

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
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOSE ANTONIO ACEVEDO-LEMUS,

Defendant.

Case No.: SACR 15-00137-CJC

**ORDER DENYING DEFENDANT’S
MOTION TO SUPPRESS**

I. INTRODUCTION AND BACKGROUND

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

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

5
6 Playpen operated as a “hidden service” located on an anonymity network known as
7 “The Onion Router,” or “Tor.” (Macfarlane Aff. ¶¶ 6–7.) Ordinarily, public websites log
8 the IP addresses of all visiting users. It is therefore an easy task for law enforcement to
9 discover who has visited a certain website—or, alternatively, which websites a computer
10 with a particular IP address has visited. The Tor network does not operate this way.
11 Instead, to even access the network, a user must first download and install particular
12 software, which subsequently shields the user’s IP address by relaying it among
13 “nodes”—computers run by volunteers all over the world. (*Id.* ¶ 8.) When a user visits a
14 website located on the Tor network—like Playpen, for example—his actual IP address is
15 not shown. Instead, Playpen can only see the IP address of the Tor “exit node”—the final
16 relay computer which sent the user’s communication to Playpen. (*Id.*) This deliberate
17 concealment of IP addresses makes it exceptionally difficult for law enforcement to
18 determine who has visited a website or hidden service located on the Tor network, as
19 there is no practical way to trace a user’s IP address back through the Tor nodes. (*Id.*)

20
21 Once on the Tor network, a user must know a website’s particular web address to
22 visit it. (He may not, as on the traditional or “open” Internet, simply perform an Internet
23 search for certain material, since websites on the Tor network are not indexed like
24 websites on the open Internet.) (Macfarlane Aff. ¶ 10.) Tor users must obtain web

25
26
27
28 ¹ “An IP address is a number that an Internet Service Provider assigns to devices that are connected to the Internet. . . . The Internet Service Provider to which an internet user subscribes can correlate the user’s IP address to the user’s true identity.” *Third Degree Films, Inc. v. John Does 1 through 4*, No. 12-CV-1849 BEN (BSG), 2013 WL 3762625, at *1 (S.D. Cal. July 16, 2013).

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

8
9 Users who entered Playpen’s web address arrived at a main page which contained
10 images of two partially clothed prepubescent females with their legs spread apart, along
11 with text stating, “No cross-board reposts, .7z preferred, encrypt filenames, include
12 preview, Peace out.” (Macfarlane Aff. ¶ 12.) This text apparently referred to a ban on
13 posting material from other message boards, an indication of which file compression
14 method was preferable, and instructions on what to include with posted materials. (*Id.*)
15 Adjacent to the text were fields for users to enter login credentials, and a hyperlink for
16 new users to “register an account with Playpen.” (*Id.*) Upon clicking the “register an
17 account” hyperlink, users were taken to additional text which explained that Playpen
18 required an email address but that rather than entering their real email address, users
19 should simply enter a made-up address: “something that matches the xxx@yyy.zzz
20 pattern.” (*Id.* ¶ 13.) Users who successfully registered for the service by entering a false
21 email address were then taken to a page containing Playpen’s forums and subforums. (*Id.*
22 ¶ 14.)

23
24 Playpen was entirely devoted to the publication and exchange of child
25 pornography. Its forums, where Playpen users could post materials, bore titles such as
26 “Jailbait Videos”² (of both “Girls” and Boys”), “Pre-teen Videos,” “Pre-teen Photos,” and
27

28

² “Jailbait” refers to underage but post-pubescent minors.

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

12
13 The FBI’s review of Playpen’s forums and subforums, as well as its Playpen Image
14 Hosting, Playpen File Hosting, and Playpen Chat features, revealed links to numerous
15 depictions of what appeared to be child pornography. A representative sampling of those
16 depictions is as follows:

- 17
- 18 • An image of a prepubescent or early pubescent female being orally penetrated by
19 the penis of a naked male. (Macfarlane Aff. ¶ 18.)
 - 20 • A video of a prepubescent female, naked from the waist down, being anally
21 penetrated by the penis of a naked adult male. (*Id.* ¶ 18.)
 - 22 • Images focused on the nude genitals of a prepubescent female. (*Id.* ¶ 23.)
 - 23 • A video of an adult male masturbating and ejaculating into the mouth of a nude
24 prepubescent female. (*Id.* ¶ 24.)
 - 25 • An image of two prepubescent females lying on a bed with their genitals exposed.
26 (*Id.* ¶ 25.)
 - 27 • An image of four females, including at least two prepubescent females, performing
28 oral sex on one another. (*Id.* ¶ 25.)

