UNIVERSAL CASE OPINION COVER SHEET

U.S. District Court for the Central District of Illinois

Complete TITLE of Case	**United States of America** **Plaintiff,** **v.** **Braman Benjamin Broy,** **Defendant.**	
Type of Document	**ORDER**	
Docket Number	Case No. 16-cr-10030.	
COURT	UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF ILLINOIS - PEORIA DIVISION	
Opinion Filed	Date: September 21, 2016	
JUDGE	Honorable Michael M. Mihm 122 U.S. Courthouse 100 N.E. Monroe Peoria, IL 61602 (309) 671-7113	
ATTORNEYS For Plaintiff	Ronald L. Hanna	Office of the United States Attorney 211 Fulton Street, Suite 400 Peoria, IL 61602
	Gail Linn Noll	318 South Sixth Street Springfield, IL 62701-1806
ATTORNEYS For Defendant	Steven A. Greenberg	Steven A. Greenberg, LTD. 53 West Jackson, Suite 1260 Chicago, IL 60604
	Louis J. Meyer	Meyer & Kiss LLC 311 West Stratford Drive Peoria, IL 61614

E-FILED
Wednesday, 21 September, 2016 01:25:29 PM
Clerk, U.S. District Court, ILCD

IN THE UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS
PEORIA DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
v.	)	Case No. 16-cr-10030
	)	
BRAMAN BENJAMIN BROY,	)	
	)	
Defendant.	)	

ORDER

This matter is now before the Court on Defendant Braman Broy's ("Broy") Motion to Suppress Evidence (ECF No. 12). For the reasons set forth below, Broy's Motion to Suppress Evidence (ECF No. 12) is DENIED.

Significance of the Present Case

The Court notes the seriousness and complexity of the legal issues in this case and that similar issues are likely to present themselves as technology continues to evolve faster than the law can keep pace. It further recognizes that reasonable jurists can – and have – come to different conclusions on these issues and that district judges will await further guidance from the courts of appeals. The Court suggests readers familiarize themselves with previous cases stemming from the warrant at issue in this case before continuing to read this Order. *See, e.g.*, *United States v. Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016); *United States v. Acevedo-Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Eure*, No. 2:16CR43, 2016 WL 4059663 (E.D. Va. July 28, 2016); *United States v. Matish*, No. 4:16CR16, 2016 WL 3545776 (E.D. Va. June 23, 2016); *United States v. Darby*, No. 2:16CR36, 2016 WL 3189703 (E.D. Va. June 3, 2016); *United States v. Werdene*, No. CR

15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Epich*, No. 15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

Background

Playpen ("Website A") was a website whose primary purpose was the advertisement and distribution of child pornography. ECF No. 20 at ¶ 1. Website A operated only on the "Tor" network, an open-source software tool which routes communications through multiple computers called "nodes" in order to mask a user's IP address and, thus, keeps the user's identity anonymous. ECF No. 13 at 1–2. These nodes are run by volunteers throughout the world. ECF No. 15 at 3. In order to use the Tor network, a user must download and run Tor software on his or her personal computer. ECF No. 13 at 2. When first logging into the Tor network, a user, whether knowingly or not, communicates his or her IP address to the first node volunteer. It is only after an IP address has been routed through multiple nodes that a user's IP address becomes masked. Indeed, when a user finally accesses a website while logged into the Tor network, only the IP address of the "exit node" is visible to that site (and, thus, any law enforcement officials monitoring that site). ECF No. 15 at 3–4. Traditional investigative techniques are therefore ineffective in finding a Tor user's real IP address. *Id.* at 4.

Website A was a "hidden service" on the Tor network. *Id.* at 4. A "hidden service" does not operate like a normal Internet website, where one could find a page by happenstance, such as by entering key terms into a search engine. *Id.* at 4. Rather, a "hidden service" requires a user to acquire its exact web address from another source, such as another user of that "hidden service" or online postings detailing its web address,

before accessing the website. *Id.* at 4. Thus, it was extremely unlikely anyone could have accessed Website A accidentally.

Website A was hosted on a server in North Carolina and maintained by an administrator in Florida. ECF No. 20 at ¶ 2. In January 2015, FBI agents executed a search warrant and copied the contents of the server. ECF No. 15 at 5. Upon searching the website logs, the FBI determined that a Tor network user with the username "maproy99" had accessed several images of child pornography in January 2015. ECF No. 20 at ¶ 16. That username was later traced to Broy. *Id.* at ¶ 19. Rather than shutting down the server and Website A, the FBI continued to operate both at a government facility in the Eastern District of Virginia. *Id.* at ¶ 4. The FBI operated the server and Website A between February 20, 2015, and March 4, 2015. *Id.* at ¶ 4.

