United States v. Jean

United States District Court for the Western District of Arkansas, Fayetteville Division

September 12, 2016, Decided

Case No. 5:15-CR-50087-001

Reporter
2016 U.S. Dist. LEXIS 123869

UNITED STATES OF AMERICA PLAINTIFF V. ANTHONY ALLEN JEAN DEFENDANT

Notice: Decision text below is the first available text from the court; it has not been editorially reviewed by LexisNexis. Publisher's editorial review, including Headnotes, Case Summary, Shepard's analysis or any amendments will be added in accordance with LexisNexis editorial guidelines.

Opinion

[*1] MEMORANDUM OPINION AND ORDER

Now pending before the Court is a Motion to Suppress Evidence (Doc. 19) filed

under seal by Defendant Anthony Allen Jean. The parties fully briefed the Motion, and on

June 28, 2016, the Court held an evidentiary hearing, at which time the Government and

Mr. Jean each called a witness to testify. The Court then entertained oral argument before

taking the matter under advisement. Now having considered these complex issues

thoroughly, the Court finds that Mr. Jean's Motion to Suppress Evidence (Doc. 19) should

be **DENIED** for the reasons explained herein.

I. BACKGROUND

Mr. Jean was indicted on December 9, 2015 (Doc. 1), on four counts of knowingly

receiving child pornography in violation of *18 U.S.C. §§ 2252(a)(2)* and *(b)(1)*; one count

of knowingly possessing a laptop computer containing images of child pornography in

violation of *18 U.S.C. §§ 2252(a)(4)(B)* and (b)(2); and a forfeiture allegation.

Mr. Jean is accused of downloading child pornography from a website called

"Playpen." The Playpen website operated as a "hidden service" on "The Onion Router,"

which allows users to roam the internet in complete anonymity. In the course of its

investigation, the FBI was able circumvent the anonymity feature-a feat that Mr. Jean now

1

challenges **[*2]** as a constitutionally impermissible violation of his rights under the Fourth

Amendment and the Federal Rules of Criminal Procedure.

The TOR Network, a/k/a the "Dark Web"

A primer of The Onion Router, or "TOR network," for short, is necessary for an

understanding of the issues presented. The Onion Router is so named because of its

onion-like layers of encryption that operate to obscure users' identities. Anyone may download TOR software for free. The TOR browser masks a user's true Internet Protocol ("IP") address by bouncing user communications around a distributed network of relay computers, called "nodes," which are run by volunteers around the world. When a TOR user accesses a website, the IP address of a TOR "exit node" will appear in the website's IP log, rather than the user's actual IP address. Through these mechanisms, the TOR software prevents the tracing of a user's IP address, thereby concealing the identity of the user at every node or "hop" along the information highway.1

The TOR network was originally designed by the United States Naval Research Laboratory to protect intelligence communications online, and legal uses for the network include whistleblowing activities, investigative journalism, **[*3]** activism, and scholarship dealing with such issues as cyber-spying and censorship. Despite these legal uses, TOR has developed a reputation for hosting illicit criminal activity, as well. For this reason, the TOR network of websites-called "hidden services"2-is commonly referred to by TOR users 2 and non-users alike as the "dark web." This name is apt for two reasons. First, the TOR browser enables users to cloak their identities in darkness-like guests to a dimly lit masquerade ball using masks to conceal their faces. Second, the TOR network is an ideal forum for dark, illegal activities to flourish, precisely because TOR users remain masked, and this allows them to escape easy detection by law enforcement.

In his testimony at the motion hearing, FBI Special Agent Dan Alfin explained the TOR network and its hidden services this way:

The Tor network is accessible initially through **[*4]** use of the regular Internet. It runs on top of the regular Internet, and it is made up of hundreds of thousands of computers all around the world.

Tor affords its users two primary uses. The first is the user using the Tor network can use it to connect to a website or other type of Internet service on the regular Internet in an anonymous capability. So a user could use the Tor software or the Tor browser software to connect to a regular Internet website, Google.com, CNN.com, any normal website. In doing so through the Tor network, that website cannot see where you're actually coming from. So if I were to access Google.com from this courtroom using the Tor software, Google would not know that I was here in Arkansas. It may pull an IP address somewhere else in the country or somewhere else in the world. It wouldn't be able to locate me here.

Another use of the Tor network [is] what are referred to as hidden services.

So when you run a website or other Internet service within the Tor network, that service is now referred

[1] This is true with respect to the relay of communications after passing through the first relay node on the distributed network. Technically, however, the user's true IP address is contained on the communication stream to the very first node on the route.

[2] TOR hidden services bear the suffix ".onion" rather than ".com."

to as a hidden service and so when a website is configured to operate as a hidden service, it can only be accessed through use of the Tor software. It can no longer be accessed **[*5]** on the traditional Internet in the manner that you would normally access Google.com. You need to use special [TOR] software to access the hidden service.

And so the hidden service affords the same [ ] benefits that I described earlier in that a user who accesses a hidden service, his or her IP address and other identifying information is concealed. The owner and operator of the hidden service cannot see it. The additional benefit that Tor provides to operators of hidden services is that the true IP address and location of the hidden service [are] similarly concealed . . . . [The operators] could be anywhere in the world. And so Tor hidden services are frequently used to host child pornography websites because of these types of security benefits afforded to operators of such websites, and these are the areas where I focus the majority of my investigative work.

(Doc. 38, pp.16-17).

3

The Playpen Website

In August of 2014, Agent Alfin discovered the existence of the Playpen website-

which was configured as a "hidden service" on the TOR network-and he came to learn

that the website's primary purpose was dedicated to the advertisement and distribution of

child pornography. Because the website operated **[*6]** in complete anonymity on the TOR

network, law enforcement had no readily available means to identify its owner/operator,

much less its users. Then, in December of 2014, the FBI received a serendipitous break.

The Playpen operator inadvertently misconfigured the website's TOR settings during an

update-temporarily deactivating its cloaking mechanism for a few days-which was

enough time for investigators to locate a computer server in North Carolina that was being

used to host the Playpen website. This, in turn, led to the arrest of Playpen's owner on

February 19, 2015, at his residence in Naples, Florida-which further resulted in the FBI

gaining access to the owner's administrative account, and with that came the ability to

control the Playpen website.

The NIT Warrant

But investigators still had no means to identify and locate the website's users, whom

they believed to be downloading and distributing child pornography in violation of federal

law.3 The users' identifying information was purposely unknown to Playpen's owner, and

the users' IP addresses remained concealed because the website was only accessible as

a hidden service on the TOR network, thus providing total anonymity to the users. So the **[*7]**

FBI devised a plan. First, agents made a copy of the Playpen website and placed it on a

government computer server located in the Eastern District of Virginia. Then, after

3*See* Agent Alfin's testimony, *id.* at pp. 36-37.

4

obtaining a search warrant, the FBI re-launched the Playpen website from its own

computer server in Virginia, secretly assuming administrative control over the website for a window of approximately 13 days, from February 20, 2015, to March 4, 2015.

The FBI submitted the application for the search warrant to Magistrate Judge Theresa Carroll Buchanan in the Eastern District of Virginia. *See* Doc. 19-2. The warrant application was supported by a 31-page affidavit signed by Special Agent Douglas Macfarlane. *See* Doc. 19-2, pp. 2-32. In the affidavit, Agent Macfarlane first explained why there was probable cause to believe that users of the Playpen website were committing criminal acts related to the exploitation of children. Agent Macfarlane's affidavit then requested Judge Buchanan to authorize the FBI to deploy computer code, which it refers to as a "Network Investigative Technique" ("NIT"), from its server in Virginia that would be used to host the Playpen website. When a Playpen user's computer (defined **[*8]** in the affidavit and warrant as an "activating computer") would log into the website using a username and password, the NIT would surreptitiously deploy and "cause" the user's "activating computer"-wherever it might be located-to report back certain identifying information to the government's computer on the other end of the line. *Id.* at pp. 30-31.

