

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF LOUISIANA

UNITED STATES OF AMERICA

CRIMINAL ACTION

VERSUS

NO: 15-266

JOSEPH RIVERA

SECTION: "J" (4)

**ORDER AND REASONS**

Before the Court are a *Motion to Suppress Evidence* (**Rec. Doc. 39**) filed by Defendant Joseph Rivera ("Defendant"), an opposition thereto (Rec. Doc. 58) filed by the United States of America ("Government"), and a reply (Rec. Doc. 68) filed by Defendant. Having considered the motion and legal memoranda, the record, and the applicable law, the Court finds that Defendant's motion should be **DENIED**.

**FACTS AND PROCEDURAL BACKGROUND**

On November 5, 2015, a grand jury returned a one-count indictment charging Defendant Joseph Rivera with violations of Title 18, United States Code, sections 2252(a)(2) and 2252(b)(1) for receipt of child pornography. (Rec. Doc. 1.) In the present motion, Defendant seeks to suppress all physical and testimonial evidence obtained in violation of the Fourth Amendment and Federal Rule of Criminal Procedure 41 ("Rule 41").

The criminal charges in this case stem from an investigation conducted by the Federal Bureau of Information ("FBI") from February 20 to March 4, 2015. During the investigation, the FBI took control of a "child pornography bulletin board and website"—referred to as "Website A"—and allowed free public access to the website on a government server. Website A operated on the Tor network, which protects users' internet protocol (IP) addresses and other identifying information by routing communications through other computers. To obtain the IP addresses of Website A's users, the FBI sought and received a search warrant from a United States magistrate judge in the Eastern District of Virginia (the "Virginia Warrant").

The application for a search warrant, which was filed on February 20, 2015, contained the following language:

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*)" See Attachment A located in the Eastern District of Virginia, there is now concealed (*identify the person or describe the property to be seized*): See Attachment B.

(Rec. Doc. 39-1, at 26.) When prompted to identify the person or describe the property to be searched, along with its location, the applicant, Special Agent Douglas Macfarlane, referred to Attachment A. Attachment A, subtitled "Place to be Searched," stated:

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

The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE . . . [that] will be located at a government facility in the Eastern District of Virginia.

The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. . . .

*Id.* at 28. Attachment B described the information to be seized from the search, including:

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 . . . to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g. Windows), version (e.g. Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the "activating" computer;
5. the "activating" computer's Host Name;
6. the "activating" computer's active operating system username; and
7. the "activating" computer's medial access control ("MAS") address . . . .

*Id.* at 29.

The Virginia Warrant allowed the FBI to use a NIT on the computers of the website's users. The NIT searched and extracted identifying information that the Tor network would typically render unavailable. On February 21, 2015, the FBI deployed a NIT to search the computer of a website user with the handle "rickybobby88." The

FBI obtained the user's IP address and other electronic information. Agents then served an administrative subpoena on Cox Communications, requesting information on the holder of the IP address. The IP address was linked to Defendant and his home address.

On August 3, 2015, agents submitted an application for a search warrant for Defendant's home under Rule 41(c). A magistrate judge in the Eastern District of Louisiana issued the warrant, finding that the affidavit established probable cause. Defendant was subsequently arrested and indicted. Defendant filed the instant motion under seal on March 30, 2016, arguing that the initial FBI search was unlawful under the Fourth Amendment and Rule 41. (Rec. Doc. 39). After several continuances, the motion was set for hearing on July 7, 2016. The Government opposed the motion on June 29, 2016. (Rec. Doc. 58.) The Court heard oral argument on the motion on July 7, 2016. After seeking the Court's leave, Defendant filed a reply brief on July 18, 2016. (Rec. Doc. 68.)

#### **PARTIES' ARGUMENTS**

In his motion, Defendant argues that the Court should suppress evidence of his computer activity pursuant to the exclusionary rule. First, Defendant claims that the search conducted by the FBI exceeded the scope of the Virginia Warrant. Defendant contends that the deployment of the NIT to Defendant's computer constituted a search for Fourth Amendment purposes and that he had a reasonable

expectation of privacy in the contents of his computer. Further, Defendant claims that suppression is an appropriate remedy because the officers could not objectively rely on the warrant in good faith because the execution of the warrant offended the Fourth Amendment. Second, Defendant argues that the warrant violated the Fourth Amendment particularity requirement. Third, Defendant contends that the warrant failed to meet the requirements of Rule 41 because the magistrate judge was not authorized to issue it. Further, Defendant claims that he suffered prejudice because of the violation of Rule 41. Thus, Defendant asks this Court to suppress all evidence obtained as a result of the improper search and seizure.

