

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
FOR THE NORTHERN DISTRICT OF CALIFORNIA
9 OAKLAND DIVISION
10

11 UNITED STATES OF AMERICA,) CR 16-102-JD
12)
Plaintiff,)
13 v.) MOTION TO DISMISS THE INDICTMENT
FOR OUTRAGEOUS GOVERNMENT
CONDUCT
14 DUMAKA HAMMOND,)
15) Date: September 8, 2016
Defendant.) Time: 10:30 am
16)
_____)

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

19 PLEASE TAKE NOTICE that the defendant DUMAKA HAMMOND hereby moves this
20 Court for an order dismissing the indictment in this case, with prejudice, based on outrageous
21 government conduct, specifically, the government’s operation of a child pornography website from
22 February 20, 2015 until March 4, 2015 that caused thousands of child pornography links, images,
23 and videos to be posted, viewed, and distributed. This motion will be heard on September 8, 2016
24 at 10:30 a.m. in Courtroom 11, on the 19th Floor of the San Francisco Courthouse.

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

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 5

A. The Government’s Operation of Playpen Facilitated the Worldwide Distribution of
Child Pornography..... 6

B. Operating Playpen Harmed the Innocent Victims of Child Pornography Offenses..... 8

CONCLUSION 12

TABLE OF AUTHORITIES

Cases

1

2

3 *New York v. Ferber*, 458 U.S. 747 (1982)..... 9

4 *Paroline v. United States*, 134 S. Ct. 1710 (2014) 9, 10

5 *Rochin v. California*, 342 U.S. 165 (1952)..... 5

6 *United States v. Archer*, 486 F.2d 670 (2d Cir. 1973)..... 6, 8

7 *United States v. Black*, 733 F.3d 294 (9th Cir. 2013)..... *passim*

8 *United States v. Bogart*, 783 F.2d 1428 (9th Cir. 1986)..... 5

9 *United States v. Duncan*, 896 F.2d 271 (7th Cir. 1990) 10, 11

10 *United States v. Russell*, 411 U.S. 423 (1973)..... 5

11 *United States v. Shrake*, 515 F.3d 743 (7th Cir. 2008)..... 11

12 *United States v. Stinson*, 647 F.3d 1196 (9th Cir. 2011) 5

13 *United States v. Thoma* 726 F.2d 1191 (7th Cir. 1984)..... 5

14 *United States v. Wright*, 625 F.3d 583 (9th Cir. 2010)..... 11

15 *United States. v. Chin*, 934 F.2d 393 (2d Cir. 1991) 8, 10, 11

Statutes

16

17

18 18 U.S.C. § 2252(a)(4)(B)..... 5

19 18 U.S.C. § 2252(b)(1) 9

20 18 U.S.C. § 2252(b)(2) 9

21 18 U.S.C. § 2258C(a)(1)..... 11

22 18 U.S.C. § 2258C(a)(3)..... 11

23 18 U.S.C. § 3509(m)..... 11

Legislative Materials

24

25

26 Pub. L. 109-248, 120 Stat. 587 (Jul. 27, 2006)..... 11

27

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

Other Authorities

Carissa Bryne Hessick, “Law Enforcement Alone Shouldn’t Decide When to use a Pornography Website to Snare Predators,” *New York Times Room for Debate* (Jan. 27, 2016), available at <http://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting/law-enforcement-alone-shouldnt-decide-when-to-use-a-pornography-website-to-snare-predators> 1

Joseph Cox, “FBI’s Mass Hack Hit 50 Computers in Austria,” *Motherboard* (July 28, 2016), available at <https://motherboard.vice.com/read/fbis-mass-hack-Playpen-operation-pacifier-hit-50-computers-in-austria> 4

INTRODUCTION

1
2 Between February 20 and March 4, 2015, the FBI operated a child pornography website.
3 During those two weeks, the website’s membership grew by over 30%, the number of unique weekly
4 visitors to the site more than quadrupled, and 200 videos, 9,000 images, and 13,000 links to child
5 pornography were posted to the site. The government has stood behind their decision to run the
6 website, arguing that doing so was the only way to deploy a piece of software needed for identifying
7 the IP addresses of the site’s users. This argument, however, overlooks the fact that, as one law
8 professor has commented, the “F.B.I. appears to have committed a more serious crime—the
9 distribution of child pornography—to catch people committing less serious crimes: the receipt and
10 possession of child pornography.”¹

11 This behavior is all the more shocking because the federal government itself—in sentencing
12 memoranda, online mission statements, reports to congress, and press releases—has repeatedly
13 emphasized that victims of child pornography are revictimized each and every time their images are
14 viewed online. Despite these frequent pronouncements, the government here made no attempt during
15 the two weeks it was running the site to reduce the harm to innocent third party victims by limiting
16 the ability for users to view or access the images. Nor could the government—as itself has admitted
17 time and time again—control the spread of these images once uploaded and available on the internet.
18 The government’s action are “so grossly shocking” that they “violate the universal sense of justice.”
19 *United States v. Black*, 733 F.3d 294, 298 (9th Cir. 2013). The only remedy for this outrageous
20 conduct is to dismiss the indictment with prejudice.

STATEMENT OF FACTS

21
22 In September 2014, the government began investigating a child pornography website,
23 variably identified in search warrant affidavits as TARGET WEBSITE or WEBSITE A and now
24 publicly identified as “Playpen.” See Exhibit A, Eastern District of Virginia Search Warrant 15-SW-
25

26 ¹ Carissa Bryne Hessick, “Law Enforcement Alone Shouldn’t Decide When to use a Pornography
27 Website to Snare Predators,” *New York Times Room for Debate* (Jan. 27, 2016), available at
28 <http://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting/law-enforcement-alone-shouldnt-decide-when-to-use-a-pornography-website-to-snare-predators>.

1 89 (“NIT warrant”) at ¶ 28. With the help of foreign law enforcement officers, the government
2 eventually determined that the Playpen website was being hosted on a server in Lenoir, North
3 Carolina. Exh. A at ¶ 28. In January 2015, the government obtained and executed a search warrant
4 in the Western District of North Carolina, seizing the server that hosted the Playpen website. *Id.*
5 The website’s administrators are currently charged with running a child exploitation enterprise in
6 violation of 18 U.S.C. § 2252A(g), a crime which carries a minimum sentence of 20 years and a
7 maximum of life in prison, and as well as production of child pornography, 18 U.S.C. § 2251(d),
8 which carries a 15 year minimum and 30 year maximum prison sentence. *See United States v. Chase*
9 *et al.*, 15-CR-00015-RLV-DCK (W.D.N.C. Feb. 18, 2015).