Judge Buchanan made a finding of probable cause and signed the warrant authorizing use of the NIT to search "[t]he activating computers4 . . . of any user or administrator who logs into the [Playpen] WEBSITE by entering a username and password." *Id.* at p. 34. The warrant's authorization was expressly limited to a period of

5

not more than 30 days. *Id*. The items authorized to be "seized" were expressly identified and limited to the following identifying information:

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 **[*9]** of numbers, letters, and/or special characters) to distinguish data from that of other activating computers, that would 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;5

Attachment B to the warrant, *id.* at p. 35.

Finding of Probable Cause

Judge Buchanan's finding of probable cause was

4 The term "activating computer" is explained in the warrant application to mean the computer of any Playpen user-"wherever located"-who subsequently logged into the website with a username and password. *See* ¶46(a) of the Warrant Application, *id.* at p. 30.

based on Agent Macfarlane's affidavit in support of the search warrant, which provided, in part:

> 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, **[*10]** 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.

Id. at pp. 13-14. Agent Alfin elaborated on this point when he testified at the hearing that it was "incredibly unlikely" that a user would simply stumble upon the Playpen website without knowing the **[*11]** website's illegal purpose. *See* Doc. 38, p. 20.

The FBI's Use of the NIT

Agent Alfin also testified that he had personal knowledge as to how the FBI went about deploying the NIT from the Playpen server onto a user's computer. The NIT was designed to automatically deploy once an activating computer (1) entered the Playpen website via a username and password, and then (2) clicked on a forum link to begin downloading child pornography.6 (Doc. 38, p. 86). The FBI was able to cause the user's computer to report the identifying information by exploiting a defective window in the TOR broswer, through which it ran what amounts to malware7 on the user's computer, with the

5 The MAC address is a unique identifier associated with a particular network adapter, and, in contrast to the IP address, does not change, because it is hardwired into the computer or device itself.

6

6 Although the warrant authorized deployment of the NIT upon the user accessing the website with his username and password, the "FBI further restricted how [it] deployed the technique," and in most instances, the NIT was not deployed until the user actually took the final step to begin the download of child pornography. (Doc. 38, p. 38).

7 Malware means "malicious software." Agent Aflin objects to describing the NIT as malware, because the term has a derogatory connotation, and in fact is used to describe criminal activity when used **[*12]** by a computer hacker for unlawful purposes. Nevertheless, Agent Alfin concedes that when used as a term of art to explain an ethical hacking technique used by law enforcement, the term malware is descriptive of the NIT used here. *See id.* at pp. 39-40. Thus,

where descriptively appropriate, the Court has used the term malware interchangeably with the term NIT.

7

objective being to override the TOR browser's and the user's computer security settings,

and then "cause" the user's computer to return discrete, content-neutral items of

identifying information back to the FBI. *Id.* at pp. 60-61.8

Important to the Court's analysis below is Agent Alfin's testimony that the NIT

deployed and returned the identifying information while the user's computer was (1)

actually online, (2) connected to and actively communicating with the FBI's computer in

Virginia, and (3) while the user was in the process of receiving child pornography. As

Agent Alfin explained:

> As soon as a user clicks on the post, they begin downloading the material from that post. Additionally they download the NIT instructions to their computer, and while the post is still . . . downloading, the NIT does its business and sends the information back to the FBI. **[*13]** This happens very quickly. In the matter at hand, the entire transmission generated by the NIT took place in approximately 0.27 seconds. Again, it happened very quickly because it was just transferring a very limited amount of information . . . .
>
> [T]he NIT would be triggered and deploy and likely complete its task before that page even fully loads.

Id. at pp. 86-87. The entire objective of the NIT transaction was consummated in the blink

of an eye,9 while the user's computer was still in the process of actively downloading child pornography from the computer hosting the Playpen website in Virginia. *See* Doc. 38, pp.

88-89.

The FBI monitored and generated reports of all Playpen user activity during the

authorized period of surveillance.10 The reports contained two sets of data. *See id.* at pp.

8 Although the Defendant's expert, Dr. Christopher Soghoian, testified that he was philosophically opposed to the FBI's use of such "exploits," *id.* at pp. 107-108, 123-125, the Motion to Suppress does not identify the FBI's use of the exploit as a constitutional infirmity.

9 Harvard Database of Useful Biological Numbers, http://bionumbers.hms.harvard.edu

/bionumber.aspx?&id=100706&ver=1 (last visited July 5, 2016) (noting that the average duration of a single eye blink is between **[*14]** 0.1 and 0.4 seconds).

10Although the warrant authorized the NIT to be used for no more than 30 days, the FBI's monitoring of the Playpen website and usage of the NIT actually took place during a 13-day

8

40-41. The first set related to Playpen website usage and included the date each user

registered his account with Playpen, the number of hours that each user was logged into

the website during the monitoring period, and the specific posts each user accessed while

online. None of this data was gathered using the malware, but was instead observed

directly by the FBI through website monitoring.

The second set of data was seized by virtue of the malware causing each user's computer to return the identifying information (without the user's knowledge) to the government's computer in Virginia. This second set of data, as authorized by the warrant, included the user's MAC address, hostname, log-on name, and the activating computer's IP address.

Interestingly though, the user's IP address-the most critical piece of information in locating the user-does not actually reside on the user's computer. IP addresses are assigned by an Internet Service Provider ("ISP")-much like one's residential address is assigned **[*15]** by the postal service. The IP address is maintained on the internet modem that connects an internet device to the internet. *See id.* at p. 43. Ordinarily, one's true IP address can be determined with relative ease because it is always attached, like a "return address," to every "envelope" of information exchanged back and forth by computers that are actively communicating with each other over the internet. But this is not so on the TOR network, where a user's true IP address is intentionally masked by the shuffling of information into different envelopes with different return addresses at each node along the route. Here, the FBI's malware circumvented TOR's veil-simply by causing the user's computer to return the "envelopes" of seized information to the government's computer via the regular internet-which had the clever side effect of causing the user's true "return address" to be written on the envelope.11 With the user's true IP address in hand, the FBI subpoenaed the internet service provider and-in effect-turned on the lights to unmask the user's real location.

The Investigation of Anthony Allen Jean

Agent Alfin testified that the Playpen website **[*16]** was accessed thousands of times during the 13 days it was monitored by the FBI. *Id.* at p. 65. As to the specific investigation of Defendant Anthony Allen Jean, Agent Alfin testified that on March 1, 2015, an individual logged into the Playpen website with the username "regalbegal" and used the website index to select a forum dedicated to "Preteen Videos-Girls Hardcore." *Id.* at pp. 44-45. There, regalbegal allegedly opened a post that purported to contain images of prepubescent female children engaged in penetrative sexual activity. Once regalbegal opened this post, the NIT protocol was triggered, and, unbeknownst to regalbegal, the malware deployed from the Playpen server in Virginia to his computer. According to Agent Alfin, in 0.27 seconds, while regalbegal was still actively connected to (and downloading child pornography from) the Playpen server, the malware caused his computer to transmit the information authorized by the warrant back to the government computer server located in the Eastern District of Virginia. And with that return transmission of data over the regular

period from February 20 through March 4, 2015.

9

internet came regalbegal's true IP address.

The Administrative Subpoena

From the IP address alone, and using publically available data, **[*17]** the FBI could

11*See* Agent Alfin's testimony, Doc. 38, p. 92. (explaining that the information "was sent[back] in clear text over the regular Internet). *See also* Dr. Soghoian's testimony, Doc. 38, p. 148. ("The NIT did not harvest the IP address. . . . the NIT harvested . . . information about the computer; . . . It put [the information] in a letter, put the letter in an envelope and sent it back. . . . the contents of the envelope does not include the IP address, and Special

Agent Alfin testified that the government, in fact, did not harvest the IP address from [Mr. Jean's] computer; they merely looked to see where the NIT response came from and assumed that was the IP address for the defendant.").

