UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

UNITED STATES OF AMERICA

VS. CASE NO: 6:16-cr-11-Orl-40GJK

RYAN ANTHONY ADAMS

ORDER

This cause comes before the Court on Defendant Ryan Adams' Motion to Suppress Evidence (Doc. 36), filed June 1, 2016, the Government's Response in Opposition (Doc. 46), filed July 1, 2016, and Defendant's Supplemental Briefing to His Motion to Suppress (Doc. 44), filed June 24, 2016. After reviewing the parties' submissions and following an evidentiary hearing held on July 11, 2016 (Doc. 49), the Defendant's Motion to Suppress is denied.

I. BACKGROUND

Defendant is charged with receipt and possession of child pornography, in violation of Title 18, United States Code, Section 2252A(a)(2)(A) and (a)(5)(B). (Doc. 1). The charges arise from the Government's investigation into a website known as "Playpen," which is a global online forum dedicated to the advertisement and distribution of child pornography. (Doc. 36-1, Ex. 3). Defendant and other users visit Playpen via the anonymous Tor network. (*Id.* ¶ 7). The Tor network is constructed to mask the user's IP address (which may be used to identify the user's physical address) by relaying the user's communication among multiple servers located worldwide. (*Id.* ¶ 8). Hence, a server receiving a query from a Tor network displays the IP address of the last node in the Tor network and thereby conceals the user's IP address. (*Id.* ¶¶ 8, 23, 24). The Tor network

prevents law enforcement from tracing the communication back through the network to the actual user—Defendant in the instant case. (*Id.* ¶ 24). For the same reason, law enforcement cannot subpoena Internet Service Providers ("ISP") to locate the user's physical address. (*Id.*).

On or about February 20, 2015, the computer server hosting Playpen was seized from a web-hosting facility in North Carolina. (Doc. 36-1, Ex. 1, ¶ 12). The website was moved to Virginia and the FBI subsequently operated the server to monitor electronic communications of users of the website. (*Id.*). The United States District Court for the Eastern District of Virginia authorized a search warrant allowing law enforcement officers to deploy a Network Investigative Technique ("NIT") on the Playpen server. (*Id.* ¶ 25). When a user accessed Playpen via the Tor network, the NIT was transmitted back to the user's computer, identified the IP address, and transmitted this information, along with the type of operating system running on the computer, the computer's MAC address, the computer's Host Name, and other data back to a server controlled by law enforcement. (*Id.*; Doc. 36-1, Ex. 3, ¶ 34). Using information generated via the NIT, on March 1, 2015, law enforcement identified Defendant as an individual using the name "Gouki" who had been accessing the Playpen database to retrieve images constituting child pornography. (Doc. 36-1, Ex. 1, ¶¶ 29–31).[1]

On September 11, 2015, law enforcement officers went to Defendant's residence in Florida. (*Id.* ¶ 32). The officers identified themselves to Defendant as FBI Agents, advised Defendant of the nature of the investigation, and requested permission to speak with Defendant. (*Id.*). The agents informed Defendant that he was not required to speak

[1] The affidavit at Doc. 36-1, Ex. 1, ¶¶ 29–30 incorrectly reports the date as February 19, 2015. This mistake was clarified during the evidentiary hearing held on July 11, 2016.

with them. (*Id.*). Defendant consented to be interviewed by the FBI Agents, and he admitted to using the screen name "Gouki" to access, download, and view child pornography. (*Id.*). Specifically, Defendant confessed to using his laptop to access websites containing child pornography, including Playpen. (*Id.*). Defendant admitted to downloading at least twenty movie files containing child pornography and having at one time over 100 files of child pornography. (*Id.*). Defendant provided a detailed description of the types of images he downloaded from various websites, the number of years he has been engaged in this illegal conduct, and that he has used Yahoo! Messenger to chat and share child pornography with others. (*Id.*).