In its opposition, the Government first argues that other district courts have resolved questions about the constitutionality of the FBI's investigation of Website A, with six of the courts denying similar motions to suppress.<sup>1</sup> Next, the

---

<sup>1</sup> At least eight district courts have ruled on similar motions to suppress arising out of the investigation. See *United States v. Darby*, No. 16-036, 2014 WL 3189703 (E.D. Va. June 3, 2016) (denying motion to suppress); *United States v. Werdene*, No. 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (denying motion to suppress) (page numbers not available); *United States v. Levin*, No. 15-10271, 2016 WL 2596010 (D. Mass. May 5, 2016) (granting motion to suppress); *United States v. Epich*, No. 15-CR-163, 2016 WL 953269 (E.D. Wisc. March 14, 2016) (denying motion to suppress); *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016) (denying motion to suppress). Three cases are available in the record but not yet available on Westlaw or Lexis: *United States v. Matish*, decided by the Eastern District of Virginia (denying motion to suppress) (Rec. Doc. 58-2); *United States v. Stamper*, decided by the Southern District of Ohio (denying motion to suppress) (Rec. Doc. 58-1); and *United States v. Arterbury*, decided by

Government contends that deployment of the NIT did not exceed the scope of the Virginia Warrant and that Defendant lacked a reasonable expectation of privacy in his IP address. Third, the Government claims that the Virginia Warrant was sufficiently particular because Attachment A and Attachment B adequately define the scope of the investigation to be conducted.

Fourth, the Government contends that Rule 41(b) authorized the magistrate judge to issue the Virginia Warrant because Rule 41(b)(4) allows a judge to issue a warrant to install a tracking device within the district where it is issued. According to the Government, the NIT may be compared to a tracking device that was installed in the Eastern District of Virginia when a user's computer accessed Website A on the Government's server. Even if the magistrate judge lacked authority, the Government argues that suppression is inappropriate because Defendant cannot demonstrate that he suffered legal prejudice as a result of the deployment of the NIT. Fifth, the Government contends that suppression is unwarranted because the Government executed the warrant in good faith.

#### **LEGAL STANDARD**

Under the Fourth Amendment to the United States Constitution, every person has the right "to be secure in their persons, houses,

---

the Northern District of Oklahoma (granting motion to suppress) (Rec. Doc. 58-3).

papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. The Supreme Court has generally interpreted this requirement to mean that a search must be based on probable cause and 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." *United States v. Thompson*, No. CR 14-153, 2016 WL 3476714, at \*4 (E.D. La. June 27, 2016) (quoting *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. See *United States v. Ragsdale*, 470 F.2d 24, 30 (5th Cir. 1972). Such evidence is excluded "not because the evidence is not probative, or to chastise errant law officers or to benefit the accused, but to compel respect for the guaranty of the Fourth Amendment 'in the only effectively available way—by removing the incentive to disregard it.'" *Id.* (quoting *Elkins v. United States*, 364 U.S. 206, 217 (1960)). Exclusion is only warranted when suppressing the evidence would serve to deter violations of the Fourth Amendment. *Davis v. United States*, 564 U.S. 229, 238 (2011). On a motion to suppress the evidence, the proponent of the motion bears the burden of proving facts that demonstrate the reasonableness of privacy in

the searched area. *United States v. Kelley*, 981 F.2d 1464, 1467 (5th Cir. 1993).

### **DISCUSSION**

Defendant challenges the Virginia Warrant on three bases. First, Defendant argues that the FBI exceeded the scope of the warrant by searching his computer in the Eastern District of Louisiana. Second, Defendant argues that the Virginia Warrant is deficient under the Fourth Amendment because it lacks particularity. Third, Defendant claims that the magistrate judge lacked the authority to issue the warrant pursuant to Rule 41. According to Defendant, the remedy for all three violations is suppression of the evidence obtained from the search. The Court will discuss each argument in turn.