10

determine the region of the country where regalbegal resided, as well as the particular ISP,

Cox Communications ("Cox"), associated with his IP address. The FBI then sent an

administrative subpoena to Cox, and Cox provided the FBI with the name and residential

address affiliated with regalbegal's IP address.

The Residential Search Warrant

Soon after obtaining this subscriber information, law enforcement applied to

Magistrate Judge Erin L. Setser of the Western District of Arkansas for a residential **[*18]** search

warrant (Doc. 19-1) to be executed at Mr. Jean's residence.12 The warrant was signed on

July 8, 2015, and executed on July 9, 2015. When the FBI first arrived at the residence,

they advised Mr. Jean that they had a search warrant, but they did not volunteer that they

had located his whereabouts by tracing his IP address. Mr. Jean apparently cooperated

with investigating agents and allegedly made incriminating statements both at the time of

his arrest and later during an interview on July 17, 2015. His computer equipment was

seized at that time, and a later search revealed that the computer contained images of

child pornography.

The Motion to Suppress

After charges were brought some five months later, Mr. Jean was arrested and

ordered detained on December 15, 2015. On March 21, 2016, his attorney filed the instant

Motion, challenging the validity of the Virginia search warrant and seeking to suppress all

physical evidence seized from Mr. Jean's computer and related equipment, as well as any

alleged incriminating statements he made to law enforcement as "fruit of the poisonous

tree." Mr. Jean maintains that the Virginia search warrant did not authorize use of the NIT

to search any activating **[*19]** computer outside the Eastern District of Virginia, and as his

12 Mr. Jean does not separately contest the validity of the administrative subpoena or the residential warrant in his Motion to Suppress.

11

computer was located outside that district, the search was not authorized. He also argues

that the Virginia warrant was issued in violation of Federal Rule of Criminal Procedure

41(b), which outlines the scope of a magistrate judge's authority to issue search warrants.

Lastly, he contends that the search warrant itself was not supported by probable cause.

The Government filed a Response to the Motion, and both sides supplied the Court with recent persuasive authority from other district courts that have considered the validity of this very same search warrant. In the following discussion, the Court will analyze whether the Virginia search warrant validly comported with the requirements of the Fourth Amendment; whether the magistrate judge who authorized the warrant did so in violation of *Rule 41(b)*; and, finally, if a violation of *Rule 41(b)* did occur, whether suppression of the evidence is the appropriate remedy.

II. DISCUSSION

A. Did the NIT Warrant Comply with the *Fourth Amendment*?

1. Was the NIT Warrant Even Necessary?

Mr. Jean **[*20]** has offered several arguments as to why the Virginia warrant failed to comply with the *Fourth Amendment* and the Federal Rules, and the Court will reach those arguments in due course. However, it seems prudent at the start of the discussion to consider whether it was even necessary for law enforcement to obtain this search warrant at all. The question is somewhat academic, since the FBI did, in fact, make an application for a search warrant, apparently believing it to be necessary, and did obtain the warrant before utilizing the NIT protocol on the Playpen website. Nevertheless the Court begins by asking whether an alleged Playpen user like Mr. Jean had any legitimate expectation of privacy in his IP address-the sole piece of information that led investigators to his door.

Agent Alfin confirmed on the stand that the FBI was able to locate the residential address of the Playpen user named regalbegal by using *only* his IP address. In fact the[12] only information placed on the administrative subpoena served on Cox was the IP address in question, and the date and time it was collected. The rest of the information reported by the NIT (including regalbegal's MAC address, host name, and operating system) potentially could **[*21]** have been helpful to the FBI if there had been a question as to which of several computers or electronic devices in the residence had been accessing Playpen.[13]

But no such question exists in Mr. Jean's case, because once investigators arrived at his home, he immediately confessed to accessing child pornography and pointed out the computer he had used. Even if the Court were to determine that Mr. Jean had a legitimate expectation of privacy in all the other information the FBI actually collected from his computer, the question of whether he had a reasonable expectation of privacy in the IP address-which was maintained on his modem and ordinarily accompanied messages sent via the regular internet-is uniquely important because it is only the IP address that gives rise to Mr. Jean's "fruit of the poisonous tree" argument in favor of suppressing the evidence.

The Eight Circuit has explained that, "[a]s a preliminary matter . . . in order to find a violation of the *Fourth Amendment*, there must be a legitimate expectation of privacy in the area searched and the items seized." *United States v. Bach, 310 F.3d 1063, 1066* (8th Cir. 2002) (citing *Smith v. Maryland, 442 U.S. 735, 740 (1979)*). "If there is no legitimate expectation of privacy, then there can be no *Fourth Amendment* violation." *Id.* The Eighth Circuit has never **[*22]** explicitly held that a defendant lacks an expectation of privacy in his IP address and username, unless he has installed a file-sharing program on his computer that makes his files accessible to others. *United States v. Stults, 575 F.3d 834, 842* (8th Cir. 2009). In general, however, "[a] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *United States v. Miller, 425 U.S. 435*, 442-44 (1976).

To access the internet at one's residence, an individual must first go through a network that is either connected to the internet or grants access to the internet. An ISP will generally provide this access and assign the resident an IP address. The IP address can change at any time at the ISP's discretion or at the resident's request. The IP address will give clues as to the identity of the ISP, as well as the region or state where the IP address has been assigned. Although the Eighth Circuit has not had the opportunity to rule on the broader issue of whether an internet user who does not use file-sharing software would otherwise enjoy a legitimate expectation of privacy in his IP address, other courts of appeal have clearly decided **[*23]** the issue, and their opinions are instructive.

Before turning to these more recent circuit court opinions, the Court begins its discussion with a Supreme Court opinion issued 40 years ago. The 1976 case of *United States v. Miller* was one in which the Court held that an individual enjoys no legitimate expectation of privacy in bank records showing his various transactions, including his checks and deposit slips. *Id.* The Court reasoned that when one voluntarily conveys such transactional information to third parties-for example, to multiple banks-one loses any expectation of privacy in those records or transactions. *Id.*

A few years later in 1979, the Court in *Smith v. Maryland* held that an individual has no legitimate expectation of privacy in the list of phone numbers he has dialed from his phone. *442 U.S. at 743-744*. In *Smith*, police had requested that a telephone company

[13] This is because several internet-capable devices in a given household may share a common IP address.

13

install a pen register at its central offices to record all the phone numbers dialed by a particular customer. *Id*. Justice Harry A. Blackmun, writing for the majority in *Smith*, explained that "[a]ll telephone users realize that they must 'convey' phone numbers to the

14

telephone company, since it is through telephone company switching equipment that their calls are completed." *Id*. Since users **[*24]** know this, he reasoned, they should also understand "that their phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills." *Id. at 742*.

An IP address does not "belong to" the user in the sense that it is not associated with the user's personal property and cannot be transported to a new location simply by moving the user's personal computer to that new location. For example, if a user were to take his home laptop computer to a local coffee shop to browse the internet, his IP address would not follow him from his home to the coffee shop. Instead, he would use the coffee shop's IP address when browsing online.

The Third Circuit has definitively held that a person has "no reasonable expectation of privacy in his IP address and so cannot establish a *Fourth Amendment* violation" because IP addresses are routinely conveyed to and from third parties, including ISPs.