At the conclusion of the non-custodial interview, Defendant voluntarily gave the agents his laptop computer, three CDs, a USB external memory 1.8 Hard Drive, and a 10 Mega External Hard Drive which he stated contained child pornography. (*Id.* ¶ 33). After the agents departed Defendant's residence, Defendant approached the agents who were seated in their vehicle and stated that he would call them if he found other devices containing child pornography. (*Id.*). Later that same day, at approximately 4:30 p.m., Defendant called the agents and informed them that he had another flash drive that he wanted to give to the agents. (*Id.*). The following day, at 10:00 a.m., agents met Defendant in a public location at which time Defendant voluntarily provided agents a PNY 16GB Black Blue USB drive, a Micro SD HC 4G, and a Lexar SD Card 128MB which Defendant said were used to store child pornography. (*Id.* ¶ 34). On September 25, 2015, fourteen days after Defendant confessed to the agents and thirteen days after Defendant gave agents additional data storage devices, FBI Special Agent Raymundo applied for, and was issued, a warrant to search the HP Laptop and all of the electronic data storage devices obtained from Defendant. (*Id.* at p. 29).

II. SUMMARY OF THE PARTIES' ARGUMENTS

Defendant contends that the magistrate judge for the Eastern District of Virginia who authorized the Government's search of his computer through the deployment of a NIT acted in violation of Federal Rule of Criminal Procedure 41(b) and 28 U.S.C. § 636(a). (Doc. 36, p. 5). Defendant submits that the violation of Rule 41(b) cannot be characterized as a "mere technical violation" of the rule, such as a violation of a procedural requirement arising under Rule 41(b); therefore, Defendant argues that the Government may not rely upon the good-faith exception to avoid suppression of evidence. (*Id.* at p. 13). That is, it is Defendant's position that the NIT search warrant issued by the magistrate judge in Alexandria, Virginia, violated clearly established jurisdictional limits established in Rule 41(b) by allowing agents to search Defendant's computer in Florida to locate the IP address associated with that device. (*Id.* at p. 6). Defendant concludes that the NIT warrant was "no warrant at all" and the search of Defendant's computer violated the Fourth Amendment to the United States Constitution. (*Id.*).

In response, the Government submits that the affidavit in support of the Government's application for the NIT warrant (Doc. 36-1, Ex. 3) establishes probable cause to search Defendant's computer. (Doc. 46, p. 7). This point is not contested by Defendant in the instant Motion to Suppress. The Government also correctly reports that Defendant does not challenge the NIT warrant on the basis that it lacks particularity or that the magistrate judge was not neutral and detached. (*Id.* at p. 14). After dispensing with these preliminary matters, the Government argues that Rule 41(b) is "a flexible rule that is broad enough to authorize the issuance of the warrant in this case." (*Id.* at p. 15). Assuming Rule 41(b) was violated, the Government submits suppression of the evidence is not warranted, because:

> (1) the defendant suffered no prejudice and the agents did not act with deliberate disregard of Rule 41(b); (2) the agents acted in good faith reliance on the warrant; and (3) the defendant's admissions that his electronic devices contained child pornography and the voluntary relinquishment of those devices to the agents attenuated the connection between the NIT warrant and the child pornography seized from the devices.

(*Id.*).

III. SUMMARY OF THE COURT'S ANALYSIS

To the extent Rule 41(b) was violated when the magistrate judge in the Eastern District of Virginia issued the NIT warrant on February 20, 2015 (Doc. 36-1, Ex. 3, Attachment A), any illegality arising from the violation of the rule is sufficiently attenuated from Defendant's voluntary confession, Defendant's act of voluntarily surrendering various electronic devices to the agents, and the act of applying for and receiving a search warrant prior to inspecting the subject electronic devices.

The NIT warrant was obtained on February 20, 2015, and Defendant's computer was searched via the NIT on March 1, 2015. Agents did not approach Defendant until six months later on September 11, 2015, at which time they identified themselves and said they were investigating Defendant for possessing child pornography. Defendant was advised that he was not required to speak with law enforcement. Armed with this knowledge, Defendant consented to a non-custodial interview and subsequently provided a detailed confession to possessing child pornography. Defendant voluntarily gave his laptop and electronic data storage devices to the agents and called the agents later that same day to advise he was in possession of additional storage devices containing child pornography. The agents collected those devices from Defendant the following day after meeting Defendant at a mutually agreed upon public location. The agents then applied

for and received a warrant to search the laptop and storage devices, giving rise to the instant criminal charges. The Court finds that any illegality arising from a violation of Rule 41(b) six months earlier was sufficiently attenuated by intervening circumstances, rendering suppression inappropriate.