10 After seizing the server, the government has explained to the Honorable Robert J. Bryan of
11 the Western District of Washington in one of the Playpen prosecutions that it considered “removing
12 [Playpen] from existence immediately and permanently.” *See* Exhibit B, United States’ Response to
13 Order Compelling Discovery, Doc. No. 109, *United States v. Michaud*, No. 15-CR-5351-RJB (W.D.
14 Wash., Jan. 8, 2016) at 6. Instead, the government placed a copy of the seized server, including the
15 child pornography contained on the Playpen website, onto a government controlled server in
16 Newington, Virginia. Exh. A at ¶ 28. It then applied for and received a warrant to run the Playpen
17 website itself for 30 days, explaining that in order to identify Playpen’s users, it would need to deploy
18 a “Network Investigative Technique” (“NIT”), a piece of computer code designed to work around
19 the fact that the use of Tor had obfuscated the IP addresses of the users on the site. *Id.* at ¶ 31.

20 In its supporting affidavit for the warrant, the government underestimated—and perhaps
21 underreported—the exponential growth in Playpen’s members. Particularly troublingly, the
22 government, averaging over “historical data” reaching back to the website’s inception, stated
23 Playpen had an average of 11,000 unique weekly visitors before February 20, 2015. *Id.* at ¶ 19.
24 After the warrant issued on February 20, 2015, however, an average of approximately 50,000 unique
25 users visited Playpen each week—more than quadruple the amount suggested by the government’s
26 figures. *See* Exh. B at 4 (“Between February 20 and March 4, 2015, approximately 100,000 unique
27 user accounts logged in to Website A.”).

1 Regardless of whether the government either misrepresented to the EDVA magistrate judge, or
2 recklessly failed to appreciate the amount of harm caused by running the Playpen website, the
3 government soon acknowledged its operation of Playpen had spiraled out of control. Although the
4 government had been permitted to operate the site for 30 days by Magistrate Judge Buchanan, it
5 ultimately shut down the operation after less than two weeks. *See* Exh. A, Attachment A. The
6 government explained to Judge Bryan that it shut the site down early due to the harm it was causing:

7 During the government’s operation of [Playpen], regular meetings were held to . . . assess
8 whether the site should continue to operate, based upon a balancing of various factors, to
9 include site users’ continued access to child pornography, the risk of imminent harm to a
10 child, the need to identify and apprehend perpetrators of those harms to children, and
11 other factors such as those described above. On March 4, 2015, it was determined that
12 the balance of those factors weighed in favor of shutting down the website.

13 Exh. B at 7. Especially harmful was the government’s distribution of large amounts of child
14 pornography. According to the government, the 100,000 users who visited Playpen during the two
15 weeks it was under government control “posted approximately 13,000 links . . . either to encrypted
16 archives containing multiple images or video files of child pornography, or to particular image files
17 depicting child pornography.” *Id.* at 3. These same users clicked at least 67,000 unique links to
18 child pornography images, videos, and encrypted archives, and posted thousands of new child
19 pornography images and videos to the website. *Id.*

20 In particular, the government told Judge Bryan it “recover[ed] approximately 9,000 images
21 and 200 videos that were made available by [Playpen] users while it operated under FBI
22 administrative control between February 20 and March 4, 2015.” *Id.* at 2. These images, however,
23 were not recovered—in the sense of being retained or retrieved—in the way that guns or drugs can
24 be recovered after a sting operation. Instead, once the images were uploaded to the Playpen website
25 the government had no control whatsoever over the images, which could be sent to other users or
26 posted to other websites. The Department of Justice (“DOJ”) has long emphasized the inability to
27 control the spread of digital child pornography, explaining on its own website that “[o]nce an image
28

1 is on the Internet, it is irretrievable and can continue to circulate forever.”²

2 By the government’s own standard, the children portrayed in these images were harmed each
3 time their images were viewed. The DOJ has repeatedly stated that anyone who views child
4 pornography “revictimizes the children by using those images for sexual gratification.”³ Federal
5 prosecutors have repeatedly used this argument to support lengthy prison sentences for individuals
6 convicted of possessing child pornography, including before this very Court. *See United States v.*
7 *Konrad Wolff*, 14-CR-00638-JD (N.D. Cal. May 12, 2016), Doc. 61, United States’ Sentencing
8 Memorandum at 6 (“The enduring and pervasive harm, of not only the original sexual abuse, but the
9 dissemination and viewing of that abuse by strangers, are [sic] evident”).

10 Nonetheless, during the two weeks the government ran Playpen, it made no effort to mitigate
11 harm to the victims of child pornography by limiting access to the child pornography on the site.
12 Instead, “[i]mages, videos and links posted by site users both before the FBI assumed administrative
13 control and afterwards, generally remained available to site users.” Exh. B at 4-5. For example, the
14 government did not—as it could have—allow users to login (permitting deployment of the NIT) but
15 restrict users’ ability to download images from the website or disable portions of the site that
16 contained child pornography while allowing users to navigate other portions of the site. Instead, the
17 government actively facilitated and participated in the distribution of thousands of child pornography
18 images around the world.⁴

19 To date, the federal government has charged 137 individuals in connection with this
20 investigation. Exh. B at 7. That number is less than 1% of the 158,094 total members that Playpen
21 had on February 3, 2015. Exh. A at ¶ 11. Notably, that percentage is roughly the same percentage

22
23 ² United States Department of Justice, Victims of Child Pornography, *available at*
24 <https://www.justice.gov/criminal-ceos/child-pornography>.

25 ³ United States Department of Justice, *The National Strategy for Child Exploitation and Prevention*
26 *and Interdiction: A Report to Congress* (Aug. 2010) at p. 9 *available at*
27 <https://www.justice.gov/psc/docs/natstrategyreport.pdf>.

28 ⁴ *See* Joseph Cox, “FBI’s Mass Hack Hit 50 Computers in Austria,” *Motherboard* (July 28, 2016),
available at <https://motherboard.vice.com/read/fbis-mass-hack-Playpen-operation-pacifier-hit-50-computers-in-austria>.