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

12
13 In the normal course of operations, websites send content to visitors. A
14 user’s computer downloads that content and uses it to display web pages on
15 the user’s computer. [Upon deployment of the NIT, Playpen,] which will be
16 located in Newington, Virginia, . . . would augment that content with
17 additional computer instructions. When a user’s computer successfully
18 downloads those instructions from [Playpen], the instructions, which
19 comprise the NIT, are designed to cause the user’s “activating” computer to
20 transmit certain information to a computer controlled by or known to the
21 government.

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

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

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

4
5 (*Id.* ¶ 34.)

6
7 On February 20, 2015, the FBI sought a warrant to deploy the NIT for thirty days.
8 (Dkt. 32 Ex. A [the "NIT Warrant"].) The warrant application explained the nature of
9 Playpen, the investigative difficulties presented by Playpen users' use of the Tor network,
10 the operation of the NIT, and the fact that the NIT could cause activating computers—
11 "wherever located"—to disclose the seven pieces of information noted above. (*See*
12 *generally* Macfarlane Aff.; *see also id.* ¶ 48.) The warrant was signed by Theresa Carroll
13 Buchanan, a United States Magistrate Judge for the Eastern District of Virginia. (NIT
14 Warrant at 1.)

15
16 Deployment of the NIT Warrant revealed that a Playpen user with the username
17 "DarkYogi" viewed at least 175 threads on Playpen during the deployment of the NIT,
18 including at least two threads containing files that appeared to the government to be child
19 pornography. (Dkt. 32 Ex. C at 1–30 ["Wrathall Aff."] ¶ 26.) The first file depicts a
20 nude white prepubescent girl with her mouth open and her hand on an adult male erect
21 penis that appears to be ejaculating into the girl's mouth. (*Id.*) The second file contains a
22 visual depiction of a female white toddler with no pants on being vaginally penetrated by
23 the erect penis of an adult male. (*Id.*) The NIT acquired the IP address of the user's
24 computer, which—a search of publicly available websites revealed—was operated by
25 Time Warner Cable. (*Id.* ¶¶ 27–28.) In March 2015, the government served an
26 administrative subpoena on Time Warner, who indicated that the IP address in question
27 was assigned to Defendant Jose Acevedo at a residence in Anaheim, California. (*Id.*
28 ¶ 29.) The FBI confirmed that Defendant indeed lived at the Anaheim address and then

1 obtained a search warrant authorizing the search of Defendant’s home for evidence of
2 child pornography. (*Id.* ¶¶ 30–33; *see generally id.*) The FBI executed the search,
3 interviewed Defendant, and seized a Hewlett Packard computer with a Western Digital
4 hard drive and a SanDisk Cruzer thumb/flash drive. The hard drive and flash drive were
5 found to contain 210 videos of child pornography and 31 still images of child
6 pornography. A grand jury subsequently returned an indictment against Defendant for
7 two counts of knowingly possessing child pornography. (*See* Dkt. 1.)
8

9 Defendant now moves for the suppression of all evidence stemming from the NIT
10 Warrant. He argues that that warrant (1) violated the Fourth Amendment and
11 (2) exceeded the magistrate’s authority under Federal Rule of Criminal Procedure 41(b).
12 (Dkt. 28.) The Court concludes that the FBI’s acquisition of the key piece of information
13 here—Defendant’s IP address—was not a search under the meaning of the Fourth
14 Amendment, and therefore did not require a warrant. The Court also concludes that in
15 any event, suppression would not be an appropriate remedy for a Fourth Amendment
16 violation in these circumstances. Accordingly, Defendant’s motion is DENIED.
17

18 **II. DISCUSSION**

19 **A. The NIT’s Acquisition of Defendant’s IP Address Was Not a Search**

20 The Fourth Amendment to the U.S. Constitution provides that “[t]he right of the
21 people to be secure in their persons, houses, papers, and effects, against unreasonable
22 searches and seizures, shall not be violated.” “As a prerequisite to establishing the
23 illegality of a search under the Fourth Amendment, a defendant must show that he had a
24 reasonable expectation of privacy in the place searched.” *United States v. Heckencamp*,
25 482 F.3d 1142, 1146 (9th Cir. 2007). A defendant may do so by demonstrating a
26 “subjective expectation that his activities would be private [and that] his expectation was
27
28