While the Court does not need to address the nature of the Rule 41(b) violation or whether the good faith exception applies in reaching a resolution of Defendant's motion, the Court will do so to ensure the record is clear for appellate review.

IV. DISCUSSION OF ALLEGED FOURTH AMENDMENT VIOLATION

Under the Fourth Amendment to the United States Constitution, every person has the right "to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. The Supreme Court has generally interpreted this to mean that a search must be based on probable cause and must be executed pursuant to a warrant. *Katz v. United States*, 389 U.S. 347, 357 (1967). The Fourth Amendment provides that "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459 (2011). Evidence obtained in violation of the Fourth Amendment may be suppressed pursuant to the exclusionary rule only when suppression is warranted to deter violations of the Fourth Amendment. *See Davis v. United States*, 564 U.S. 229, 238 (2011).

"[T]he application of the Fourth Amendment depends on whether the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (internal quotation marks omitted). A person claiming a violation of the Fourth Amendment must demonstrate that he has a subjective expectation of privacy and that

society is prepared to recognize that expectation as objectively reasonable. *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).

Computer users lack a legitimate expectation of privacy in information regarding the to and from addresses for emails, the IP addresses of websites visited, the total traffic volume of the user, and other addressing and routing information conveyed for the purpose of transmitting Internet communications to or from a user. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008), *rev'd on other grounds sub. nom*, *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), *cert. denied*, 555 U.S. 908 (2008); *see also United States v. Christie*, 624 F.3d 558, 573–74 (3d Cir. 2010) (finding no reasonable expectation of privacy in IP address or subscriber information because such information is voluntarily conveyed to third parties), *cert. denied*, 526 U.S. 1236 (2011). At least one court has further held that using Tor does not involve a reasonable expectation of privacy in the IP address. *United States v. Werdene*, No. 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016). The *Werdene* Court found that "a necessary aspect of the Tor network is the initial transmission of a user's IP address to a third party." *Id.* "[I]n order for a prospective user to use the Tor network[,] they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations." *Id.* (quoting *United States v. Farrell*, No. 15-cr-029, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016)).

Applying these principles, the Court finds Defendant does not have a reasonable expectation of privacy in the IP address associated with the computer he used to access Playpen. Defendant called Mr. Richard Connor, a computer forensic expert witness, at the evidentiary hearing on his motion to suppress. Mr. Connor explained that an individual

using the Tor network exposes his IP address to the "entry node" in the Tor system—that is, the first server to receive the search query from Defendant. After the IP address is exposed to the entry node, the address is unknown to the relay nodes—the servers responsible for bouncing the search query among other various servers until it reaches Playpen. Mr. Connor further explained that each relay node has its own IP address and with each relay additional IP addresses are used, thereby masking Defendant's IP address. While law enforcement can see the IP address of the last Tor server to transmit the search query to Playpen, that server (the exit node) has no way to identify Defendant's IP address. However, this does not alter the fact that Defendant must first disclose his IP address upon entering the Tor system. Defendant's expectation of privacy in his IP address is lost once he discloses the IP address to the first server in the Tor system. It is for this precise reason that the Government is not required to obtain a search warrant to subpoena an Internet Service Provider the physical address connected with a visible IP address. *See Forrester*, 512 F.3d at 510.