1 of Playpen members the government admitted it could have found IP addresses for without deploying
2 the NIT or keeping Playpen running once it had seized the server hosting the site in 2014. *Id.* at ¶
3 29 n. 7 (“The true IP addresses of a small number of users of the TARGET WEBSITE (that amounted
4 to less than 1% of the TARGET WEBSITE) were captured in the log files stored on the [seized]
5 server”).

6 Mr. Hammond is one of the 137 individuals charged in connection with the Playpen
7 investigation. As detailed in his previously filed motions to suppress, the NIT determined that an IP
8 address linked to Mr. Hammond’s apartment in Richmond had visited the Playpen site. In July 17,
9 2015, the government executed a search warrant at Mr. Hammond’s apartment, seizing his computer.
10 A one count indictment charging Mr. Hammond with possession of child pornography in violation
11 of 18 U.S.C. § 2252(a)(4)(B), was filed on March 10, 2016.

12 ARGUMENT

13 The Supreme Court has recognized that when “the conduct of law enforcement agents is so
14 outrageous that due process principles would absolutely bar the government from invoking judicial
15 processes to obtain a conviction.” *United States v. Russell*, 411 U.S. 423, 431 (1973); *see also Rochin*
16 *v. California*, 342 U.S. 165, 169 (1952) (finding due process requires courts review whether criminal
17 proceedings “offend those canons of decency and fairness which express the notions of justice of
18 English-speaking peoples even toward those charged with the most heinous offenses.”). An
19 indictment may be dismissed on due process grounds where the facts underlying the defendant’s
20 arrest and prosecution is “so grossly shocking and so outrageous as to violate the universal sense of
21 justice.” *United States v. Black*, 733 F.3d 294, 298 (9th Cir. 2013) (quoting *United States v. Stinson*,
22 647 F.3d 1196, 1209 (9th Cir. 2011) (quotations omitted)).

23 There are two scenarios where courts have recognized government action could be so
24 outrageous that a criminal indictment should be dismissed. First, it is outrageous misconduct when
25 “the Government supplies contraband, or becomes intimately involved in its production.” *United*
26 *States v. Thoma*, 726 F.2d 1191, 1199 (7th Cir. 1984); *see also United States v. Bogart*, 783 F.2d
27 1428, 1436 (9th Cir. 1986) (outrageous conduct when government “manufactures crimes that would
28

1 otherwise not occur”). Second, it is outrageous misconduct when government conduct results in
2 injuries to an innocent third party. *See United States v. Archer*, 486 F.2d 670, 677 (2d Cir. 1973).

3 The government’s unprecedented decision to operate a child pornography website for two
4 weeks, exposing thousands of victims to harm that—by the DOJ’s own admission—is both severe
5 and uncontrollable, warranting dismissal of the indictment.

6 **A. The Government’s Operation of Playpen Facilitated the Worldwide Distribution of**
7 **Child Pornography.**

8 In *Black*, the Ninth Circuit articulated six factors to be considered in assessing whether
9 government conduct is outrageous:

10 (1) known criminal characteristics of the defendants; (2) individualized suspicion of
11 the defendants; (3) the government’s role in creating the crime of conviction; (4) the
12 government’s encouragement of the defendants to commit the offense conduct; (5)
13 the nature of the government’s participation in the offense conduct; and (6) the nature
of the crime being pursued and necessity for the actions taken in light of the nature of
the criminal enterprise at issue.

14 733 F.3d at 303. Critically, while the Court should consider these factors, it must ultimately “resolve
15 every case on its own particular facts.” *Id.* at n. 7.

16 Regarding the first two factors, the government had no individualized knowledge or suspicion
17 of Mr. Hammond prior to deploying the NIT. Although it had identified a “category of persons it
18 had reason to believe were involved in the type of illegal conduct being investigated”—specifically
19 users of the Playpen site—the government knew nothing of Mr. Hammond’s “criminal background
20 or propensity” when it “initiated its sting operation.” *Id.* at 304.

21 More critically, the government played an essential role in creating the crime here because
22 the government continued operating the site—and facilitating the distribution of child
23 pornography—once it seized the Playpen server in North Carolina in January 2015. Although the
24 Ninth Circuit explained in *Black* that the government’s role in creating a crime is less problematic
25 when the government merely “attached itself” to an “established and ongoing” criminal enterprise,
26 that is not what happened here. *Id.* at 305. The government did not merely attach itself to a criminal
27 enterprise but *became* the criminal enterprise.

1 The fourth and fifth *Black* factors look to the government’s encouragement of criminal
2 activity and its participation in the crime, specifically focusing on the duration and nature of the
3 government’s participation and whether the government’s participation was necessary—that is
4 whether the defendants would have been able to “commit such a crime without the government’s
5 intervention.” *Black*, 733 F.3d at 308. By running the Playpen website for two weeks, the
6 government both encouraged and actively participated in the distribution of child pornography,
7 facilitating crimes that otherwise would simply not have occurred if the site had been shut down
8 immediately when seized. As a result, the government is responsible for the active distribution of
9 the 9,000 images, 200 videos, and 13,000 links made available on Playpen between February 20 and
10 March 4, 2015. Exh. B at 2-3.

11 The final *Black* factor looks at “the need for the investigative technique that was used in light
12 of the challenge of investigating and prosecuting the type of crime being investigated.” *Black*, 733
13 F.3d at 309. The government has argued their decision to run the Playpen website was justified
14 because but for deploying the NIT, they would not have been able to identify the individual users of
15 the Playpen site since the site was only accessible through Tor. Exh. A at ¶ 31 (given the nature of
16 Tor, “other investigative procedures that are usually employed in criminal investigations of this type
17 have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried”).
18 And while shutting down the website once seized “would have ended the trafficking of child
19 pornography taking place via Website A, it would have also prevented law enforcement from
20 attempting to locate and identify its users, who were the ones who possessed, and were distributing
21 and receiving, those illicit materials.” Exh. B at 5-6. But that was not true for the Playpen site.

22 Once the government seized the server hosting the Playpen site, it possessed a wealth of
23 information it could use to criminally prosecute users without resorting to operating the site for two
24 weeks in order to deploy the NIT. After all, the government was ultimately able to indict the
25 administrators of the site in North Carolina *before* it deployed the NIT. Even if the government
26 wanted to deploy an NIT, it could have done so without also rendering the Playpen site functional.
27 It could have, for example, disabled access to the images of child pornography, turned off the ability
28

1 to upload pictures or videos, or even just run the site for a much shorter period of time.