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

3
4 **1. Defendant Lacked a Subjective Expectation of Privacy in His IP**
5 **Address Because He Routinely Disclosed It to Others**

6
7 First, Defendant could not have had a subjective expectation that his IP address³
8 would remain private because he routinely disclosed it to third parties, including Time
9 Warner, the Tor network, and websites he visited on the open Internet. “What a person
10 knowingly exposes to the public, even in his own home or office, is not a subject of
11 Fourth Amendment protection.” *Katz v. United States*, 389 U.S. 347, 351 (1967).
12 Applying this principle, the Ninth Circuit has on a number of occasions concluded that
13 Internet users do not have reasonable expectations of privacy in their own IP addresses or
14 the IP addresses of the websites they visit. *See United States v. Forrester*, 512 F.3d 500,
15 510 (9th Cir. 2007) (“Internet users have no expectation of privacy in the . . . IP addresses
16 of the websites they visit because they should know that this information is provided to
17 and used by Internet service providers for the specific purpose of directing the routing
18 information.”); *Heckencamp*, 482 F.3d 1142, 1148 (holding that a defendant had “no
19 reasonable expectation of privacy” in “network logs” that contained his computer’s IP
20 address); *United States v. Martinez*, 588 Fed. Appx. 741 (Mem.) (9th Cir. 2014)
21 (unpublished) (“The use by law enforcement of proprietary forensic software packages
22 that revealed information, such as hash values and IP addresses, did not make the search
23 unlawful, as there was no reasonable expectation of privacy in this information[.] It was
24 available to others, even though they may not have known how to view it.”). Multiple
25

26
27 ³ Although the NIT seized seven pieces of information, the parties apparently agree that the crucial
28 piece of information was Defendant’s IP address. The warrant to search Defendant’s home makes clear
that it was this information, not anything else identified by the NIT, that led the FBI to Defendant.
(Wrathall Aff. ¶¶ 7; 27–33.) The search warrant did not rely on any of the other six pieces of
information, and the Court will limit its analysis to the fruits of the IP address.

1 district courts who have entertained motions to suppress evidence stemming from the
2 NIT Warrant are in accord. *United States v. Matish*, --- F. Supp. 3d ----, 2016 WL
3 3545776, at *21 (E.D. Va. June 23, 2016) (holding that the FBI “did not need to obtain a
4 warrant before deploying the NIT” because the defendant had “no reasonable expectation
5 of privacy in his IP address”); *United States v. Werdene*, --- F. Supp. 3d ----, 2016 WL
6 3002376, at III.B (E.D. Pa. May 18, 2016) (holding that because the defendant “did not
7 have a reasonable expectation of privacy in his IP address, the NIT cannot be considered
8 a ‘search’ within the meaning of the Fourth Amendment”); *United States v. Michaud*,
9 Case No. 3:15-cr-05351-RJB, 2016 WL 337263, at *7 (W.D. Wash. Jan. 28, 2016)
10 (“[The defendant] has no reasonable expectation of privacy of [sic] the most significant
11 information gathered by deployment of the NIT, [his] assigned IP address[.]”); *but see*
12 *United States v. Darby*, --- F. Supp. 3d ----, 2016 WL 3189703, at *6 (E.D. Va. June 3,
13 2016) (concluding that the NIT constituted a search, but noting that the government did
14 not argue otherwise); *United States v. Arterbury*, Case No. 15-CR-182-JHP (N.D. Okla.
15 Apr. 25, 2016) (report and recommendation) (concluding that the defendant had a
16 reasonable expectation of privacy in his IP address because the government obtained the
17 information from his computer, and not from a third party).

18
19 Two peculiar facts in this case—first, that the FBI obtained Defendant’s IP address
20 from his computer, not from a third party, and second, that Defendant *attempted* to
21 obscure his IP address by using the Tor network—do not alter this conclusion.