However, Defendant pointedly argued during the evidentiary hearing that Defendant's IP address was obtained via the NIT by searching Defendant's computer, which is a correct assertion. The Government, in connection with its application for a warrant to the NIT, attests that the NIT operates by attaching once a user logs onto the Playpen website with a username and password. (Doc. 36-1, Ex. 3, ¶ 32). Once a user's computer downloads the content from Playpen—or more accurately once the exit node in the Tor network downloads the content—the NIT causes the user's computer to transmit information to a computer controlled by the Government. (*Id.* ¶ 33). Stated differently, the NIT travels to the user's computer and identifies the IP address along with the type of operating system running on the computer, information about whether the NIT

was previously delivered to avoid duplication of data, the Host Name assigned to the device connected to the network, and the MAC address for the computer.[2] (*Id.* ¶ 34).

When the Court considers the issue of Defendant's reasonable expectation of privacy, the question becomes whether the IP address should be the focus of this analysis or whether Defendant's expectation of privacy in his computer is the proper subject of this analysis. There is little doubt that had law enforcement officers obtained Defendant's IP address from a non-Tor-based server and issued a subpoena to the ISP to determine Defendant's physical address, a motion to suppress the information obtained from the ISP would be without merit.[3] However, Defendant's IP address was discovered only after property residing within Defendant's home—his computer—was searched by the NIT. The courts which have thus far grappled with the extent to which a person has a reasonable expectation of privacy in an IP address have analyzed the issue in the context of a subpoena to an ISP to identify the person assigned the IP address. To the extent the *Werdene* Court has concluded that an individual waives his or her expectation of privacy in his or her computer by connecting to the Tor network, this Court disagrees with that conclusion as having improperly conflated the expectation of privacy associated with an IP address with the expectation of privacy one has in the computer searched by the NIT.

The NIT searches the user's computer to discover the IP address associated with that device. Therefore, one's expectation of privacy in that device is the proper focus of

---

[2] The MAC is a unique number assigned to the computer by the manufacturer. (Doc. 36-1, Ex. 3, ¶ 34).

[3] Non-Tor-based websites have IP address logs that law enforcement can use in conjunction with publicly available databases to determine the ISP that owns the targeted IP address. (*Id.* ¶ 29). A subpoena is issued to the ISP and the identity of the user assigned to the IP address at a particular time is determined. (*Id.*).

the analysis, not one's expectation of privacy in the IP address residing in that device. For example, a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage. *See United States v. Lanford*, 838 F.2d 1351, 1353 (5th Cir. 1988). Remove the stolen car from the garage, and no expectation of privacy in the vehicle exists. An IP address located in the "open" is akin to a stolen car parked on the street. However, the agents were required to deploy the NIT to search the contents of Defendant's laptop, and Defendant enjoyed a reasonable expectation of privacy in that device. The Court therefore turns to whether the NIT warrant was properly issued and whether the agents may rely in good faith upon that warrant.

V. DISCUSSION OF RULE 41(b)

The Federal Magistrates Act, 28 U.S.C. § 636(a), provides that "[e]ach United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge . . . (1) all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure." Federal Rule of Criminal Procedure 41(b) confers upon the magistrate judge the authority to issue search warrants in five distinct circumstances:

> (1) a magistrate judge with authority in the district—or if none is reasonable available, a judge of a state court of 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 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 purpose; 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 asserts that the NIT warrant comported with Rule 41(b)—presumably subsection (b)(1)—because the Playpen server was located in the Eastern District of Virginia, the NIT was placed on the server in that district, and only users who logged onto the server in that district downloaded the NIT. (Doc. 46, p. 15). However, this argument misses the point that Rule 41(b) addresses the location of the property to be searched and places limitations upon the magistrate judge's authority to authorize searches of that property. While the NIT was installed in the Eastern District of Virginia,

the search of Defendant's computer occurred in Florida. Recognizing this dilemma, the Government argues for a liberal or broad interpretation of Rule 41. (*Id.*). The Government cites *United States v. New York Telephone Co.*, 434 U.S. 159, 169 & n.16 (1977), wherein the Supreme Court upheld a search warrant for a pen register to collect dialed telephone number information even though Rule 41 at the time did not specifically include electronic intrusions in the definition of property. The Government also cites a more recent case where the Ninth Circuit Court of Appeals upheld a warrant allowing video surveillance, despite Rule 41's silence on this type of warrant. *See United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (en banc). However, neither of these opinions authorize a magistrate judge to authorize a search of property outside his or her district pursuant to Rule 41(b)(1). This Court recognizes that some flexibility in the type of search is appropriate, but the Court is unwilling to expand the authority of the magistrate judge beyond the geographic limitations clearly established by Rule 41(b).