United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010). Similarly, the Ninth Circuit, relying on an analogy to the pen register in *Smith*, has determined that IP addresses are not subject to *Fourth Amendment* protection because they "are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in **[*25]** order to direct the third party's servers." *United States v. Forrester, 512 F.3d 500, 510* (9th Cir. 2008) (discussing and comparing to *Smith, 442 U.S. at 742*). Both of these appellate courts concluded that there is no need to obtain a search warrant to capture an IP address because the IP address itself conveys no substantive information about the user or the contents of the user's online communications-just as a pen register, which does not require a warrant to install, only captures "the addressing information associated with phone calls" and not the content of the communications themselves. *See id.* at 509.

15

The Fourth, Tenth, and Sixth Circuits have long held that subscriber information that is provided to an ISP is not protected by the *Fourth Amendment's* privacy expectations, since the subscriber voluntarily conveys that information to the system operator and thus assumes the risk that the company might later provide it to law enforcement if served with an administrative subpoena. *See United States v. Bynum, 604 F.3d 161, 164* (4th Cir. 2010); *United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008)*; *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001). In general, then, "when an individual reveals private information to another, he assumes the risk that this confidant will reveal that information to the authorities, and if that occurs the *Fourth Amendment* does not prohibit governmental use of that information." **[*26]** *United States v. Jacobsen 466 U.S. 109, 117 (1984)*.

Turning now to the thorny issue of whether any of the above cases and legal principles should apply when an internet user has gone to the trouble of downloading TOR software to mask his IP address from public view, a reasonable question to ask is whether the TOR user's expectation of privacy in his IP address may be stronger, or more legitimate, than that of an internet user who has taken no affirmative steps to conceal his IP address. As explained previously, the TOR software operates on top of the regular internet-and in the normal course of using the internet, one's IP address is routinely attached to the back-and-forth transmissions that occur when two computers are actively communicating with each other. This is exactly what happened here when the NIT caused the seized information from Mr. Jean's computer to be transmitted back across the unencrypted regular internet.

16

TOR's encryption works by substituting components of the IP address of each volunteer node as it hops across the internet, but on its very first hop, the TOR user's true IP address is disclosed to the first node computer in the TOR chain. Thus, the user's true IP address is not a complete secret, and the user must necessarily **[*27]** assume some measure of risk that TOR's encryption technology could be defeated and thereby potentially reveal his true IP address. Taking this reasoning to its logical conclusion, the principles behind the decision in *United States v. Miller* would apply: If a user engaged in illegal activity while using TOR, and law enforcement obtained the user's true IP address, it would follow that the user would have no legitimate expectation of privacy in the IP address, as he "[took] the risk, in revealing his affairs to others,"-namely, to both his ISP and the owner of the first node computer in the TOR chain-"that the information [would] be conveyed by that person to the Government." *425 U.S. at 443*. Indeed, the Supreme Court has repeatedly held "that the *Fourth Amendment* does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.*

All of the above authority leads the Court to consider that, if pressed, it could potentially find that the FBI in the instant case was under no legal obligation to obtain a search warrant to discover **[*28]** the residential IP addresses of Playpen users in the manner that it did, as IP addresses are unlikely to be entitled to the same *Fourth Amendment* protections as are the substantive contents of users' computers.[14] However, as the reality of the situation is that the FBI *did* obtain a warrant, and there is no definitive authority in this Circuit as of yet regarding the privacy interests either a general user or a TOR user would have in an IP address, the Court will assume that a warrant was necessary in this case, and will analyze below whether the warrant complied with both the Fourth Amendment and the Federal Rules.

17

2. Was the Virginia search warrant supported by probable cause?

A court **[*29]** reviewing the validity of a search warrant issued by a magistrate judge must make sure "that the magistrate had a substantial basis for . . . [concluding] that probable cause existed." *Illinois v. Gates, 462 U.S. 213, 238-39 (1983)* (internal quotation and citation omitted). The question now becomes whether, under the totality of the circumstances, it was reasonable for the magistrate judge to infer that there was a probability or substantial chance of criminal activity being committed by Playpen users, and that deploying the NIT protocol onto the Playpen website in Virginia would reveal evidence of violations of federal law. *See id.* at 230-31. The Court must bear in mind that "after-the-fact scrutiny by courts of the sufficiency of an affidavit [written in support of a warrant] should not take the form of *de novo* review. A magistrate's 'determination of probable cause should be paid great deference by reviewing courts.'" *Id. at 236* (quoting *Spinelli v. United States, 393 U.S. 410, 419 (1969)*). Further, "so long as the magistrate had a substantial basis for . . . conclud[ing] that a search would uncover evidence of wrongdoing, the *Fourth Amendment* requires no more." *Id.* (internal quotation and citation omitted).

18

Mr. Jean focuses his probable cause argument on his contention that some of the statements made by Agent Macfarlane in the supporting affidavit were either untrue or

[14] This would be a very close call though, because unlike some of the cases cited by the Court, the Government here did not actually obtain the information at issue from a third party. Another important distinction has to do with the source of the information which the defendant seeks to have suppressed. For example, if the MAC address (or any other content derived from a search of the computer) was the subject of suppression, the Court would likely find a warrant necessary because such information wasn't obtained or freely available from a third party, but rather it was seized directly from Mr. Jean's computer. The difference here is that Mr. Jean's true IP address is the one piece of information that wasn't **[*30]** harvested from a search of his computer. In fact, the IP address at issue does not even belong to Mr. Jean. The IP address is assigned by the ISP with the intent and understanding that it will be automatically attached to every transmission of data which is directed across the regular internet.

potentially misleading. For example, Mr. Jean asserts that innocent TOR users could have unknowingly stumbled upon the Playpen website without understanding that it was dedicated to child pornography. He notes that the homepage of the website did not include enough information or images to allow an unsuspecting user to conclude that child pornography lay within. He contends that accessing the Playpen website did not require as many affirmative steps or as much advance knowledge of the content of the site as Agent Macfarlane's affidavit led the magistrate judge to believe. Finally, he maintains that the name "Playpen" might not have signaled to potential users **[*31]** that the site was devoted to advertising and distributing child pornography, since, according to Mr. Jean, the name "Playpen" is more commonly associated with a men's lifestyle magazine that is a knock-off of *Playboy* magazine, featuring legal, adult pornography. *See* Doc. 19-5 (images from *Playpen* magazine and print advertisements for adult strip clubs that use the name "Playpen").

The Court has considered Mr. Jean's arguments as to probable cause and has reviewed Agent Macfarlane's affidavit carefully. Considering Agent Macfarlane's many years of experience and the level of detail contained in the 31-page affidavit, the Court is well satisfied that the information provided to Judge Buchanan about the contents of the Playpen website, the details of the NIT protocol, and the way that the TOR software and TOR network operated afforded her a substantial basis for determining there was probable

19

cause to believe that Playpen users knew about the contents of the site when they logged in, and did so with the intent to engage in illegal acts. Agent Macfarlane's affidavit is neither conclusory, nor "bare-bones," but is instead filled with a wealth of information about the reasons why the NIT protocol provided **[*32]** a minimally intrusive method for revealing the locations of Playpen users. The Court is not persuaded, nor does Mr. Jean directly allege, that Agent Macfarlane sought to deceive the magistrate judge in some manner or intentionally placed demonstrably false information in the affidavit. Instead, it appears Mr. Jean simply disagrees with some of the representations made in the affidavit.15 As the warrant easily meets the totality-of-the-circumstances test for probable cause, it passes constitutional muster on that front.

The Government points out that other Courts of Appeal have held that mere membership in a child pornography website-even without specific evidence of downloading activity-provides sufficient probable cause for a search warrant. *See United States v. Gourde, 440 F.3d 1065,1071 (9th Cir. 2006) (en banc)* (citing *United States v. Martin, 426 F.3d 68, 75 (2d Cir. 2005)*, and *United States v. Froman, 355 F.3d 882*, 890-91 (5th Cir. 2004), for the same proposition). This commonsense rule strikes the

Court as sound and lends further support to the Court's finding that Judge Buchanan had

a substantial basis for concluding that probable cause existed to issue the search warrant

and deploy malware to uncover the hidden IP addresses of individuals who logged in as

members of the child pornography website known as Playpen.