#### **I. Scope of the Virginia Warrant**

First, Defendant argues that the Government exceeded the scope of the Virginia Warrant because the warrant only authorized the Government to search a person or property in the Eastern District of Virginia. Further, Defendant claims that the Government's use of the NIT constituted a search pursuant to the Fourth Amendment. The Court will presume for purposes of this analysis that the FBI's use of the NIT constituted a search. Thus, the only remaining issue on this point is whether the FBI exceeded the scope of the Virginia Warrant.



"Searches conducted pursuant to a valid warrant and within the scope of that warrant are presumptively reasonable." *Rundus v. United States*, No. 3:06CV1032P, 2010 WL 1254335, at \*11 (N.D. Tex. Mar. 30, 2010); see *Ybarra v. Illinois*, 444 U.S. 85, 102 (1979). Courts in the Fifth Circuit have found that police do not exceed the scope of warrants when they execute them reasonably and in good faith. See *United States v. Christie*, 208 F. App'x 332, 336 (5th Cir. 2006); *Watts v. Kroczyński*, 636 F. Supp. 792, 801 (W.D. La. 1986). Items outside the scope of the warrant will only be suppressed if the officers flagrantly disregarded the scope of the warrant. *Watts*, 636 F. Supp. at 801 (citing *United States v. Crozier*, 777 F.2d 1376, 1381 (9th Cir. 1985); *United States v. Lambert*, 771 F.2d 83, 93 (6th Cir. 1985); *United States v. Wuagneux*, 683 F.2d 1343, 1354 (11th Cir. 1982)).

In this case, the FBI did not exceed the scope of the Virginia Warrant. The application for a search warrant specified that the FBI sought property located in the Eastern District of Virginia. However, the application prompted the magistrate to "see Attachment A" for a detailed description of the property to be searched and its location. (Rec. Doc. 39-1, at 26.) Attachment A specified that the NIT would be used on "activating computers" of "any user or administrator who logs into the TARGET WEBSITE by entering a username and password." *Id.* at 28. The attachment also noted that the computer server itself was located in the Eastern District of

Virginia. However, the attachment makes it reasonably clear that the activating computers may be located outside the district. Therefore, the FBI did not exceed the scope of the warrant by searching Defendant's computer in the Eastern District of Louisiana.

Defendant argues that the Virginia Warrant, on its face, did not authorize the search of Defendant's computer in Louisiana. Defendant quotes the following language from the Fifth Circuit: "If an objective reading of the description contained on the face of the warrant did not fairly direct attention to the place actually searched, we would be compelled to hold the search illegal without further discussion. An insufficient warrant cannot be cured by the most detailed affidavit." *United States v. Haydel*, 649 F.2d 1152, 1157 (5th Cir. 1981). However, Defendant omits a salient part of the quote: "If, as is the case here, the warrant is ambiguous, but fairly directs attention to the place actually searched, and if the affidavit supporting the warrant is attached to the warrant when issued, the affidavit may be considered to clarify an ambiguity on the face of the warrant." *Id.* In this case, the Virginia Warrant directs attention to Attachment A, which sufficiently describes the place to actually be searched. Attachment A was included with the Virginia Warrant when it was issued. Thus, Defendant's argument lacks merit.

Moreover, even if the Virginia Warrant only authorized a search in the Eastern District of Virginia, the FBI did not flagrantly disregard the scope of the warrant. Defendant did not introduce any evidence to show that the FBI did not execute the Virginia Warrant reasonably and in good faith. Defendant generally alleges that the FBI recklessly misled the magistrate judge, but his allegations do not overcome the presumptively reasonable search.