The Government next turns to Rule 41(b)(4) in an attempt to analogize the NIT to a "tracking device." (Doc. 46, p. 17). Rule 41(b)(4) allows the magistrate judge "to issue a warrant to install within the district a tracking device." Because a tracking device monitors the movement of a person or object, the person or object must be located within the district at the time the tracking device is installed. *See* Fed. R. Crim. P. 41(a)(2)(E); 18 U.S.C. § 3117(b). The Government offers a tempting interpretation of this rule by comparing the placement of the NIT onto the government-controlled Playpen server to the concealment of a tracking device in a container holding contraband which is then

tracked outside of the district where the warrant was issued.[4] (Doc. 46, p. 18). However, by the Government's admission, once installed on the Playpen server, the NIT does nothing until the user logs onto the government-controlled server in that district and downloads the NIT. (Doc. 46, p. 15). The warrant authorizes the installation of the NIT onto the government-controlled Playpen server and not onto Defendant's computer, which is located outside of the Eastern District of Virginia. Moreover, the NIT does not track; it searches. As discussed above, the NIT is designed to search the user's computer for certain information, including the IP address, and to transmit that data back to a server controlled by law enforcement. *See United States v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan 28, 2016); *United States v. Levin*, No. 15-cr-10271-WGY, 2016 WL 1589824, at *6 (D. Mass. May 5, 2016); *United States v. Arterbury*, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *21 (N.D. Okla. Apr 25, 2016). The Government relies upon *United States v. Matish*, No. 4:16cr16, 2016 WL 3545776, at *17 (E.D. Va. June 23, 2016), and *United States v. Darby*, No. 2:16cr36, 2016 WL 3189703, at *12 (E.D. Va. June 3, 2016), which hold that a magistrate judge has authority under Rule 41(b)(4) to issue a warrant to deploy a NIT as a "tracking device," because anyone logging in to Playpen makes a "virtual trip" to Virginia. The Court does not find this analysis persuasive for the reasons given. Accordingly, Rule 41(b)(4) is inapplicable.

To the extent that the Government argues 28 U.S.C. § 636(a) only limits where a magistrate judge may possess powers conferred by the Federal Magistrates Act and by

[4] *See United States v. Knotts*, 460 U.S. 276, 285 (1983) (upholding against a Fourth Amendment challenge the use of a tracking device placed in a container of chloroform which was thereafter tracked).

the Federal Rules of Criminal Procedure and does not, therefore, restrict the geographic locale where a search warrant may be executed (Doc. 46, p. 21), the Court rejects this argument as a basis for finding the NIT warrant proper under Rule 41(b)(1) and (b)(4). That is, Rule 41(b)(1), (2), and (4) all require the property to be located within the district where the magistrate judge is sitting. Only Rule 41(b)(3) and (5) authorize a magistrate judge to issue a warrant to search property not located within the district where the magistrate judge sits. Therefore, the two subsections of Rule 41(b) relied upon by the Government clearly render a warrant authorizing a search outside of the issuing magistrate judge's district ineffective. The Government does not rely upon any other subsection of Rule 41(b), and the Court finds the remaining subsections inapplicable. Having found that the magistrate judge in the Eastern District of Virginia violated Rule 41(b) by issuing the NIT warrant and thereby allowing a search of property located outside of her district, the Court turns to whether the Defendant's confessions and the physical evidence obtained on September 11 and 12, 2015 should be suppressed.