2 Most critically, so far the government has charged 137 defendants in connection with this
3 investigation. Exh. B at 7. That number is less than 1% of the 158,094 total members that Playpen
4 had on February 3, 2015. See Exh. A at ¶ 11. Notably, that percentage is the same percentage of
5 true IP addresses the government admitted in the NIT warrant it was able to identify before deploying
6 the NIT. Specifically, the government explained the “true IP addresses of a small number of users
7 of the TARGET WEBSITE (that amounted to less than 1% of the TARGET WEBSITE) were
8 captured in the log files stored on the [seized] server.” *Id.* at ¶ 29 n. 7. Given the end results, the
9 government did not need to keep the site up for two weeks in order to locate, investigate and
10 prosecute 1% of the individual users of the Playpen site.

11 Thus, considering all of the *Black* factors, the government acted outrageously when it decided
12 to operate Playpen for two weeks, facilitating thousands of users to commit crimes that otherwise
13 would not have occurred, in order to prosecute a tiny fraction of those users—in fact, roughly the
14 same fraction it could have prosecuted without running the website. The indictment should therefore
15 be dismissed.

16 **B. Operating Playpen Harmed the Innocent Victims of Child Pornography Offenses.**

17 “Governmental ‘investigation’ involving participation in activities that result in injury to the
18 rights of its citizens is a course that courts should be extremely reluctant to sanction.” *Archer*, 486
19 F.2d at 677. The harm to innocent third parties is especially crucial in the context of undercover
20 child pornography investigations. Government conduct that encourages others to commit real child
21 pornography crimes “raises very serious concerns with respect to the rights of third parties—namely,
22 the rights of the children Congress sought to protect in enacting the prohibitions on child
23 pornography.” *United States v. Chin*, 934 F.2d 393, 399 (2d Cir. 1991). Thus, the Second Circuit
24 has warned “law enforcement agents to think twice before engaging in investigative techniques that
25 encourage individuals to commit actions that harm innocent third parties.” *Id.* at 400.

26 The government has repeatedly emphasized in press releases how “[y]oung victims are
27 harmed every time an image is generated, every time it is distributed, and every time it is viewed.”
28

1 United States Attorney’s Office, Central District of California May 27, 2016 Press Release, *Actor*
2 *Named in Federal Indictment Alleging Receipt and Possession of Child Pornography on his*
3 *Computer and Flash Drive.*⁵ The government invokes similar language in its sentencing memoranda
4 to argue for lengthy maximum sentences for possession of child pornography, repeatedly citing the
5 fact that victims experience the “powerlessness, pain, and humiliation that accompany the pervasive
6 feeling that the original abuse is being repeated each time the images are viewed.” *United States v.*
7 *Wallace*, No. 15-CR-00160-CRB, Doc. 20, United States’ Sentencing Memorandum (N.D. Cal. Sept.
8 4, 2015) at 11. In a 2010 Report to Congress, the DOJ expanded on its view, stating that victims
9 “suffer not just from the sexual abuse graphically memorialized in the images, but also from a
10 separate victimization, knowing that the images of that abuse are accessible, usually on the Internet,
11 and are traded by other offenders who receive sexual gratification from the children’s distress.”
12 Department of Justice, *The National Strategy for Child Exploitation Prevention and Interdiction: a*
13 *Report to Congress* (Aug. 2010) at 9.

14 Unsurprisingly, courts have embraced the DOJ’s position. Images of child pornography are
15 “a permanent record” of a child’s abuse and “the harm to the child is exacerbated by their
16 circulation.” *New York v. Ferber*, 458 U.S. 747, 759 (1982). “It is common ground that the victim
17 suffers continuing and grievous harm as a result of her knowledge that a large, indeterminate number
18 of individuals have viewed and will in the future view images of the sexual abuse she endured.
19 Harms of this sort are a major reason why child pornography is outlawed.” *Paroline v. United States*,
20 134 S. Ct. 1710, 1726 (2014) (citations omitted). This harm is why the distribution of child
21 pornography is punished more harshly than the mere possession of child pornography. *Compare* 18
22 U.S.C. § 2252(b)(1) (minimum sentence of five years and maximum sentence of twenty years for
23 distribution of child pornography) *with* 18 U.S.C. § 2252(b)(2) (no minimum and maximum sentence
24 of ten or twenty years for possession of child pornography).

25
26
27 ⁵ Available at [https://www.justice.gov/usao-cdca/pr/actor-named-federal-indictment-alleging-](https://www.justice.gov/usao-cdca/pr/actor-named-federal-indictment-alleging-receipt-and-possession-child-pornography-his)
28 [receipt-and-possession-child-pornography-his](https://www.justice.gov/usao-cdca/pr/actor-named-federal-indictment-alleging-receipt-and-possession-child-pornography-his).

1 Yet remarkably, the government ignored these harms and distributed a significant amount of
2 child pornography by operating the Playpen site for two weeks. In essence, the government
3 committed a more serious crime—distribution of child pornography—in order to apprehend
4 defendants committing the less serious crime of accessing and viewing child pornography.

5 Unsurprisingly, given the harms involved, the small number of undercover child pornography
6 investigations approved by the courts have typically involved far less child pornography than the
7 government’s conduct here. For example, in *United States v. Duncan*, 896 F.2d 271 (7th Cir. 1990)
8 the government sent a brochure to Duncan, offering to sell child pornography. 896 F.2d at 272.
9 After Duncan responded by placing an order for 48 photos, the government mailed him images from
10 its stock of previously seized child pornography images, and then promptly arrested him ten minutes
11 after the images were delivered. *Id.* at 274. The Seventh Circuit found no outrageousness because
12 the third party injury was controlled, as the government only produced a small number of already
13 seized images and Duncan only possessed the images for minutes. *Id.* at 276-77.

14 Similarly in *Chin*, the Second Circuit found no outrageous conduct when postal inspectors
15 solicited defendant to order child pornography and after he responded, ultimately mailed him two
16 magazine covers and then quickly arrested him. *Chin*, 934 F.2d at 396, 399-400.