## **II. Fourth Amendment Particularity Requirement**

Second, Defendant argues that the Virginia Warrant operated as a general warrant and lacked the particularity mandated by the Fourth Amendment. The Fourth Amendment prohibits search warrants that allow "a general, exploratory rummaging in a person's belongings." *Williams v. Kunze*, 806 F.2d 594, 598 (5th Cir. 1986) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). "The items to be seized must be described with sufficient particularity such that the executing officer is left with no discretion to decide what may be seized." *Id.* (citing *Marron v. United States*, 275 U.S. 192, 196 (1927)). However, generic language suffices in situations where providing detailed particulars is impossible, as long as the language "particularizes the types of items to be seized." *Id.* (quoting *United States v. Webster*, 734 F.2d 1048, 1055 (5th Cir. 1984)). Furthermore, the search must be "directed in good faith toward the objects specified in the warrant

or for other means and instrumentalities by which the crime[s] charged had been committed. It must not be a general exploratory search through which the officers merely hope to discover evidence of wrongdoing." *Gurleski v. United States*, 405 F.2d 253, 258 (5th Cir. 1968).

Defendant contends that "[t]he Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents." *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). While this statement is true, Defendant ignores the fact that "a court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant." *Id.* at 557-58. After examining the Virginia Warrant and the attachments it incorporates by reference, the Court finds that the warrant is sufficiently particular. As described above, Attachment A describes the place to be searched as "[t]he activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password." (Rec. Doc. 39-1, at 28.) Moreover, Attachment B lists the items to be seized as follows:

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 . . . to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;

3. the type of operating system running on the computer, including type (e.g. Windows), version (e.g. Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the "activating" computer;
5. the "activating" computer's Host Name;
6. the "activating" computer's active operating system username; and
7. the "activating" computer's medial access control ("MAS") address . . . .

*Id.* at 29. Thus, the Court concludes that the Virginia Warrant was not a mere general warrant. Therefore, suppression is not warranted on this basis.

### III. Rule 41 Violation

The Court will first consider whether the FBI violated Rule 41. Next, the Court will consider the appropriate sanction for the alleged violation.

#### *a. The Requirements of Rule 41*

Defendant argues that the Virginia Warrant violates Rule 41 because the magistrate judge was not authorized to issue it. Rule 41(b) provides:

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

(1) a magistrate judge with authority in the district—or if none is reasonably 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 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.

Fed. R. Crim. P. 41. Defendant argues that the Virginia Warrant was not authorized by any of the subsections of Rule 41(b).

The Court agrees that subsections (b)(1), (b)(2), (b)(3), and (b)(5) clearly do not apply. First, the property to be searched was not located in the Eastern District of Virginia. Defendant's

computer was located in the Eastern District of Louisiana, and the other activating computers that accessed Website A were located all over the country and the world. Second, Defendant's computer was not located in the Eastern District of Virginia when the warrant was issued, as required by subsection (b)(2). At all pertinent times, Defendant's computer was located in the Eastern District of Louisiana. Third, the FBI investigation in this case did not involve domestic or international terrorism, as required by subsection (b)(3). Fourth, Defendant's computer was not located outside the jurisdiction of any state or district, as described by subsection (b)(5).

The Government argues that subsection (b)(4) applies because the NIT may be likened to a tracking device installed within the Eastern District of Virginia when Defendant's computer accessed Website A on the Government's server. The Government's analogy comparing the NIT to a tracking device fails. The NIT could do much more than simply track a computer's location, as described by Attachment B to the Virginia Warrant, quoted above. In addition, other courts have rejected this argument. The Eastern District of Pennsylvania noted that section (b)(4) is "premised on the person or property being located in the district." *Werdene*, 2016 WL 3002376. Further, the Western District of Washington noted, "If the 'installation' occurred on the government-controlled computer, located in the Eastern District of Virginia, applying [section

(b)(4)] breaks down, because [Defendant] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district." *Michaud*, 2016 WL 337263, at \*6. While *Michaud* also notes that Rule 41(b) is intended to be applied flexibly, not rigidly, the Court finds that the Virginia Warrant technically violates Rule 41(b). *Id.* at \*5 (citing *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992)).