Defendant contends that, for purposes of the Fourth Amendment, a search warrant issued in violation of Rule 41(b) is "no warrant at all." *United States v. Krueger*, 809 F.3d 1109, 1126 (10th Cir. 2015) (Gorsuch, J., concurring). For this reason, Defendant submits that the violation of Rule 41(b) renders the Government's search of his laptop a warrantless search in violation of the Fourth Amendment. (*Id.*). Defendant contends that the instant NIT warrant was void *ab initio* because of the magistrate judge's lack of jurisdiction to authorize the search in the first instance. *See Levin*, 2016 WL 2596010, at *10–13 (holding that the good faith exception to suppression is unavailable where warrant is void *ab initio*). This Court declines to follow the cases holding that a violation of Rule 41(b) renders the warrant void *ab initio*. The Court finds that the magistrate judge in the

Eastern District of Virginia had the authority to issue search warrants—that is, the inherent power to do so. The Court views a Rule 41(b) violation to be a technical or procedural violation, similar to a violation of Rule 41(a), (c), (d), or (e), which Defendant concedes are technical violations.[5] (Doc. 36, p. 13).

The Government accurately asserts that the Fourth Amendment does not impose a venue requirement for applying for a search warrant. (Doc. 46, p. 26). The Fourth Amendment imposes three requirements: (1) a search warrant must be issued by a neutral magistrate; (2) it must be based on a showing of probable cause, and (3) it must satisfy the particularity requirement. *Dalia v. United States*, 441 U.S. 238, 255 (1979). Defendant does not contend that any of these considerations were not met in the application for, and issuance of, the NIT warrant in this case.

In the absence of a constitutional violation, such as the case at bar, "Rule 41 requires suppression of evidence only where (1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." *United States v. Loyd*, 721 F.2d 331, 333 (11th Cir. 1983) (per curium) (quoting *United States v. Sefanson*, 648 F.2d 1231, 1235 (9th Cir. 1981)). Even assuming prejudice has been established by Defendant, the good faith exception applies in this case as discussed below.

---

[5] If the lack of probable cause supporting the search warrant under Rule 41(d) is a technical violation, then issuing a warrant supported by probable cause but erroneously authorizing the search of property outside the issuing court's district is also a technical violation. After all, the Fourth Amendment requires a showing of probable cause prior to the issuance of a warrant.

The Supreme Court in *United States v. Leon*, 468 U.S. 897, 923 (1984) identified four situations in which the good faith exception does not apply: (1) when "the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth," (2) when "the issuing magistrate wholly abandoned his judicial role," (3) when the affidavit supporting the application for a warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," and (4) when "a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." Defendant submits that the NIT warrant recklessly described the search would take place in the Eastern District of Virginia and that no objectively reasonable FBI agent with nineteen years of experience would believe the NIT warrant was valid due to the limitations imposed by Rule 41(b). (Doc. 36, pp. 13–14). Defendant's argument appears to focus on the fourth category identified by the Supreme Court in *Leon*: facial deficiencies in the search warrant.

The Government counters that suppression is a "last resort," not the "first impulse," and any benefit to suppressing evidence must outweigh the substantial social costs that result when "guilty and possibly dangerous defendants go free." *Herring v. United States*, 555 U.S. 135, 140–41 (2009). In *United States v. Berkos*, the Seventh Circuit observed that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause and with advance judicial approval." 543 F.3d at 396 (quoting *United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008)). The Court in *Berkos* further remarked that the remedy of allowing a defendant to go free based

on a violation of Rule 41's requirements would be "wildly out of proportion to the wrong."[6] *Id.* (quoting *Cazares-Olivas*, 515 F.3d at 730). In addition, "[t]he exclusionary rule should be limited to those situations where its remedial objectives are best served; i.e., to deter illegal police conduct, not mistakes by judges and magistrates." *United States v. Burgos-Montes*, 786 F.3d 92, 109 (1st Cir. 2015) (quoting *United States v. Bonner*, 808 F.2d 864, 867 (1st Cir. 1986)), *cert. denied*, 136 S. Ct. 599 (2015).

Returning to the question of prejudice arising from the Rule 41(b) violation, the defense does not suggest that law enforcement officers intentionally and deliberately disregarded a provision in the Rule. At most, Defendant submits "the NIT Warrant recklessly described the search would take place in the Eastern District of Virginia." (Doc. 36, pp. 13–14). Therefore, the Court must consider whether prejudice is established under the first prong—that the search utilizing a NIT might not have occurred if the rule had been followed.