17 The government’s conduct here, however, was not isolated to a handful of images possessed
18 momentarily. The government’s operation of Playpen for two weeks resulted in an additional 9,000
19 images, 200 videos, and 13,000 links of child pornography being disseminated across the world
20 without any ability to stop the further distribution of this material. The harm caused to these victims
21 is exacerbated by the digital nature of the specific images. “Because child pornography is now traded
22 with ease on the Internet, ‘the number of still images and videos memorializing the sexual assault
23 and other sexual exploitation of children, many very young in age, has grown exponentially.’”
24 *Paroline*, 134 S. Ct at 1717. As far back as 1999, the Department of Justice warned that undercover
25 online investigations

26 may have greater capacity than similar physical-world undercover entities to cause
27 unintended harm to unknown third parties. Because digital information can be easily
28 copied and communicated, it is difficult to control distribution in an online operation
and so limit the harm that may arise from the operation.

1 Department of Justice, *Online Investigative Principles for Federal Law Enforcement Agents* (Nov.
2 1999) at p. 44.⁶

3 Unsurprisingly, the undercover child pornography investigations approved in *Duncan* and
4 *Chin* took place through the physical mail and before the advent of the modern Internet. They also
5 took place before 2006 and the passage of the Adam Walsh Act. *See* Pub. L. 109-248, 120 Stat. 587
6 (Jul. 27, 2006). Under the Adam Walsh Act, the FBI is *prohibited* by federal law from disseminating
7 child pornography outside of the government. For example, under the Adam Walsh Act, in a criminal
8 case any child pornography “shall remain in the care, custody, and control of either the Government
9 or the court.” 18 U.S.C. § 3509(m); *see* Pub. L. 109–248, Title V, § 504, 120 Stat. 629, 631. Not
10 even defense attorneys can obtain a copy of the child pornography for purposes of representing their
11 clients. *See id.* (“Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall
12 deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or
13 otherwise reproduce any property or material that constitutes child pornography...so long as the
14 Government makes the property or material reasonably available to the defendant.”). This statute
15 has survived constitutional challenge because of the nature of child pornography, with the Seventh
16 Circuit stating that “the assertion that § 3509(m) lacks a rational basis is unfathomable.” *United*
17 *States v. Shrake*, 515 F.3d 743, 745 (7th Cir. 2008) (rejecting facial constitutional challenge to §
18 3509(m)); *see also United States v. Wright*, 625 F.3d 583, 614-617 (9th Cir. 2010) (rejecting as
19 applied constitutional challenge to § 3509(m)).

20 Similarly, Congress has directed the National Center for Missing and Exploited Children to
21 alert internet providers of “hash values or other unique identifiers associated with a specific” child
22 pornography image in order to help those providers to identify images and alert the NCMEC. 18
23 U.S.C. § 2258C(a)(1). But Congress prohibited the NCMEC from disclosing “actual images” of
24 child pornography to the Internet providers for the same reason it prohibited access to defense
25 attorneys: because “Congress is entitled to reduce the number of copies in circulation” of child
26 pornography. *Shrake*, 515 F.3d at 746; *see also* 18 U.S.C. § 2258C(a)(3).

27 _____
28 ⁶ Available at <https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf>.

1 Yet despite their awareness of this risk, the government here allowed thousands of images to
2 be viewed and distributed to thousands of individuals outside of the government (and outside the
3 country) during the two weeks it ran the Playpen website, harming the victims in those images in
4 ways that will have ramifications for a lifetime. Causing this harm to innocent third parties is
5 outrageous government conduct that should result in dismissal of the indictment.

6 **CONCLUSION**

7 For the reasons stated above, the Court should dismiss the indictment due to outrageous
8 government conduct.

9
10 DATED: August 4, 2016

STEVEN G. KALAR
Federal Public Defender

11
12 /S/
HANNI M. FAKHOURY
Assistant Federal Public Defender

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,)	DECLARATION OF HANNI M.
)	FAKHOURY IN SUPPORT OF MOTION
12 v.)	TO DISMISS FOR OUTRAGEOUS
)	GOVERNMENT CONDUCT
13 DUMAKA HAMMOND,)	
)	Date: September 8, 2016
14 Defendant.)	Time: 10:30 a.m.
)	

- 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 United States’ Response to Order Compelling Discovery, Docket
 - 25 number 109 in *United States v. Michaud*, 15-CR-5351-RJB (W.D. Wash. Jan. 8, 2016). I
 - 26 obtained this document from the Western District of Washington’s CM/ECF system on
 - 27 August 3, 2016.

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

2 DATED: August 4, 2016

3 
HANNI M. FAKHOURY

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

EXHIBIT A

U.S. v. DUMAKA HAMMOND

CR-16-102-JD

MOTION TO DISMISS THE
INDICTMENT FOR OUTRAGEOUS
GOVERNMENT CONDUCT

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

Alexandria Division

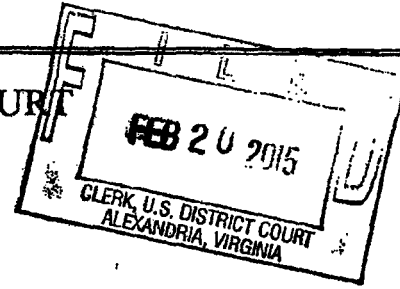
IN THE MATTER OF THE SEARCH) FILED UNDER SEAL
OF COMPUTERS THAT ACCESS)
upf45jv3bziuctml.onion) Case No. 1:15-SW-89

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 upf45jv3bzuiuctml.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.

Theresa Carroll Buchanan United States Magistrate Judge

Date: 02/20/2015

Theresa Carroll Buchanan 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)
upf45jv3bz1uctml.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

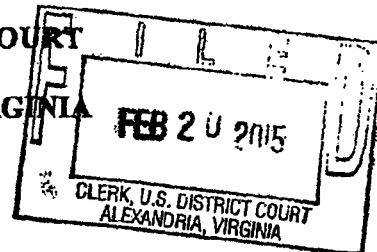
From any “activating” computer described in Attachment A:

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, 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 [REDACTED] in January 2015 and a copy of the server (hereinafter the "TARGET SERVER") that was assigned IP Address 192.198.81.106 was seized. FBI Agents reviewed the contents of the Target Server and observed that it contained a copy of the TARGET WEBSITE. A copy of the TARGET SERVER containing the contents of the TARGET WEBSITE is currently located on a computer server at a government facility in Newington, VA, in the Eastern District of Virginia. Further investigation has identified a resident of Naples, FL, as the suspected administrator of the TARGET WEBSITE, who has administrative control over the computer server in Lenoir, NC, that hosts the TARGET WEBSITE.

