash Pen	87	1,273	
[the TARGET WEBSITE] Chan			
Jailbait ⁴ – Boy	58	154	
Jailbait – Girl	271	2,334	
Preteen – Boy	32	257	
Preteen – Girl	264	3,763	
Jailbait Videos			
Girls	643	8,282	
Boys	34	183	
Jailbait Photos			
Girls	339	2,590	
Boys	6	39	

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

Pre-teen Videos		
Girls HC ⁵	1,427	20,992
Girls SC/NN	514	5,635
Boys HC	87	1,256
Boys SC/NN	48	193
Pre-teen Photos		
Girls HC	433	5,314
Girls SC/NN	486	4,902
Boys HC	38	330
Boys SC/NN	31	135
Webcams		
Girls	133	2,423
Boys	5	12
Potpourri		
Family [TARGET WEBSITE] – Incest	76	1,718
Toddlers	106	1,336
Artwork	58	314
Kinky Fetish		
Bondage	16	222
Chubby	27	309
Feet	30	218
Panties, nylons, spandex	30	369
Peeing	101	865
Scat	17	232
Spanking	28	251
Vintage	84	878
Voyeur	37	454
Zoo	25	222
Other Languages		
Italiano	34	1,277
Portugues	69	905
Deutsch	66	570
Espanol	168	1,614
Nederlands	18	264
Pyccknn – Russian	8	239

⁵ Based on my training and experience, I know that the following abbreviations respectively mean: HC – hardcore, i.e., depictions of penetrative sexually explicit conduct; SC – softcore, i.e., depictions of non-penetrative sexually explicit conduct; NN – non-nude, i.e., depictions of subjects who are fully or partially clothed.

Stories		
Fiction	99	505
Non-fiction	122	675

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

16. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as ".rar" files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

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

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

On February 3, 2015, the user [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
- Scat⁶
- Stories - Non-Fiction
- Zoo
- Webcams - Girls
- Webcams - Boys

Identification and Seizure of the Computer Server Hosting the TARGET WEBSITE

28. In December of 2014, a foreign law enforcement agency advised the FBI that it suspected IP address 192.198.81.106, which is a United States-based IP address, to be associated with the TARGET WEBSITE. A publicly available website provided information that the IP Address 192.198.81.106 was owned by [REDACTED] a server hosting company headquartered at [REDACTED]

[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 ██████████ 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 ██████████ 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 I by engaging in substantial posting activity, or in particular areas of TARGET WEBSITE, such as the TARGET WEBSITE sub-

type information that may assist in identifying the user's computer, its location, and the user of the computer, as to which there is probable cause to believe is evidence of violations of the statutes cited in paragraph 4. In particular, the NIT will only reveal to the government the following items, which are also described in Attachment B:

- a. The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
- b. A unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating" computers. That unique identifier will be sent with and collected by the NIT;
- c. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
- d. Information about whether the NIT has already been delivered to the "activating" computer;
- e. The "activating" computer's "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;
- f. the "activating" computer's active operating system username; and
- g. The "activating" computer's Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the

forums described in Paragraph 27.

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

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

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

37. In the normal course of the operation of a web site, a user sends “request data” to the web site in order to access that site. While the TARGET WEBSITE operates at a government

facility, such request data associated with a user's actions on the TARGET WEBSITE will be collected. That data collection is not a function of the NIT. Such request data can be paired with data collected by the NIT, however, in order to attempt to identify a particular user and to determine that particular user's actions on the TARGET WEBSITE.

REQUEST FOR DELAYED NOTICE

38. Rule 41(f)(3) allows for the delay of any notice required by the rule if authorized by statute. 18 U.S.C. § 3103a(b)(1) and (3) allows for any notice to be delayed if “the Court finds reasonable grounds to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in 18 U.S.C. § 2705) . . . ,” or where the warrant “provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay.” Because there are legitimate law enforcement interests that justify the unannounced use of a NIT, I ask this Court to authorize the proposed use of the NIT without the prior announcement of its use. Announcing the use of the NIT could cause the users or administrators of the TARGET WEBSITE to undertake other measures to conceal their identity, or abandon the use of the TARGET WEBSITE completely, thereby defeating the purpose of the search.

39. The government submits that notice of the use of the NIT, as otherwise required by Federal Rule of Criminal Procedure 41(f), would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing the TARGET WEBSITE. It would, therefore, seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence

of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(1) and 18 U.S.C. § 2705).

40. Furthermore, the investigation has not yet identified an appropriate person to whom such notice can be given. Thus, the government requests authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.

41. The government further submits that, to the extent that use of the NIT can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation. Furthermore, the NIT does not deny the users or administrators access to the TARGET WEBSITE or the possession or use of the information delivered to the computer controlled by or known to the government, nor does the NIT permanently alter any software or programs on the user's computer.