In seeking the NIT warrant, the FBI attests, in pertinent part, as follows:

> Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or "nodes," as described herein, other investigative procedures [aside from the NIT] that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

(Doc. 36-1, Ex. 3, ¶ 31). The application in support of the NIT warrant makes it abundantly clear that law enforcement had no realistic chance of identifying the IP address associated with Defendant's computer without the NIT. Had the magistrate judge followed

[6] The Court in *Berkos* remarked that had the government made and preserved this argument below, the Court would have affirmed the district judge's denial of Defendant's motion to suppress. 543 F.3d at 396.

Rule 41(b), the search of Defendant's computer would not have occurred. Accordingly, Defendant has clearly proven that he was prejudiced by the violation of Rule 41(b). However, the FBI agents acted upon the NIT warrant with objectively reasonable reliance on the warrant's authority. *See Leon*, 468 U.S. at 992. The Court does not accept Defendant's argument that the special agents should have known the limits of Rule 41(b) vis-à-vis the NIT warrant. The parties in briefing the motion to suppress have expended sixty pages of written argument, and have cited competing case law largely addressing the scope and import of the various subsections of Rule 41(b). Furthermore, Defendant failed to offer evidence that the agents possessed some unique knowledge rendering their reliance upon the NIT warrant objectively reasonable.[7] *See id.* ("In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination . . . ."). Accordingly, the Court finds the good faith exception to suppression is applicable.

Finally, the Court turns to the Government's argument that an alleged violation of Rule 41(b) is sufficiently attenuated from Defendant's subsequent confession and voluntary relinquishment of his laptop and electronic data storage devices. (Doc. 46, p. 37). It is undisputed that six months after agents obtained the IP address associated with Defendant's residence, they went to his home, identified themselves as law enforcement officers, disclosed the purpose of their investigation, cautioned the Defendant that he was not required to submit to an interview, and were nevertheless invited inside by Defendant. Thereafter, Defendant provided a detailed and voluntary

[7] *See United States v. Zimmerman*, 277 F.3d 426, 436 (3d Cir. 2002) ("The test for whether the good faith exception applies is 'whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.'") (quoting *United States v. Loy*, 191 F.3d 360, 367 (3d Cir. 1999)).

statement in which he confessed to accessing and downloading child pornography from the Playpen server as well as other servers. Defendant voluntarily relinquished his laptop and numerous electronic storage medium. As the agents were departing his residence, Defendant went to the agent's vehicle and offered to contact them if he discovered additional devices containing child pornography. Later that same day, Defendant in fact called the agents to advise he had additional devices that he wanted to surrender. The agents met Defendant the following morning in a public location where he turned over additional storage devices. Thirteen days later, the agents applied for and were granted a warrant to search the laptop and storage devices. The warrant was issued by a magistrate judge sitting in the Middle District of Florida, and that search warrant is not challenged, although Defendant seeks the exclusion of his confession, his laptop, and all storage devices as fruit of the poisonous tree.

"Where a 'consent to search' follows allegedly unlawful police conduct, the court *must* determine (1) whether the consent was voluntary; *and* (2) whether the consent, even if voluntary, was the product of the unlawful police conduct. *United States v. Moreno-Ortega,* 522 F. App'x 729, 732 (11th Cir. 2013) (per curiam), *cert. denied sub. nom.*, 134 S. Ct. 704 (2013). The Government bears the burden on both issues. *Id.* Three non-exhaustive factors guide this attenuation analysis under the second prong: (1) the temporal proximity between the unlawful conduct and the consent; (2) the presence of intervening circumstances; and (3) the purpose and flagrancy of the unlawful conduct.