29. While possession of the server data will provide important evidence concerning the criminal activity that has occurred on the server and the TARGET WEBSITE, the identities of the administrators and users of the TARGET WEBSITE would remain unknown without use of additional investigative techniques. Sometimes, non-Tor-based websites have IP address logs that can be used to locate and identify the board's users. In such cases, a publicly available lookup would be performed to determine what ISP owned the target IP address, and a subpoena would be sent to that ISP to determine the user to which the IP address was assigned at a given date and time. However, in the case of the TARGET WEBSITE, the logs of member activity will contain only the IP addresses of Tor "exit nodes" utilized by board users. Generally, those IP address logs cannot be used to locate and identify the administrators and users of the TARGET WEBSITE.⁷

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

⁶ Based on my training and experience, "scat" refers to sexually explicit activity involving defecation and/or feces.
⁷ [REDACTED] the true IP
Addresses of a small number of users of the TARGET WEBSITE (that amounted to less than 1% of registered users

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

THE NETWORK INVESTIGATIVE TECHNIQUE

31. Based on my training and experience as a Special Agent, as well as the experience of other law enforcement officers and computer forensic professionals involved in this investigation, and based upon all of the facts set forth herein, to my knowledge a network investigative technique ("NIT") such as the one applied for herein consists of a presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location and identity of those users and administrators of the TARGET WEBSITE described in Attachment A who are engaging in the federal offenses enumerated in paragraph 4. Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or "nodes," as described herein, other investigative procedures that are usually employed in criminal investigations of this

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

type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

32. Based on my training, experience, and the investigation described above, I have concluded that using a NIT may help FBI agents locate the administrators and users of the TARGET WEBSITE. Accordingly, I request authority to use the NIT, which will be deployed on the TARGET WEBSITE, while the TARGET WEBSITE operates in the Eastern District of Virginia, to investigate any user or administrator who logs into the TARGET WEBSITE by entering a username and password.⁸

33. In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the TARGET WEBSITE, which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the TARGET WEBSITE, located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

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

⁸ Although this application and affidavit requests authority to deploy the NIT to investigate any user who logs in to the TARGET WEBSITE with a username and password, in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation, in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users, such as those who have attained a higher status on Website 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.

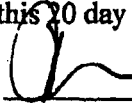
49. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of these crimes.

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: <i>Between 2/20/15 and 3/4/15</i>	Copy of warrant and inventory left with: <i>N/A</i>
Inventory made in the presence of: <i>N/A</i>		
Inventory of the property taken and name of any person(s) seized: <i>Data from computers that accessed TARGET WEBSITE between 2/20/15 and 3/4/15</i>		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: <i>March 31, 2015</i>	 <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> <i>Executing officer's signature</i>	
	<i>Special Agent FBI, Daniel I. Alfin</i> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> <i>Printed name and title</i>	

EXHIBIT B

U.S. v. DUMAKA HAMMOND

CR-16-102-JD

MOTION TO DISMISS THE
INDICTMENT FOR OUTRAGEOUS
GOVERNMENT CONDUCT

Judge Robert J. Bryan

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

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,

Plaintiff,

v.

JAY MICHAUD,

Defendant.

NO. CR15-5351RJB

UNITED STATES’ RESPONSE TO
ORDER COMPELLING DISCOVERY

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, Matthew P. Hampton, Assistant United States Attorney for said District, and Keith A. Becker, Trial Attorney, hereby files this response to the Court’s December 15, 2015, order compelling discovery (Dkt. 81):

A. Number of pictures, videos, and links

The Court first ordered the government to provide the defense with the number of child pornography pictures, videos, and links to pictures and videos that were posted on Website A between February 20 and March 4, 2015, “[p]rovided however, if the plaintiff cannot produce the exact picture, video and link totals listed above with reasonable effort, the plaintiff should provide a good faith estimate of the totals.” Dkt. 81, pp. 1-3.

Website A was an online bulletin board through which users provided the content of the site by posting messages and/or replies to messages within categories set up by the site

1 administration. In accordance with the site rules and guidelines, users generally posted textual
2 messages in which “preview” images (generally consisting of still frames taken from a video or a
3 selection of images) were embedded, and that included a link to a URL, the address of a website
4 or server at which the videos or images could be downloaded, along with any password
5 necessary to download and decrypt the videos or images.

6 During the course of the investigation of Website A, before and after its seizure, the FBI
7 expended significant efforts to document and capture as many of the images/videos posted in this
8 fashion by site users as practicable. Given the significant number of users and activity on the
9 website, it was not possible to capture all of that content. To access the images and videos, the
10 agents had to access the website or link contained in the message, download the files or a file
11 “archive” – that is, a compressed file containing numerous other files – and then enter a
12 password in order to access the files. This process could not be automated, meaning that it was
13 necessary for an agent physically to take these steps rather than simply direct a computer to do
14 the work. Moreover, images and videos that were made available by Website A users were
15 generally only available for a limited time. Thus, if the agents were not able to complete
16 accessing all of the website’s advertised materials at or near the time of posting, those materials
17 might no longer be available. With that understanding, we provide the following good faith
18 estimates based upon FBI agents’ downloads of files made available by the users of Website A
19 through their posts and through the seizure of data from the Website A image and file hosts.

20 Through the efforts described above, the FBI recovered approximately 48,000 images
21 and 200 videos that were made available by the site’s at least 184,000 users between the
22 inception of Website A in August 2014 and its seizure on February 20, 2015. In addition, the
23 FBI was able to recover approximately 9,000 images and 200 videos that were made available by
24 Website A users while it operated under FBI administrative control between February 20 and
25 March 4, 2015. The vast majority of those images/videos appeared to depict child pornography
26 or child erotica. In some instances, particularly with respect to sets of images pertaining to a
27 particular child, children were depicted in various states of undress progressing to nudity and/or
28 sexually explicit activity. This is common among child pornography images.

Website A users posted approximately 110,000 links on the website between August
2014 and February 20, 2015. During the period from February 20 through March 4, 2015,

1 Website A users posted approximately 13,000 links on the website. As noted above, links posted
2 by Website A users typically pointed either to encrypted archives containing multiple image or
3 video files of child pornography, or to particular image files depicting child pornography.