15 After considering **[*33]** the testimony during the motion hearing of both the Government's expert, Agent Alfin, and Mr. Jean's expert, Dr. Soghoian, the Court is further convinced of the accuracy of the representations in Agent Macfarlane's supporting affidavit. Agent Alfin testified that it would be "incredibly unlikely" for any TOR user to accidentally stumble upon the Playpen website without having prior knowledge of its illegal contents. (Doc. 38, p. 20). None of Dr. Soghoian's testimony during the hearing undermined that assertion.

20

3. Did the Virginia search warrant meet the particularity requirement of the

***Fourth Amendment*?**

The next question the Court must answer is whether the search warrant sufficiently

described the place to be searched and items to be seized. According to Mr. Jean, the

cover sheet of the Virginia warrant application requested a search warrant as to persons

or property "located in the Eastern District of Virginia . . . ." *See* Doc. 19-2. His argument

is that the warrant only authorized a search to take place in the Eastern District Virginia,

but the malware actually searched Mr. Jean's computer in the Western District of

Arkansas. He further argues that "a fair reading of the warrant and attachment . . .

[*34] authorize[s] searches of 'activating computers' wherever they may be located *in the*

Eastern District of Virginia, [and that] there is nothing within the four corners of the warrant

that alters its plain language or can reasonably be construed to expand the search

authorization to anywhere in the world." (Doc. 19, p. 7 (emphasis added)).

Essentially, Mr. Jean contends that because the data seized from his computer was

located outside Virginia, it must be suppressed. Mr. Jean's counsel argues: "To state the

obvious, when a warrant authorizes searches in one location, it does not authorize

searches in other locations." *Id.* at p. 6. In support of his argument, he cites to various

cases in which a warrant was issued to search a particular residential address, but officers

searched a different address instead. *See, e.g., Simmons v. City of Paris, Tex.*, 378 F.3d

476 (5th Cir. 2004) (warrant for 400 N.W. 14th Street did not justify search of 410 N.W.

14th Street); *Pray v. City of Sandusky, 49 F.3d 1154 (6th Cir. 1995)* (warrant for 716 Y2

Erie Street, upper level of a duplex home, did not justify search of 716 Erie Street, lower

level of the duplex).

The Government counters that the cases cited to by Mr. Jean are inapposite. The

21

instant case involves an internet-based search, not a search of **[*35]** an apartment building or a duplex. Moreover, the instant search was only triggered after website users voluntarily and remotely accessed a server that was physically located in Virginia. Attachments A and B to the warrant application explain that the NIT protocol and malware would be deployed on "all activating computers" that logged into the website "by entering a username and password." (Doc. 19-2, p. 34).

The Government contends that since the server was located in the Eastern District of Virginia, that jurisdiction was the proper place to seek the warrant, as it had the most significant ties to the known location of the server. According to the Government, a reasonable reading of the warrant's scope means the FBI was granted the authority to deploy the NIT protocol from the server in Virginia to the "activating computer" of any user who logged into the server, no matter the user's physical location. As the entire aim of the NIT protocol was to identify the unknown locations of users who were masking their identities through TOR, the Government maintains it was obvious from the face of the warrant application that the NIT protocol was intended to be deployed to computers in any jurisdiction.

After **[*36]** considering both sides' briefing on this issue, the Court agrees with the Government. The term "activating computer" as used in the exhibits attached to and incorporated into the warrant has a specific meaning and context. The term refers to the computer of any Playpen user who subsequently logged into the website with a username and password. *See* Attachment A to the warrant, Doc. 19-2, p. 34. As stated in the affidavit submitted in support of the warrant request, it is clear that users' "activating computers" are understood to be accessing the website via the internet, and given the anonymity provided by the TOR browser, the users could be located anywhere in the

22

world-which created the necessity of the NIT in the first place. Thus, the context for what the FBI was seeking-and what the magistrate judge knowingly ordered by using this term in her warrant-was authority to search any "activating computer"-"wherever located." *Id*. at p. 30.

The Court therefore finds that the warrant application meets the Fourth Amendment's particularity requirement, as "the items to be seized and the places to be searched [were] described with sufficient particularity as to enable the searcher to locate and identify **[*37]** the places and items with reasonable effort and to avoid mistakenly searching the wrong places or seizing the wrong items." *United States v. Gleich, 397 F.3d 608, 611* (8th Cir. 2005).

B. Did the Virginia warrant satisfy *Rule 41(b)*?

Mr. Jean's next argument is that Judge Buchanan exceeded the authority granted

to her by Rule 41(b) of the Federal Rules of Criminal Procedure in issuing the warrant.

Rule 41(b) authorizes a magistrate judge to issue a warrant only in certain situations, and

that authority is more limited than a district judge's authority.16 In general, a magistrate

judge cannot issue a warrant in her own district to search and seize property located

outside the district, unless certain factual situations are present.

Rule 41(b) provides as follows:

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

16 District judges are not limited by Rule 41(b) as magistrate judges are. Instead, district judges may issue warrants to search property located outside their judicial districts when the requirements of the Fourth Amendment are met. "The Fourth Amendment commands that 'no Warrants shall issue, but upon probable cause, supported by Oath or affirmation.'" United States v. Fiorito, 640 F.3d 338, 345 (8th Cir. 2011) (quoting U.S. Const. amend. IV).

23

(1) a magistrate judge with authority in the district-or if none is reasonably available, a judge of a state court of **[*38]** record in the district-has authority to issue a warrant to search for and seize a person or property located within the district;

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

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

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

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction **[*39]** of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises-no matter who owns them-of a United

States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

The Government argues that the search warrant at issue here met the requirements

of subparts (2) and/or (4) above. According to the Government, Judge Buchanan had

24

authority to issue the warrant under subpart (2) because the NIT constituted "property"17

that was located in the Eastern District at the time the warrant was issued, and that "might move . . . outside the district before the warrant is executed." (Doc. 21, pp. 17-18). The Government also contends that the NIT operated like a "tracking device" described in subpart (4), since the NIT "installed" in the Eastern District of Virginia when users logged into the Playpen website, and then revealed the locations of the users outside **[*40]** the district. *Id.* at p. 18. In response to these arguments, Mr. Jean maintains that subpart (2) does not apply because the "property" to be searched was not the NIT located in the Eastern District of Virginia, but the target information on the users' computers outside the district. *See* Doc. 24, p. 2. As for subpart (4), Mr. Jean disagrees that the NIT was "installed" in the Eastern District of Virginia and argues instead that the NIT installed on the users' computers outside the district.

1. *Rule 41(b)(2)*

The Court has considered the parties' arguments and finds that subpart (2) does not apply, since the "property" that was the target of the warrant was not the NIT itself, but the information collected by the NIT. This information, at least in Mr. Jean's case, was not "located within the [Eastern District of Virginia] when the warrant was issued." Rule 41(b)(2). Therefore, as applied to the facts here, Judge Buchanan had no authority to issue a search warrant under subpart (2) for property that was not within her judicial district when the warrant was issued.

2. *Rule 41(b)(4)*

Having likewise considered the parties' arguments with respect **[*41]** to subpart (b)(4), the Court finds that the FBI's NIT was an electronic tool or technique designed and executed for the purpose of tracking the movement of information both within and outside the Eastern District of Virginia. For the reasons explained more fully below, Judge Buchanan had the authority to issue such a warrant pursuant to *Rule 41(b)(4)*, and thus the seizure in question was not unlawful.