22
23 First, it does not matter that the government procured Defendant’s IP address from
24 his computer as opposed to getting it from a third party because an IP address is not a
25 private physical feature of a computer, but a commonly disclosed digital one assigned by
26 a third party. When a consumer purchases a computer, takes it home, opens it up, and
27 turns it on, that computer does not have an IP address. Instead, it is assigned an IP
28 address by an internet service provider (like Time Warner) when it connects to a

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

16
17 In that sense this case is very much like *United States v. Knotts*, 460 U.S. 276
18 (1983). There, the government—with a storeowner’s consent—installed a “beeper” in a
19 drum of chloroform subsequently purchased by an individual whom the government
20 suspected of drug production. *Id.* at 277. After the drum was purchased and placed in
21 the trunk of a vehicle, agents followed the vehicle, both maintaining visual contact and
22 monitoring electronic signals from the beeper. *Id.* at 278. Eventually, the vehicle made
23 “evasive maneuvers,” and both visual and electronic contact were lost. *Id.* A helicopter
24 with another monitor later picked up the signal, however, and tracked it to a cabin. *Id.*
25 After performing additional surveillance of the cabin, the government obtained a
26 residential search warrant, based on part on the electronic tracking of the chloroform
27 drum. *Id.* The search revealed a drug lab, and the defendant moved to suppress, arguing
28 that the tracking of the beeper was an unreasonable search.

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

17
18 *Knotts* was recently distinguished by *United States v. Jones*, where the Supreme
19 Court ruled that the warrantless installation of a GPS tracker on a suspect’s car was a
20 search. 132 S. Ct. 945 (2012). That case was different from *Knotts*, the Supreme Court
21 explained, in two ways. First, the beeper in *Knotts* was installed in the drum of
22 chloroform *before* the drum came into the defendant’s possession. In *Jones*, by contrast,
23 the GPS device was installed on a car already owned and possessed by the defendant’s
24 wife. *Jones*, 132 S. Ct. at 952 (reasoning that “Jones, who possessed the Jeep at the time
25 the Government trespassorily inserted the information-gathering device, [wa]s on much
26 different footing” from the defendants in *Knotts* and another beeper case, *United States v.*
27 *Karo*, 468 U.S. 705 (1984).) Second, the *Jones* Court noted the *Knotts* Court’s emphasis
28 on the “limited use” of the beeper, as well as its reservation of the constitutionality of

1 warrantless “dragnet type law enforcement practices,” *see Knotts*, 460 U.S. at 284.
2 *Jones*, the Supreme Court said, involved a long-term, “dragnet-style” search and was
3 therefore not a “limited use” case like *Knotts*. *Jones*, 132 S. Ct. at 952 n.6.
4

5 These two distinctions illustrate why *Knotts*, not *Jones*, is the correct analogue in
6 this case. First, as in *Knotts*, the information-gathering technique used here was
7 originally installed on something controlled by the government—Playpen content—and
8 only then transferred to Defendant’s computer, *at Defendant’s request*. Defendant is
9 therefore “on much different footing” than the defendant in *Jones*, 132 S. Ct. at 952, and
10 instead is like the defendant in *Knotts* who unknowingly purchased the bugged
11 chloroform. And second, the NIT obtained *very* limited information from Defendant’s
12 computer. It did not, for example, search for files containing child pornography or
13 otherwise inspect the computer’s contents. Indeed, its crucial operation was only to
14 acquire a piece of information, normally public and often disclosed to third parties, that
15 Defendant had managed to successfully obscure from the FBI: his IP address.
16

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

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

11 **2. Society Does Not Recognize Defendant’s Expectation as Reasonable**

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

1 III.B (rejecting the defendant’s attempt to “serendipitously receive Fourth Amendment
2 protection because he used Tor in an effort to evade detection”); *Matish*, 2016 WL
3 3545776, at *24 (“[The defendant] should not be rewarded for allegedly obtaining
4 contraband through his virtual travel through interstate commerce on a Tor hidden
5 service.”). Indeed, this Court agrees with the *Matish* court that the government “should
6 be able to use the most advanced technological means to overcome criminal activity that
7 is conducted in secret.” *Matish*, 2016 WL 3545776, at *24. Law enforcement cannot
8 afford to be hamstrung by technologically creative criminals, especially when what is at
9 risk is the sexual exploitation and sadistic abuse of children.