4 Although FBI cannot specify exactly how many images and videos were contained within each
5 of those encrypted archives, as noted above, FBI was able to recover approximately 9,000
6 images and 200 videos that were made available by Website A users while it operated under FBI
7 administrative control between February 20 and March 4, 2015.

8 **B. Views and downloads from February 20 through March 4, 2015**

9 The Court next ordered the government to provide the defense with the number of child
10 pornography pictures and videos that were viewed and downloaded from Website A between
11 February 20 and March 4, 2015, or a good faith estimate of these totals. Because of the manner
12 in which Website A works, it is not possible to give an exact total of child pornography images
13 or videos viewed or downloaded by site users during that time period. As noted above, Website
14 A was a bulletin board on which users posted messages with embedded links and preview
15 images. Another user may choose simply to view the preview image that is embedded on a web
16 page without clicking that image or taking an action that would be recorded by Website A.
17 Moreover, there are numerous ways for a user to save or download images contained on a
18 website such as Website A that would not be recorded by the website. For example, a user might
19 “right click” and save an image to the user’s computer. The user could also take a “screen shot”
20 of the computer screen, or go directly to the external website where linked images or videos were
21 contained by typing the URL for the site after leaving Website A, and then entering the
22 appropriate password, and downloading the images/videos. With that understanding, we provide
23 the following good faith estimates.

24 Information about the number of links Website A users clicked on between August 2014
25 and February 20, 2015, before the FBI was in administrative control of the website, is not
26 available. Between February 20 and March 4, 2015, Website A users clicked on approximately
27 67,000 unique links on the website. As explained above, links on Website A typically pointed
28 either to encrypted archives containing multiple image or video files of child pornography, or to
particular image files depicting child pornography. Of those 67,000 links, 25,000 were links to

1 image files, the majority of which appeared to depict child pornography. The remaining links
2 were to websites, which typically contained the sort of encrypted archives described above.

3 **C. Statistics concerning Website A usage between February 20 and March**
4 **4, 2015**

5 The Court next ordered the government to provide the defense with the number of
6 visitors to the site between February 20 and March 4, 2015, the number of total visits, and some
7 measure of the length of visits. Between February 20 and March 4, 2015, approximately
8 100,000 unique user accounts logged in to Website A, and there were approximately one million
9 total logins. An individual could have more than one user account on the site, so it is not clear
10 how many individuals this actually represents. Website A tracked total time spent on the site by
11 each user during the course of the user's membership. From the inception of the website in
12 August of 2014 until March 4, 2015, site data indicate that its more than 200,000 users
13 aggregately spent approximately seven million hours logged into the site. Based on available
14 data and with reasonable effort, the government cannot provide an estimate of the total or
15 average length of site visits between February 20 and March 4, 2015. Providing such figures
16 would require a manual review of every single session by every single site user in order to total
17 the amount of time spent during each session, and then average that amount of time. That
18 manual analysis has been done for Mr. Michaud (via data that have been provided to the defense
19 in discovery pertaining to his use of Website A) and shows that during his fourteen total sessions
20 on Website A between February 21, 2015, and March 2, 2015, Michaud spent approximately
21 sixteen-and-a-half hours on Website A for an average of 1.18 hours per visit. As previously
22 disclosed, Michaud spent a total of approximately ninety-nine hours logged into the site between
23 October 31, 2014, and March 2, 2015.

24 **D. Mitigation efforts**

25 The Court next ordered the government to provide the defense with a summary of any
26 measures that were taken by the FBI or other law enforcement entities to block access to the
27 pictures, videos and links available on or through the Website A between February 20 and March
28 4, 2015.

During the brief period when the FBI assumed administrative control of Website A, the
FBI did not post any images, videos, or links to images or videos of child pornography. Images,

1 videos and links posted by site users both before the FBI assumed administrative control and
2 afterwards, generally remained available to site users.

3 While Website A operated under FBI administrative control, FBI Special Agents
4 monitored all site postings, chat messages, and private messages twenty-four hours per day in
5 order to comply with Title III monitoring requirements and in order to assess and mitigate any
6 risk of imminent harm to children. In the event that FBI Special Agents perceived a risk of
7 imminent harm to a child, agents took actions to mitigate that risk and immediately forwarded
8 available identifying information, including NIT results, to the appropriate FBI office. Specific
9 actions taken in any particular instance were tailored to the specific threat of harm. The
10 particular actions taken by law enforcement agents in response to particular circumstances are
11 protected by a qualified law enforcement privilege, which the United States hereby asserts. In
12 particular, disclosure of this information at this point in time would alert subjects of ongoing
13 investigations to the particular investigative techniques used by law enforcement in response to
14 such circumstances, creating a risk that criminal suspects will recognize and circumvent such
15 techniques in the future and leading to increased danger of harm to the public, including
16 children. The risk of circumvention of an investigative technique if information is released has
17 been recognized as a factor in applying law enforcement privilege to electronic surveillance. *See*
18 *United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1986). In any event, no such actions
19 pertained to any postings or messages involving the defendant's known username, Pewter.

19 **E. Reason for shutting down Website A**

20 The Court also required the government to produce the reasons the site was shut down on
21 March 4 (rather than earlier or later). As the government explained to the two separate judges
22 who authorized the NIT and the Title III authorization to monitor site users' communications, the
23 fourteen-day period during which the FBI allowed the operation of Website A to continue was
24 necessary in order to deploy the court-authorized NIT to identify users of this site who, like Mr.
25 Michaud, used Tor to conceal their identity, location, and illegal conduct. Without using the
26 NIT, the identities of the users of Website A would remain unknown because, unlike a non-Tor
27 website, any IP address logs of user activity on Website A would disclose only Tor "exit nodes,"
28 which could not be used to locate and identify the actual administrators or users of the site.
Further, because of the unique nature of the Tor network and the method by which the network

1 routes communications through multiple other computers, investigative procedures that are
2 usually employed in criminal investigations of this type were tried and failed or reasonably
3 appeared to be unlikely to succeed.

4 The government demonstrated the necessity of the investigative strategy and technique
5 used in this investigation in the affidavit submitted in conjunction with its Title III authorization.
6 As the government indicated in that affidavit, agents considered seizing Website A and removing
7 it from existence immediately and permanently. In the judgment of law enforcement agents,
8 while doing so would have ended the trafficking of child pornography taking place via Website
9 A, it would have also prevented law enforcement from attempting to locate and identify its users,
10 who were the ones who possessed, and were distributing and receiving, those illicit materials. It
11 also would have frustrated agents' attempts to obtain information that could help identify and
12 rescue child victims from ongoing abuse. Accordingly, it was the judgment of law enforcement
13 that the seizure and continued operation of Website A, for a limited period of time, paired with
14 the court-authorized deployment of a NIT and monitoring of user communications, was
15 necessary and appropriate in order to identify Website A users. The judges who signed the NIT
16 warrant and Title III authorization obviously agreed.