The *In Re Warrant* Case

In reaching its conclusion, the Court has considered the cases Mr. Jean cites in opposition to the Government's arguments. *In re Warrant to Search a Target Computer at Premises Unknown* is a decision issued in 2013 by Magistrate Judge Stephen William *Smith in the Southern District of Texas. 958 F. Supp. 2d 753 (S.D. Tex. 2013)*. *In re Warrant* concerned law enforcement's application for a search warrant to surreptitiously install data extraction software on a computer that was allegedly being used by unknown persons at an unknown location to violate federal laws concerning bank fraud, identity theft, and computer security. *Id. at 755*. Law enforcement had obtained an email address they

[17] *Rule 41(a)(2)* defines "property" to include documents, books, papers, any other tangible objects, and information.

suspected was being used by an individual or individuals engaging in bank fraud and identity theft online. *Id. at 759*. The FBI's plan was to email a malware program to the suspected email address. Once the email was opened and the **[*42]** malware downloaded, the malware would scour the individual's computer for information about the user's web-based activities and his or her physical location, and then send that information back to the FBI.

Id.

26

For a variety of fact-specific reasons not present in Mr. Jean's case, the magistrate judge in *In re Warrant* declined to sign the search warrant authorizing the deployment of malware. First, he found that the government had provided nothing more than "conclusory assurance that its search technique will avoid infecting innocent computers or devices."

Id. This was because the FBI had not been certain about who had access to the email address in question, and could not give the magistrate judge assurances that an innocent user with access to that same email account could avoid being subjected to the malware search. *Id.* By contrast, with respect to the Virginia warrant in Mr. Jean's case, the malware protocol would only deploy *after* a registered Playpen user affirmatively accessed the Playpen server in Virginia and logged into the website with a username and password.

Accordingly, the NIT protocol for the Virginia warrant made it almost impossible for an innocent user to be subjected to the malware search.18 **[*43]**

The second reason given by Judge Smith in declining the warrant was because the malware in that case was invasive-far more so than the malware used in Mr. Jean's case.

The malware in the Texas case was designed to take control of the user's computer's camera and generate photographs of the user, and also generate the latitude and longitude coordinates for the computer's physical location. *Id. at 756*. Judge Smith was concerned that "[i]n between snapping photographs, the Government [would] have real time access to the camera's video feed," which would, in turn, "amount[] to video surveillance." *Id. at 759*. This fact alone provided sufficient grounds for him to refuse to authorize the warrant, since the malware protocol failed to meet established Fourth Amendment standards for video camera surveillance. *Id. at 761*.

18 It appears that in Mr. Jean's particular case, the malware only deployed after the FBI observed the user named "regalbegal" committing a crime in the Eastern District of Virginia by opening a file containing child pornography.

27

The third reason advanced by the Texas court in refusing to issue the warrant was that the malware would have collected a great deal of content-specific data from the target's computer. **[*44]** The warrant authorized a 30-day period of monitoring the target's internet activity and authorized the collection of

"Internet browser history, search terms,

e-mail contents and contacts, 'chat', instant messaging logs, photographs,

correspondence, and records of applications run, among other things . . . ." *Id. at 760*. By

contrast, the protocol for the Virginia warrant in Mr. Jean's case identified and returned

content-neutral information over the course of approximately 0.27 seconds-while the

user's computer in Arkansas was actively communicating with (and in the act of

downloading child pornography from) the Playpen server in Virginia.

Considering the factual circumstances surrounding the Texas warrant, it comes as

no surprise that Judge Smith found the warrant to exceed his authority as set forth in Rule

41(b), primarily because the malware's method of deployment in that case was not

sufficiently targeted to those individuals likely to be committing crimes, nor was it

reasonably limited in time, place, and manner of search.

Opinions Discussing the NIT Warrant at Issue

Setting aside the *In Re Warrant* case, which is too factually distinguishable to be

persuasive of the outcome here, Judge Buchanan's warrant has been **[*45]** the subject of

extensive motion practice across the United States and, fortunately for this Court, has been

the subject of no less than eleven helpful opinions. In six of those opinions, the courts

found that the Virginia warrant was issued in at least technical violation of *Rule 41(b)*-or

else assumed without deciding that there was a technical violation-and, nonetheless,

declined to suppress the evidence. *See United States v. Adams*, 2016 WL 4212079, at

*6 (M.D. Fla. Aug. 10, 2016) (opining that the tracking exception under subpart (4) did not

28

apply, as "the NIT does not track; it searches"; but declining to suppress the evidence

because the *Rule 41* violation was only "a technical or procedural violation"); *United States*

v. Acevedo-Lemus, 2016 WL 4208436, at *7 (C.D. Cal. Aug. 8, 2016) (observing that

"there are credible arguments to be made that *Rule 41* was never violated at all," but

finding that even if the Rule were violated, there was no justification for suppressing the

evidence); *United States v. Werdene*, 2016 WL 3002376, at *11 (E.D. Pa. May 18, 2016)

(refusing to apply the tracking exception because, technically, the defendant's computer

was never physically present in the Eastern District of Virginia and so could not be outfitted

with a tracking device there; but finding "suppression is not the appropriate remedy") (Doc.

27-9, p. 23); *United States v. Epich, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016)*

(Doc. 27-1, p. 23) (adopting report and recommendation **[*46]** of magistrate judge, *see* Doc. 27-

1, and declining to decide whether *Rule 41(b)* had been violated, as "[s]uppression of the

evidence is rarely, if ever, the remedy for a violation of *Rule 41*, even if such a violation has occurred")*; United States v. Stamper*, No. 1:15-CR-00109 (S.D. Ohio Feb. 19, 2016) (finding without explaining that "the NIT Warrant technically violates Rule 41(b)," but concluding that "exclusion is not necessary because there has not been a showing of prejudice or an intentional and deliberate disregard of the Rule") (Doc. 27-4, p. 21); *United States v. Michaud*, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016) (finding that to apply the tracking exception to the NIT protocol "stretches the rule too far" because the defendant's computer was "unlike a car with a tracking device leaving a particular district" and at no point was ever physically present in the Eastern District of Virginia; but conceding that "the arguments to the contrary are not unreasonable and do not strain credulity") (Doc. 27-3, p. 13).

Only two out of the eleven reviewing courts interpreted Rule 41(b)(4) rigidly and

29

found that a violation occurred, and then went so far as to suppress the evidence collected from the search, due to their opinion that Judge Buchanan's apparent lack of jurisdiction rendered the warrant **[*47]** void *ab initio*. *See United States v. Levin*, 2016 WL 2596010, at *6 (D. Mass. April 20, 2016) (suppressing the evidence after finding that Rule 41(b) had been violated, since the FBI's internet transmittal of malware to the defendant's computer was not analogous to "the installation of a tracking device in a container holding contraband . . . regardless of where the 'installation' occurred"); *United States v. Arterbury*, No. 15-CR-182 (N.D. Okla. April 25, 2016) (interpreting Rule 41(b)(4) narrowly and suppressing the evidence as a result, after observing that "[t]he NIT did not track Defendant's computer as it moved," and the warrant "was not for the purpose of installing a device that would permit authorities to track the movements of Defendant or his property") (Doc. 27-8, pp. 16-17).