11 **B. Suppression is Unwarranted in Any Event**

12
13 Suppression would not be the proper remedy regardless of whether the FBI’s
14 deployment of the NIT was a search. “[S]uppression is not an automatic consequence of
15 a Fourth Amendment violation. Instead, the question turns on the culpability of the
16 police and the potential of exclusion to deter wrongful police conduct.” *Herring v.*
17 *United States*, 555 U.S. 135, 137 (2009). Defendant argues that the evidence stemming
18 from the NIT Warrant must be suppressed because the NIT Warrant inappropriately
19 authorized an out-of-district search of his computer.⁴ See Fed. R. Crim. P. 41(b) (“[A]

20
21
22 ⁴ Defendant’s alternative argument—that the NIT Warrant failed the Fourth Amendment’s particularity
23 requirement—is without merit. That argument has been rejected, as near as the Court can tell, by every
24 federal court to consider it. See, e.g., *Matish*, 2016 WL 3545776, at *14 (finding that “the NIT Warrant
25 did not violate the Fourth Amendment’s particularity requirement” because “there existed a fair
26 probability that anyone accessing Playpen possessed the intent to view and trade child pornography”);
27 *Michaud*, 2016 WL 337263, at *5 (“Although the FBI may have anticipated tens of thousands of
28 potential suspects as a result of deploying the NIT, that does not negate particularity, because it would
be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor
network.”); *United States v. Epich*, Case No. 15-CR-163-PP, 2016 WL 953269, at *2 (E.D. Wis. Mar.
14, 2016) (concluding that the NIT Warrant satisfied the particularity requirement because it “explained
who was subject to the search, what information the NIT would obtain, the time period during which the
NIT would be used, and how it would be used, as well as bearing attachments describing the place to be
searched and the information to be seized”).

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

3 4 **1. Any Rule 41 Violation Does Not Require Suppression**

5
6 In the Ninth Circuit, suppression is only available for Rule 41 violations if “1) the
7 violation rises to a constitutional magnitude; 2) the defendant was prejudiced, in the sense
8 that the search would not have occurred or would not have been so abrasive if law
9 enforcement had followed the Rule; or 3) officers acted in intentional and deliberate
10 disregard of a provision in the Rule.” *United States v. Weiland*, 420 F.3d 1062, 1071 (9th
11 Cir. 2005). For reasons the Court has already explained, no violation of “constitutional
12 magnitude” has occurred here because Defendant had no reasonable expectation of
13 privacy in his IP address. *See Werdene*, 2016 WL 3002376, at III.B (“Since [the
14 defendant] did not have a reasonable expectation of privacy in his IP address, . . . the
15 violation [of Rule 41] is therefore not constitutional.”). Nor was Defendant prejudiced by
16 any potential Rule 41 violation. After all, the FBI *could* have installed copies of Playpen
17 in every judicial district in the country (there are 94) and then secured a corresponding
18 number of Rule 41 warrants. It only chose not to do so because of the enormous burden
19 and expense of such an undertaking. But the fact remains that the issuance of a modified
20 NIT Warrant that fully complied with even a narrow reading of Rule 41 was entirely
21 possible. Defendant’s argument that he was prejudiced by this search boils down to an
22 assertion that his consumption of child pornography was totally immunized by his use of
23 Tor, and there was nothing the government could do about it. Not so.

24
25 Finally, there is no reason to believe that the FBI intentionally and deliberately
26 violated Rule 41 by seeking the NIT Warrant. As an initial matter, there are credible
27 arguments to be made that Rule 41 was never violated at all, casting doubt on
28 Defendant’s assertion that the FBI was knowingly flouting the Rule. Rule 41(b)(4), for