17 To be sure, shutting down a facility such as Website A would have prevented its
18 unidentified users from continuing to post and disseminate child pornography through that
19 website, but it would not prevent those users from continuing to unlawfully possess and
20 disseminate child pornography by other means. Website A users engaged in that sort of activity
21 before the FBI seized and shut down Website A, and those users who were not identified and
22 apprehended undoubtedly continued to engage in that activity after Website A was shut down,
23 often through other online facilities. For instance, before the February 20, 2015, seizure of
24 Website A, it contained at least 184,000 active user accounts, 103,000 posts, and facilitated
25 access to thousands of images and videos of child pornography. There are currently child
26 pornography bulletin boards operating on the Tor network that are similar in structure and
27 function to Website A, that contain hundreds of thousands of user accounts, tens of thousands of
28 postings, and which facilitate access to thousands of images and videos of child pornography.
Law enforcement agents can view and document those websites, their contents, and the child
pornography images and videos trafficked through them – but because they operate as Tor

1 hidden services, the location of the computer servers hosting the websites, and the location and
2 identity of their users who are perpetrating crimes against children, and their child victims, are
3 currently unknown.

4 Stopping the unlawful possession and dissemination of child pornography materials by
5 particular individuals, and rescuing children from the ongoing abuse and exploitation of
6 individual perpetrators, therefore requires more than just shutting down one facility through
7 which such materials are disseminated. Law enforcement must identify and apprehend the
8 perpetrators. Here, the FBI briefly assumed administrative control over an existing facility
9 through which users were already posting and accessing child pornography, for a limited period
10 of time, in order to deploy a court-authorized investigative technique and engage in court-
11 authorized monitoring of user communications, which were necessitated by the particular
12 anonymizing technology deployed by the users of the site, in an effort to identify those
13 perpetrators. This difficult decision, which was disclosed both to the magistrate who approved
14 the NIT and the district judge who approved the Title III monitoring, was amply justified by the
15 particular facts of the investigation.

16 During the government's operation of Website A, regular meetings were held to discuss
17 the status of the investigation and identification of site users and assess whether the site should
18 continue to operate, based upon a balancing of various factors, to include site users' continued
19 access to child pornography, the risk of imminent harm to a child, the need to identify and
20 apprehend perpetrators of those harms to children, and other factors such as those described
21 above. On March 4, 2015, it was determined that the balance of those factors weighed in favor
22 of shutting down the website.

23 **F. Statistics concerning charges**

24 Although it is not reflected in the Court's written order, during the December 11, 2015,
25 hearing the court also stated: "[i]f specifics are not available, I think also the number of charges
26 arising from this investigation should be – the numbers, only numbers, I am saying – should be
27 provided to the defense." Dec. 11, 2015, Tr. at 34. The investigation into users of Website A
28 remains ongoing. To date, at least 137 individuals in the United States are known to have been
charged in connection with the underlying investigation of Website A. That includes thirty-five
individuals who have been determined to be "hands on" child sexual offenders, and seventeen

1 individuals who have been determined to be producers of child pornography. More importantly,
2 twenty-six child victims have been identified or recovered from abuse. Individual charging
3 decisions are made at the discretion of United States Attorneys' Offices and/or appropriate state
4 authorities and this does not represent a complete reporting of all individuals who could be
5 charged in connection with the investigation.

6 **G. Documents regarding FBI administrative control of Website A**

7 Although the Court also ordered the government to provide: "All documents relating to
8 review and authorization of the FBI's administrative control of the site by the Department of
9 Justice or other governmental agencies that were involved in the 'Website A' investigation and
10 deployment of the NIT at issue in our case," the Court qualified its directive, stating: "Provided
11 further, that the government need not provide to defense counsel any documents under the above
12 requirement that constitute reports, memoranda, or other internal government documents made
13 by an attorney for the government or other government agent in connection with investigating or
14 prosecuting this case[.] FRCP 16(a)(2)." Dkt. 81 at pp. 2-3.

15 Discovery materials already provided, including the NIT search warrant and the Title III
16 application paperwork, clearly indicate the scope and purpose of the operation to identify users
17 who were abusing and exploiting children online while masking their location via the Tor
18 network. The NIT search warrant affidavit, which clearly described the operation of the website
19 at a government facility for a limited time in order to identify users, was sworn to by an FBI
20 Special Agent and presented by an Assistant U.S. Attorney from the Eastern District of Virginia
21 and a Trial Attorney with the Department of Justice's Child Exploitation and Obscenity Section.
22 The Title III application and affidavit, which also clearly described the scope and purpose of the
23 operation, including the website's operation at a government facility for a limited period of time
24 in order to deploy a court-authorized NIT to identify users, was submitted by two Department of
25 Justice attorneys, based on an affidavit sworn to by an FBI Special Agent, and approved, as all
26 Title III applications are required to be, by a Deputy Assistant Attorney General of the
27 Department of Justice's Criminal Division.

28 Although the United States is in possession of documents that would be responsive to the
first portion of the Court's order, the United States is not producing those documents at this time
pursuant to the second portion of the Court's order, Federal Rule of Criminal Procedure 16(a)(2),

1 attorney-client, work product and deliberative process privileges. *See United States v.*
2 *Fernandez*, 231 F.3d 1240, 1246-47 (9th Cir. 2000).

3 DATED this 8th day of January, 2015.

4 Respectfully submitted,

5 ANNETTE L. HAYES
6 United States Attorney

STEVEN J. GROCKI
Chief

7
8 /s/ Matthew P. Hampton
9 Matthew P. Hampton
10 Assistant United States Attorney
11 1201 Pacific Avenue, Suite 700
12 Tacoma, Washington 98402
13 Telephone: (253) 428-3800
14 Fax: (253) 428-3826
15 E-mail: matthew.hampton@usdoj.gov

/s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity
Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on January 8, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney of record for the defendant.

/s/ Matthew P. Hampton
MATTHEW P. HAMPTON
Assistant United States Attorney