*b. Remedies for Rule 41 Violation*

Having found that the Virginia Warrant was not authorized by Rule 41(b), the Court must consider whether suppression is an appropriate remedy for this violation. In the Rule 41 context, suppression is only warranted if the defendant's constitutional rights were violated or the defendant experienced prejudice "in the sense that the search would likely not have occurred or been as abrasive or intrusive had Rule 41 been followed." *United States v. Comstock*, 805 F.2d 1194, 1207 (5th Cir. 1986). Further, exclusion is not appropriate "if the officers concerned acted in the affirmative good faith belief that the warrant was valid and authorized their conduct. Good faith in this context implies not only that Rule 41 was not knowingly and intentionally violated, but also that the officers did not act in reckless disregard or conscious indifference to whether it applied and was complied with." *Id.* Further, "good faith" does not require the officers' conduct to be objectively reasonable. *Id.* The good faith standard



is subjective. *United States v. McKeever*, 894 F.2d 712, 717 (5th Cir. 1990).

1. Constitutional Violations

First, the Court will consider whether Defendant's Fourth Amendment rights were violated. The "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 has an expectation of privacy protected by the Fourth Amendment if he has a subjective expectation of privacy, and if society is prepared to recognize that expectation as objectively reasonable. *Katz*, 389 U.S. at 361.

The Fifth Circuit has held that IP addresses are not subject to a reasonable expectation of privacy. *United States v. Weast*, 811 F.3d 743, 747 (5th Cir. 2016). As noted by the Fifth Circuit, "Federal courts have uniformly held that subscriber information provided to an internet provider, including IP addresses, is not protected by the Fourth Amendment's privacy expectation because it is voluntarily conveyed to third parties." *Id.* (quoting *United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010)) (internal quotation marks omitted); see also *Smith*, 442 U.S. at 738 (no reasonable expectation of privacy in telephone numbers dialed because the dialer voluntarily conveyed the numbers to the

telephone company). In contrast, the Supreme Court has held that a reasonable expectation of privacy exists in the contents of a cell phone. *Riley v. California*, 134 S. Ct. 2473, 2485 (2014). The Fifth Circuit has explained that the contents of a cell phone are not voluntarily conveyed to third parties, unlike IP addresses. *Weast*, 811 F.3d at 747.

Courts have also decided that using the Tor network does not create a reasonable expectation of privacy in IP addresses. See *Werdene*, 2016 WL 3002376. The *Werdene* court noted that "a necessary aspect of Tor 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)).

In *Werdene*, the defendant argued that he maintained a reasonable expectation of privacy in his IP address because it "subsequently bounced from node to node within the Tor network to mask his identity." *Id.* The court rejected the argument, finding that the defendant lost any subjective expectation of privacy when he initially conveyed his IP address to a third party. This Court agrees with the reasoning of the *Werdene* court and finds that

Defendant lacked a subjective expectation of privacy in his IP address, even when using the Tor network.

Moreover, even if Defendant had a subjective expectation of privacy, his expectation was not objectively reasonable. Society does not recognize a legitimate expectation of privacy when the defendant's conduct is clearly unauthorized or illegal. *United States v. Lanford*, 838 F.2d 1351, 1353 (5th Cir. 1988) (no legitimate expectation of privacy in a stolen vehicle); see *United States v. Jacobsen*, 466 U.S. 109, 142-46 (1984) (Brennan, J., dissenting) (no reasonable expectation of privacy in illegal drugs in plastic bags shipped via common carrier when legitimate pharmaceuticals would not have been packaged in this way); *United States v. Stanley*, 753 F.3d 114, 120 (3d Cir. 2014) (no reasonable expectation of privacy when using neighbor's wireless internet connection without permission).

The *Werdene* court found that the defendant lacked a legitimate expectation of privacy because "[the defendant's] use of Tor to view and share child pornography is not only an activity that society rejects, but [also] one it seeks to sanction." 2016 WL 3002376. The Court finds that Defendant lacked a legitimate, reasonable expectation of privacy in his IP address when he used it to access child pornography. Thus, Defendant cannot show that the violation of Rule 41 resulted in a constitutional violation.