In *Moreno-Ortega*, officers responded to the defendant's residence to execute an outstanding arrest warrant. *Id.* at 731. A woman opened the door and, upon seeing the police, ran down the hallway, prompting officers to enter the home without permission, conduct a protective sweep and detain the occupants. *Id.* When the defendant arrived

home, he was arrested and brought into the house. *Id.* Approximately thirty to thirty-five minutes later an interpreter arrived, the defendant was interviewed for approximately eleven minutes, was advised of his rights, and provided verbal and written consent to search. *Id.* Officers discovered contraband during the execution of the consensual search, and the defendant moved to suppress the evidence as the product of the initial illegal entry into the residence. *Id.* at 732. The district judge, and subsequently the Eleventh Circuit Court of Appeals, found the verbal and written consent sufficiently attenuated from the initial illegality, thus rendering suppression inappropriate.

As the Supreme Court observed long ago:

> We need not hold that all evidence is fruit of the poisonous tree simply because it would not have come to light but for the illegal actions of the police. Rather, the more apt question in such a case is whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.

Wong Sun v. United States, 371 U.S. 471, 487–88 (1963) (citation and internal quotation marks omitted). Rather, the Court is obliged to determine whether the consent "was sufficiently an act of free will to purge the primary taint of the unlawful invasion," or, alternatively, whether the causal connection had "become so attenuated as to dissipate the taint." *Id.* at 486–87.

The police officers in *Delancy* arrived at the defendant's residence to execute an arrest warrant and observed through the partially open door the defendant seated on a couch. *Id.* at 1301. Officers observed the defendant hiding an object in the cushions of the couch and entered the house to conduct a protective sweep. *Id.* The defendant's girlfriend spoke with officers for ten to twenty minutes and provided written consent to

search the residence. *Id.* at 1310–11. On appeal, the Court noted that although the temporal proximity between the unlawful entry and the consent to search was relatively brief, the written consent to search which included notification of the right to refuse consent constitutes an intervening circumstance that interrupted the causal connection between the illegal act and the consent. *Id.* Turning to the third factor, the Court found the purpose of the entry was to secure the officers' safety, particularly since the defendant was known to possess weapons, and that the conduct was not flagrant. *Id.* at 1312. Accordingly, the motion to suppress was denied. Additionally, the Supreme Court recently held that discovery of a valid, pre-existing arrest warrant attenuated the connection between an unconstitutional investigatory stop and evidence seized incident to the defendant's arrest. *See Utah v. Strieff*, 136 S. Ct. 2056, 2061–63 (2016).

In the instant case, the NIT warrant was obtained on February 20, 2015, and Defendant was searched via the NIT on March 1, 2015. Six months later, on September 11, 2015, officers conducted a consensual, non-custodial interview of Defendant. There is no dispute over whether Defendant consented to speak with the officers or whether he knew he had the right to refuse their request. Similarly, there is no dispute that Defendant provided a voluntary confession to the officers. The passage of twenty-six weeks from the NIT search to the consensual encounter with Defendant weighs heavily in favor of admissibility. Secondly, intervening circumstances exist which support admission of the evidence. Defendant's voluntary confession, his voluntarily relinquishing of his laptop and electronic devices, and his initiative in notifying the officers later in the day that he had located additional storage devices for the officers' inspection all constitute intervening circumstances favoring admissibility. Added to these intervening circumstances, the Court considers that the officers sought and obtained a search warrant prior to inspecting

the devices obtained from Defendant. It is also abundantly clear that the officers did not act with any purposeful or flagrant misconduct. To the contrary, the officers went to considerable lengths to ensure Defendant understood his rights, including the right not to cooperate in the investigation, and sought judicial oversight at the appropriate time. For these reasons, the violation of Rule 41(b) is sufficiently attenuated from the events giving rise to Defendant's confession and the procurement of his laptop and electronic storage devices to support admission of that evidence.

VI. CONCLUSION

It is therefore **ORDERED AND ADJUDGED** that Defendant Adams' Motion to Suppress Evidence (Doc. 36) is **DENIED**.

DONE AND ORDERED in Orlando, Florida on August 10, 2016.

PAUL G. BYRON
UNITED STATES DISTRICT JUDGE

Copies furnished to:
Counsel of Record