1 example, provides that a magistrate judge may “issue a warrant to install within the
2 district a tracking device” and that the warrant “may authorize use of the device to track
3 the movement of a person or property located within the district, outside the district, or
4 both[.]” It is not a stretch to say that the NIT functioned as a permissible “tracking
5 device” attached to child pornography that was subsequently downloaded by Defendant
6 when his computer sent a request to the Playpen server. Indeed, at least two district
7 courts have agreed with this position. *See Matish*, 2016 WL 3545776, at *18 (“[T]he
8 NIT Warrant authorized the FBI to install a tracking device on each user’s computer
9 when that computer entered the Eastern District of Virginia . . . [w]hen that computer left
10 Virginia—when the user logged out of Playpen—the NIT worked to determined its
11 location . . . all relevant events occurred in Virginia.”); *United States v. Darby*, ---
12 F. Supp. 3d ----, 2016 WL 3189703, at *12 (E.D. Va. June 3, 2016) (holding that Rule
13 41(b)(4) authorized the NIT Warrant because “[u]sers of Playpen digitally touched down
14 in the Eastern District of Virginia” and the FBI was then entitled to install a tracking
15 device); *but see Michaud*, 2016 WL 337263, at *6 (rejecting the argument that Rule
16 41(b)(4) permitted the NIT Warrant); *United States v. Levin*, --- F. Supp. 3d ----, 2016
17 WL 2596010, at *6 (D. Mass. May 5, 2016) (same). The fact that courts are presently
18 divided over whether the NIT Warrant even violated Rule 41 is compelling evidence that
19 the FBI did not intentionally and deliberately violate that Rule by seeking the warrant in
20 the first instance.

21
22 Moreover, as the government points out, the Supreme Court has recently
23 recommended that Rule 41 be modified to explicitly permit magistrate judges to “issue a
24 warrant to use remote access to search electronic storage media and to seize or copy
25 electronically stored information located within or outside that district if . . . the district
26 where the media is located has been concealed through technological means.” (Dkt. 38
27 Ex. B at 6.) Defendant takes this proposed amendment to mean that the FBI knew it was
28 operating outside Rule 41. But the amendment actually cuts the other way. It would be

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

6 7 **2. The Good Faith Exception Applies**

8
9 Even in the presence of a violation, the good faith exception to the exclusionary
10 rule would bar suppression here.⁵ Application of the exclusionary rule is only
11 appropriate in those “unusual cases” where suppression will “deter police misconduct.”
12 *United States v. Leon*, 468 U.S. 897, 916, 918 (1984). When police officers “acting with
13 objective good faith ha[ve] obtained a search warrant from a judge or magistrate and
14 acted within its scope,” there is “no police illegality and thus nothing to deter.” *Id.* at
15 920–21.

16
17 Here, Defendant’s technical sophistication meant that to adequately prosecute the
18 child pornography laws, FBI agents were required to design a tool that was up to the task.
19 The NIT was the solution. FBI agents were, at every juncture, up front with the
20 magistrate judge about how the NIT worked, what it would seize from “activating
21 computers,” and where “activating computers” could be located. (Macfarlane Aff. ¶ 48.)
22 That Rule 41 may not yet be a perfect fit for our technological world does not mean that
23 the FBI agents here acted in bad faith.

24
25
26
27 ⁵ Traditional limitations on the exclusionary rule, like the good faith exception and the balancing of the
28 costs of suppression against any violation, still apply in the Rule 41 context, since the suppression
provisions of Rule 41 are “no broader than the constitutional rule,” *Alderman v. United States*, 394 U.S.
165, 173 n.6 (1969).

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

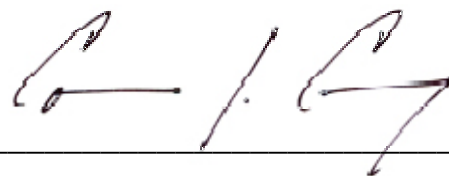
6
7 The [good faith] analysis must also account for the substantial social costs
8 generated by the [exclusionary] rule. Exclusion exacts a heavy toll on both
9 the judicial system and society at large. It almost always requires courts to
10 ignore reliable, trustworthy evidence bearing on guilt or innocence. And its
11 bottom-line effect, in many cases, is to suppress the truth and set the
12 criminal loose in the community without punishment. Our cases hold that
13 society must swallow this bitter pill when necessary, but only as a last resort.
14 For exclusion to be appropriate, the deterrence benefits of suppression must
15 outweigh its heavy costs.

16
17 *Davis v. United States*, 564 U.S. 229, 237 (2011) (internal citations and quotation marks
18 removed). Considering the unspeakable harm caused by child pornography, and the
19 creative and limited conduct of the FBI that was undertaken to mitigate that harm, the
20 Court has no trouble concluding that suppression is entirely unwarranted here.

21 **III. CONCLUSION**

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

23
24
25 DATED: August 8, 2016



26
27 CORMAC J. CARNEY
28 UNITED STATES DISTRICT JUDGE