Finally, in three out of the eleven opinions, two district judges-both from the Eastern District of Virginia-concluded that the warrant was properly issued under Rule 41(b)(4). Judge Robert G. Doumar first considered a motion to suppress the Playpen warrant in *United States v. Darby*, 2016 WL 3189703 (E.D. Va. June 3, 2016) (Doc. 27-11), and he later applied his reasoning from *Darby* to a different defendant making the identical argument in favor of suppression in *United States v. Eure*, 2016 WL 4059663 (E.D. Va. July 28, 2016). In *Darby*, Judge Doumar opined that the warrant authorized something "exactly analogous" to the installation **[*48]** of a traditional tracking device. 2016 WL 3189703, at *12. He believed that "[u]sers of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government about their location." *Id.*

In like fashion, Judge Henry Coke Morgan, Jr., in *United States v. Matish*, 2016 WL

30

354776 (E.D. Va. June 1, 2016) (Doc. 27-10), analogized that "whenever someone entered

Playpen, he or she made 'a virtual trip' via the Internet to Virginia, just as a person logging

into a foreign website containing child pornography makes 'a virtual trip' overseas." 2016

WL 354776, at *18. Continuing the analogy, "the installation [of a tracking device by the

FBI] did not occur on the government-controlled computer but on each individual computer

that entered the Eastern District of Virginia when its user logged into Playpen via the Tor

network. When the computer left Virginia-when the user logged out of Playpen19-the

NIT worked to determine its location, just as traditional tracking devices inform law

enforcement of a target's location." *Id.*

This Court's Ruling

Citing *Levin* and *Arterbury*, ***[*49]*** Mr. Jean argues that the NIT here was "installed" outside

of Virginia, because the NIT was downloaded onto regalbegal's computer in Arkansas. But

such an interpretation of the term "install" sacrifices substance in favor of mere form.

Internet crime and surveillance defy traditional notions of place. An individual may commit

the crime of knowingly receiving child pornography without ever having visited the physical

location of the server containing these images. All acts are committed over the virtual

highways of the internet. And while advances in technology always seem to outpace the

abilities of rules committees to keep up,20 that doesn't necessarily mean that the newer

techniques used here were outside the bounds of *Rule 41(b)*, as presently defined.

It is true that the FBI was not seeking to install a tangible tracking device to some

other physical piece of property, but *Rule 41(b)(4)* is not constrained or limited to traditional

tracking techniques. Applying the definitions in *Rule 41(a)(2)*, a "tracking device" is any

"electronic or mechanical device which permits the tracking of the movement of a person

or object."21 And subpart (b)(4) authorizes the tracking of "property," which is specifically

defined to include the tracking of mere intangible "information." *See Rule 41(a)(2)(A)*.

19 Judge Morgan's explanation of the technology at issue is spoken in the virtual sense. No "individual computer" literally entered and left Virginia, simply because the computer's operator logged into and out of the Playpen server. Instead, a Playpen user would remotely visit the server in Virginia and access images located there. While accessing the images, malware would deploy from Virginia to follow the user's signal back to his computer and identify his IP address.

20It appears the Judiciary Conference's Committee on **[*50]** Rules of Practice and Procedure must have anticipated that courts might have difficulty reconciling the newly evolving technology of electronic surveillance techniques with the current version of the Federal Rules. The Committee therefore updated *Rule 41(b)* to keep abreast of advances in

31

Although the term "device" is not more specifically defined in the Rule, it is a word

commonly used to describe "a tool or *technique* used to do a task." *Device*, American

Heritage Dictionary, *http://www.yourdictionary.com/device#americanheritage* (last visited

September 12, 2016).

Here, the government was essentially seeking authority to conduct a sting operation,

whereby it would re-launch the Playpen website **[*51]** from its own server in Virginia, after which

the FBI would then monitor the flow of electronic information as Playpen users accessed

technology by submitting an amendment to the Supreme Court in October of 2015. The

Court approved the amendment on April 28, 2016, and it is scheduled to take effect on December 1, 2016. The amendment explicitly authorizes magistrate judges to issue warrants that employ remote access techniques to search electronic media, when such media is "concealed through technological means"-exactly the situation in Mr. Jean's case, where Playpen users were using technological means (TOR software) to conceal their IP addresses. Supreme Court of the United States,*http://www.supremecourt.gov*/ orders/courtorders/frcr16_mj80.pdf (last visited July 8, 2016). In light of this new Rule amendment, the Court agrees with the Central District of California in *Acevedo-Lemus* that "[i]t would be strange indeed for the Court to suppress the evidence in this case in the face of a strong signal from the Supreme Court that *Rule 41* should explicitly permit the issuance of warrants like the NIT Warrant." 2016 WL 4208436, at *8.

21 *Rule 41(a)(2)(E)* cross-references this definition from *18 U.S.C. § 3117(b)*.

32

the website for allegedly unlawful purposes. Upon entering this "watering hole,"22 **[*52]** a

user-while still immersed-would become infected with the malware as it was deployed

to the user's computer incident to the process of downloading child pornography.

Looking to the express language of the warrant application before Judge Buchanan,

it was explained that the purpose of the NIT was to secure proof of "the actual location and

identity of the [Playpen] users." (Doc. 19-2, p. 24). When a Playpen user accessed the

website's content, the NIT electronically "augment[ed]" that content with "additional

computer instructions." *Id.* at p. 25. These instructions caused the user's activating

computer to electronically transmit certain identifying information to a computer controlled

by the government. *Id.* at p. 26. As explained above, the simplicity of the NIT was that it

caused this information to be transmitted back to the government over the regular

internet-thus circumventing TOR's encryption-which in turn allowed the government to

track the user's true IP address.

After considering the reasoning set forth above by the various district courts to have

considered Judge Buchanan's authority to issue the warrant in question, this Court is

persuaded that the investigative technique comports with *Rule 41(b)(4)*'s tracking

exception. First, **[*53]** the NIT is an "electronic device" within the meaning of 18 U.S.C.

§3117(b), because it is an investigative tool consisting of computer code transmitted electronically over the internet. Second, the purpose of the NIT was to track the movement of "property"-which in this case consisted of intangible "information," something expressly contemplated by the definition in *Rule 41(a)(2)(A)*.

33

The third requirement is that the device be "install[ed]" within the issuing district. As reflected in many of the opinions addressing Judge Buchanan's warrant, the term "install" is problematic, primarily because-in a more traditional scenario-the tracking of tangible property under *Rule 41(b)(4)* requires the tracking device to be physically attached within the warrant issuing district. But the investigative technique used here was not designed or intended to track a tangible item of physical property. Rather, the NIT was designed to track the flow of intangible property-information-something expressly contemplated by *Rule 41(a)(2)(A)*. So when one uses **[*54]** an intangible technique to track the flow of information, to what does the term "install" refer, and where does "installation" take place?

Mr. Jean argues that the NIT was downloaded onto his computer, and therefore installation occurred in Arkansas. But that statement isn't entirely correct. While it is obviously true that Mr. Jean and his computer were never physically present in Virginia, it is equally accurate that the warrant did not violate *Rule 41(b)(4)*'s jurisdictional boundaries, because law enforcement did not leave the Eastern District of Virginia to attach the tracking device used here.23

The whole point of seeking authority to use a tracking device is because law enforcement does not know where a crime suspect-or evidence of his crime-may be located. In such instances, *Rule 41(b)(4)* allows a magistrate judge to authorize law enforcement's use of electronic tracking tools and techniques. When an unknown crime suspect, or unknown evidence of his crime, is located in an unknown district, it would be nonsensical to interpret the Rule-as Mr. Jean does-to require law enforcement to make application for such a warrant to an unknown magistrate judge in the unknown district. The

22 The Defendant's expert, Dr. Soghoian, described these types of virtual sting operations as "watering holes," because of the propensity of an illicit website to attract users of such contraband. (Doc. 38, p. 118).

23 Nor, to the best of this Court's understanding, was the NIT actually "downloaded" to Mr. Jean's computer-in the sense that something remained installed on the computer until deleted. Instead, the NIT consisted of computer code deployed to Mr. Jean's computer.

The code "ran" on Mr. Jean's computer and **[*55]** "instructed" it to execute a command, *i.e.*, to return identifying pieces of information over the regular internet. But the only thing downloaded onto Mr. Jean's computer, in the sense of remaining on the computer after the fact, was the child pornography.