TIMING OF SEIZURE/REVIEW OF INFORMATION

42. Rule 41(e)(2) requires that the warrant command FBI "to execute the warrant within a specified period of time no longer than fourteen days" and to "execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time." After the server hosting the TARGET WEBSITE is seized, it will remain in law enforcement custody. Accordingly, the government requests authority to employ the NIT onto the TARGET WEBSITE at any time of day, within fourteen days of the Court's authorization. The NIT will be used on the TARGET WEBSITE for not more than 30-days from the date of the issuance of the warrant.

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

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

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

SEARCH AUTHORIZATION REQUESTS

46. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

- a. the NIT may cause an activating computer – wherever located – to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location,

other information about the computer and the user of the computer, as described above and in Attachment B;

- b. the use of multiple communications, without prior announcement, within 30 days from the date this Court issues the requested warrant;
- c. that the government may receive and read, at any time of day or night, within 30 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by or known to the government;
- d. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an “activating” computer that accessed the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

47. I further request that this application and the related documents be filed under seal. This information to be obtained is relevant to an ongoing investigation. Premature disclosures of this application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of this technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.⁹

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

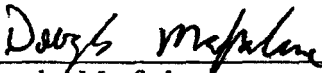
CONCLUSION

48. Based on the information identified above, information provided to me, and my experience and training, I have probable cause to believe there exists evidence, fruits, and instrumentalities of criminal activity related to the sexual exploitation of children on computers that access the TARGET WEBSITE, in violation of 18 U.S.C. §§ 2251 and 2252A.

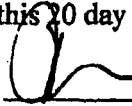
49. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of these crimes.

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

Sworn to under the pains and penalties of perjury.



Douglas Macfarlane
Special Agent

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


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

issue any written opinion regarding any aspect of this request, the United States requests notice and an opportunity to be heard with respect to the issue of law enforcement privilege.

ATTACHMENT A

Place to be Searched

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

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

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

ATTACHMENT B

Information to be Seized

From any “activating” computer described in Attachment A:

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

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

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

UNITED STATES DISTRICT COURT

for the Eastern District of Virginia

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

Theresa Carroll Buchanan United States Magistrate Judge

City and state: Alexandria, Virginia

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

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


Return		
Case No.: 1:15-SW-89	Date and time warrant executed: Between 2/20/15 and 3/4/15	Copy of warrant and inventory left with: N/A
Inventory made in the presence of: N/A		
Inventory of the property taken and name of any person(s) seized: Data from computers that accessed TARGET WEBSITE between 2/20/15 and 3/4/15		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: <u>March 31, 2015</u></p> <div style="text-align: right; margin-right: 100px;">  <hr style="width: 100%;"/> <p style="text-align: center; font-size: small;">Executing officer's signature</p> <p style="text-align: center;">Special Agent FBI, Daniel I. Alfin <small>Printed name and title</small></p> </div>		

EXHIBIT B

U.S. v. DUMAKA HAMMOND

CR-16-102-JD

MOTION TO SUPPRESS NIT SEARCH
WARRANT FOR VIOLATING THE
FOURTH AMENDMENT

1 STEVEN G. KALAR
Federal Public Defender
2 HANNI M. FAKHOURY
Assistant Federal Public Defender
3 1301 Clay Street, Suite 1350N
Oakland, CA 94612
4 Telephone: (510) 637-3500
5 Attorneys for DUMAKA HAMMOND

6
7 UNITED STATES DISTRICT COURT
8 FOR THE NORTHERN DISTRICT OF CALIFORNIA
9 OAKLAND DIVISION

10 UNITED STATES OF AMERICA,) CR 16-102-JD
11 Plaintiff,)
12 v.) DECLARATION OF MADELINE LARSEN
13 DUMAKA HAMMOND,) IN SUPPORT OF MOTION TO SUPPRESS
14 Defendant.) NIT WARRANT
15) Date: September 8, 2016
16) Time: 10:30 a.m.

- 17 I, MADELINE LARSEN, hereby state and declare:
- 18 1. I am an investigator employed with the Office of the Federal Public Defender in Oakland,
19 California.
 - 20 2. On July 29, 2016, I accompanied Assistant Federal Public Defender Hanni Fakhoury to the
21 Silicon Valley Regional Computer Forensics Laboratory in Menlo Park, California to review
22 a copy of the Playpen website.
 - 23 3. The website is hosted on an FBI network that only FBI personnel can directly access. FBI
24 Special Agent Brian Lester controlled the computer mouse and pointed on links that Mr.
25 Fakhoury and I asked him to click on.
 - 26 4. On the top of the Playpen website was a link called "staff list" which had a list of eight "global
27 moderators" and four "administrators." These individuals appeared to have more
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

involvement and activity in the site than other users.

5. There was another link on the top of the Playpen site called "Member List" which contained a list of every Playpen user. The list could be searched in order to find a specific user. Next to every specific user was information, including how many times they had made posts on the site. The top poster had made 1,309 posts on the Playpen website.

6. At the time we reviewed the Playpen website, there appeared to be approximately 214,980 users of the site. Of those users, it appears only 11,640 users had made posts on the website. The rest of the users had not made a post on the Playpen site.

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

DATED: August 4, 2016


MADELINE LARSEN