2. Prejudice Caused by Rule 41 Violation

Having found that Defendant's constitutional rights were not violated, the Court will consider whether Defendant was prejudiced by the failure to comply with Rule 41. The Fifth Circuit defines "prejudice" to mean that "the search would likely not have occurred or been as abrasive or intrusive had Rule 41 been followed." *Comstock*, 805 F.2d at 1207. Rule 41 did not authorize the magistrate judge to issue the Virginia Warrant. However, the search for Defendant's IP address still could have occurred in other ways. In deciding the same issue in a case based on the Virginia Warrant, the Western District of Washington noted that "using the Tor network does not strip users of all anonymity, because users accessing Website A must still send and receive information, including IP addresses, through another computer." *Michaud*, 2016 WL 337263, at \*7. Like an unlisted telephone number, the FBI would have eventually discovered the IP address, even if it had to use different means. *Id.*

In his affidavit in support of the Virginia Warrant, FBI special officer Douglas Macfarlane noted that, due to the unique nature of the Tor system, "other investigative procedures 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." (Rec. Doc. 39-1, at 74-75.) Based on this statement, Defendant could argue that he suffered prejudice

because the FBI was unlikely to discover his IP address by other means. The Southern District of Ohio discussed this issue in a challenge to evidence seized pursuant to the Virginia Warrant.<sup>2</sup> The court concluded that the improper search only revealed the defendant's IP address and did not lead directly to the defendant. (Rec. Doc. 58-1, at 22.) The court concluded that the defendant was not prejudiced by the NIT search.

On the issue of prejudice, this Court agrees with the Western District of Washington and the Southern District of Ohio. Moreover, the Court has decided that Defendant did not have a reasonable expectation of privacy in his IP address, meaning that the Government was not required to seek a warrant to conduct the NIT investigation. (Rec. Doc. 58-2, at 40.)<sup>3</sup> Therefore, the FBI could have conducted the same investigation without complying with Rule 41. Because the NIT search would have occurred regardless of the Rule 41 violation, the Court finds that Defendant has not suffered prejudice that would warrant suppression.

---

<sup>2</sup> The decision in the case is under seal. Therefore, the Court will refer to the copy of the opinion provided by the Government as Exhibit A to its opposition. (Rec. Doc. 58-1.)

<sup>3</sup> This decision by the Eastern District of Virginia, unavailable on Westlaw at the time of this Order and Reasons, determines that the defendant lacked a reasonable expectation of privacy in his IP address and that the FBI was not required to seek the Virginia Warrant.

### 3. Good Faith

Finally, the Court considers whether the FBI acted in good faith, meaning that the officers did not knowingly and intentionally violate Rule 41 or act in reckless disregard or conscious indifference to whether they complied with Rule 41. *Comstock*, 805 F.2d at 1207. If the officers acted in good faith, suppression is unwarranted. *Id.* The Supreme Court has noted 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," 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." *United States v. Leon*, 468 U.S. 897, 923 (1984).

In this case, the record does not reveal any evidence of bad faith, a knowing and intentional violation, or a reckless disregard or conscious indifference to the requirements of Rule 41. In contrast, the Fifth Circuit found a lack of good faith when a local sheriff told a DEA agent at the scene of the investigation that a

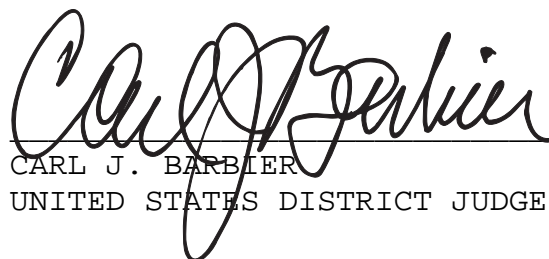
court of record did not issue the warrant, as required by Rule 41. *United States v. McKeever*, 894 F.2d 712, 717 (5th Cir. 1990). Moreover, none of the situations described in *Leon* occurred in this case. The record does not suggest that the magistrate judge was misled by false information or that she abandoned her judicial role. Defendant did not challenge the probable cause underlying the Virginia Warrant, and the Court notes that the warrant seems sufficiently supported by probable cause. Finally, the warrant was not facially deficient, such as by failing to specify a place to be searched or items to be seized. Therefore, to the extent that suppression would otherwise be warranted, the Court finds that the FBI reasonably relied on the Virginia Warrant in good faith. Exclusion of the evidence is not warranted.

**CONCLUSION**

Accordingly,

**IT IS HEREBY ORDERED** that Defendant's *Motion to Suppress Evidence (Rec. Doc. 39)* is **DENIED**.

New Orleans, Louisiana this 19th day of July, 2016.

  
CARL J. BARBIER  
UNITED STATES DISTRICT JUDGE