34

fact that the NIT was purposely designed to allow the FBI to electronically trace the activating computer by causing it to return location identifying information from outside the Eastern District of Virginia-is not only authorized by *Rule 41(b)(4)*, but is the very purpose intended by the exception.

The warrant application alleged that unknown Playpen users would likely access the website server located in Virginia for purposes of engaging in illegal activity. The application sought authority to track the flow of electronic information while these suspected crimes were occurring. It is undisputed that the NIT authorized by the warrant was executed by the FBI from its computer located within **[*56]** the Eastern District of Virginia.

It is also undisputed that *but for* Mr. Jean electronically traveling in search of child pornography to the watering hole in Virginia, the NIT could not have been deployed. Thus, on the facts of this case, the only reasonable interpretation of where the information-tracking NIT was "install[ed]" for purposes of *Rule 41(b)(4)*, is the Eastern District of Virginia, where the tracking device-in this case a string of computer code-was caused to be executed and deployed. The only alternative reading of the Rule would require a finding that magistrate judges do not currently possess authority to issue information-tracking warrants; but such a reading is squarely contradicted by the plain language of Rule 41(a)(2)(A).

Accordingly, for all of these reasons, this Court finds that *Rule 41(b)(4)* is applicable, that Judge Buchanan possessed the authority to issue the warrant on that basis, and that the resulting seizure of evidence was not unlawful.

35

C. Suppression of the Evidence Not Justified Regardless

Even if the Court had agreed with Mr. Jean and found that Judge Buchanan issued the warrant in violation of *Rule 41(b)(4)*, this Court would nevertheless find the violation to be technical in nature, which would **[*57]** not, in any event, justify the suppression of evidence.

1. Fundamental vs. Non-Fundamental Violation

The Court's first step in this analysis is to determine whether the violation of Rule 41(b)-assuming such occurred-was either "fundamental" and rendered the search unconstitutional under traditional *Fourth Amendment* standards, or "non-fundamental."

United States v. Freeman, 897 F.2d 346, 350 (8th Cir. 1990). A fundamental violation would require automatic suppression of the evidence, whereas a non-fundamental violation, where no constitutional error occurred, would not trigger automatic suppression.

Id. A non-fundamental violation would only justify suppression where there was prejudice to the defendant, "in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed," or if the defendant were able to show that law enforcement and/or the magistrate judge demonstrated an "intentional and deliberate disregard of a provision in the Rule." *Id*.

Here, if there was any violation of the Rule at all, it was certainly non-fundamental. The search warrant was constitutionally sufficient in that it was supported by probable cause and satisfied the particularity requirement. *See supra*, Section II.A.2-3. Another indication that the violation **[*58]** was, if anything, non-fundamental, is the fact that the search warrant could have been authorized by an Article III judge, apparently without incident. The crux of Mr. Jean's Motion to Suppress is the *Rule 41(b)* violation. His counsel admitted when pressed by the Court during the motion hearing that a district court judge

36

could have authorized the FBI's warrant application. Furthermore, at least two district court judges in the Eastern District of Virginia have stated in written opinions that they found the search warrant to be constitutionally valid and compliant with *Rule 41(b)(4)*'s tracking-device exception. *See Darby*, 2016 WL 3189703; *Matish*, 2016 WL 354776; *Eure*, 2016 WL 4059663.

If a non-fundamental violation of *Rule 41(b)* occurs, the suppression of evidence is only justified if a defendant can demonstrate that the search might not have occurred if the Rule had been followed. Mr. Jean argues that he has been prejudiced by the search because it led to his arrest and detainment on federal charges. The Government counters that, by Mr. Jean's logic, every defendant could potentially argue he was prejudiced due to a search, even though the underlying search warrant was constitutionally valid. The Court agrees with the Government that a showing of prejudice must require more than **[*59]** the fact that the defendant would have been better off had the search not been conducted at all. The simple fact to which both parties appear to agree is that an Article III judge in the Eastern District of Virginia could have authorized this particular search warrant. For these reasons, Mr. Jean has not convinced the Court that the extreme remedy of suppression is required due to a showing of prejudice.

Turning to the second possible argument Mr. Jean could make in favor of suppression under the *Freeman* test, he must show that law enforcement and/or the magistrate judge evinced an "intentional and deliberate disregard of a provision in the Rule." *897 F.2d at 350*. Initially, the Court notes that Mr. Jean has made no attempt to characterize as improper the magistrate judge's motivations in signing the warrant application. Instead, he suggests that the FBI should have known better than to submit

37

this search warrant to the magistrate judge when she so obviously lacked jurisdiction under *Rule 41(b)* to authorize the search. However, at the time the FBI presented the search warrant to the magistrate judge, at least a good-faith basis existed to allow the officers to believe that the warrant satisfied Rule 41(b)(4), as this Court and others have **[*60]** now endorsed that particular reading of the Rule. Moreover, the warrant was not facially insufficient, and there is no persuasive argument that the FBI failed to carry out the NIT protocol as per the description in the warrant application. For these reasons, Mr. Jean has failed to demonstrate to the Court's satisfaction that law enforcement evinced an intentional or deliberate disregard of a provision in the Rule. Therefore, suppression of the evidence would not be supported even if a non-fundamental violation of the Rule had occurred.

2. The Good Faith Exception

The parties' final argument in their briefing contemplates whether the good-faith exception to the Exclusionary Rule, as announced by the Supreme Court in *United States v. Leon*, would save the evidence here from suppression if the warrant were found to be invalid. 468 U.S. at 922. In light of the Court's previous findings, there is no pressing need to reach this argument at all, as the warrant is, in this Court's view, entirely valid. However, since the parties have so thoroughly briefed this issue, the Court will consider it.

The good-faith exception to the Exclusionary Rule provides that when a search warrant is declared invalid, the evidence obtained **[*61]** as a result of the warrant's execution must not be suppressed if law enforcement's reliance on the warrant was objectively reasonable. In the instant case, Mr. Jean does not suggest that the FBI's search of his computer was not in keeping with the warrant application's written description of how the

38

NIT protocol would function. Neither does Mr. Jean directly allege that Agent Macfarlane's affidavit in support of the warrant was written in such a way as to mislead the magistrate judge about the contents of the Playpen website or the likelihood that users of the site knew in advance the site's content. Mr. Jean does not even maintain that the affidavit's descriptions of TOR's functionality-and the way TOR masked users' IP addresses-were untrue. It appears instead that Mr. Jean's argument boils down to his belief that it was not objectively reasonable for the FBI to rely on the validity of the data returned by the malware. He argues that the FBI failed to encrypt the connection between his computer and the FBI server during the deployment of the malware, and this might have caused the data to be compromised in some way.

Mr. Jean's argument fails to persuade the Court that law enforcement's reliance **[*62]** on the warrant was objectively unreasonable, and really goes more to the weight of the evidence than to the suppression of the evidence. There is simply no indication that law enforcement suspected the warrant was lacking in probable cause or sufficient particularity, or that agents believed the magistrate judge might lack the jurisdictional authority to

authorize the relatively new technology described in the warrant application. Mr. Jean's

speculation that hackers could have corrupted the data in transit, or that the FBI's

unencrypted connection might have led to some irregularity, does not go to the ultimate

question of whether the good-faith exception from *Leon* should apply. The Court therefore

finds that, if somehow the warrant were deemed deficient in some respect, the good-faith

exception would save the evidence from suppression.

39

Ill. CONCLUSION

For the reasons explained herein , the Court finds that Mr. Jean's Motion to

Suppress Evidence (Doc. 19) is **DENIED .**

IT IS SO **ORDERED** on this **f**3~yof September, 2016 .

KS

DISTRICT JUDGE

40

End of Document