Also on February 20, 2015, the FBI obtained from a district judge in the Eastern District of Virginia an order pursuant to Title III of the Electronic Communications Privacy Act, which prohibits the government from intercepting private electronic communications without a court order. *Id.* at ¶ 5. The Title III order permitted the FBI to intercept communications between Website A users. *Id.* at ¶ 5. On the same day the FBI obtained the order from the district judge, they also obtained from a magistrate judge in the Eastern District of Virginia a warrant which allowed them to implement a Network Investigation Technique ("NIT") on the Website A server. *Id.* at ¶ 7. The NIT operated by sending to "activating computers" instructions designed to cause those computers to transmit certain information to a separate government computer, also located in the Eastern District of Virginia. *Id.* at ¶¶ 9, 12. The warrant authorized the FBI to obtain from an "activating computer" seven pieces of information: (1) the IP address of the computer and the date and time the NIT determined the IP address; (2) a unique identifier generated by the NIT to distinguish data from one activating computer from

that of another; (3) the type of operating system used by the computer; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's host name; (6) the computer's operating system username; and (7) the computer's media access control address. *Id.* at ¶ 8.

On February 26, 2015, Broy, under the username maproy99, accessed a post containing child pornography from Website A, at which point the NIT was deployed to the activating computer.[1] ECF No. 13 at 3. The NIT, without Broy's awareness, collected the above-listed information and sent it to the separate government computer in the Eastern District of Virginia. ECF No. 20 at ¶ 12. The unmasked IP address allowed the FBI to determine the physical address of the activating computer, which was ultimately determined to be Broy's.[2] *Id.* at ¶ 13. It is undisputed that without the use of the NIT, law enforcement would not have been able to identify the IP address connected to Broy. *Id.* at ¶ 18. On October 19, 2015, the FBI obtained a residential search warrant from United States Magistrate Judge Tom Schanzle-Haskins, a magistrate in the district of Broy's residence, the Central District of Illinois. *Id.* at ¶ 20. On October 21, 2015, FBI agents executed that warrant at Broy's home, where they identified files containing child pornography. *Id.* at ¶ 20. Broy was subsequently indicted for receipt of child pornography, possession of child pornography, and access with intent to view child pornography. *Id.* at ¶ 21.

Discussion

Broy argues the execution of the NIT warrant constituted an unreasonable search and seizure under the Fourth Amendment and requires suppression of the evidence to

[1] The NIT ultimately revealed Broy also accessed posts containing child pornography on March 2 and March 4, 2015.

[2] It is possible the computer did not technically belong to Broy, as it was found at his mother's address. Broy, however, admitted to using the computer to access images of child pornography.

which it led. Specifically, he argues the warrant contravened the Fourth Amendment's particularity requirement with regard to the place to be searched, rendering it a general warrant. He also claims the NIT's activation constituted a search in violation of his reasonable expectation of privacy in his computer and its contents. Broy further argues the magistrate judge lacked authority to issue the NIT warrant under the Federal Magistrate's Act and Rule 41(b) of the Federal Rules of Criminal Procedure. For the reasons set forth below, the Court finds that although the warrant itself was sufficiently particular, Broy was nevertheless the subject of an unreasonable, warrantless search in contravention of the Fourth Amendment. The Court, however, holds suppression is not an appropriate remedy in this case.

A. Whether the NIT Warrant Lacked Particularity and Amounted to a General Warrant

The Fourth Amendment to the United States Constitution provides, in part, "[n]o warrants shall issue, but upon probable cause, . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. AMEND. IV. This particularity requirement limits "the authorization to search to the specific areas and things for which there is probable cause to search" and, thus, "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). With regard to place, "[t]he requirement is satisfied if 'the description is such that the officer with a search warrant can with reasonable effort ascertain and identify the place intended.'" *United States v. McMillian*, 786 F.3d 630, 639 (7th Cir. 2015) (quoting *Steele v. United States*, 267 U.S. 498, 503 (1925)). With regard to the items or information to be seized, "nothing [may be] left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). Only if both of these requirements are satisfied is a warrant sufficiently particular.

Here, Broy asserts the NIT warrant did not state with particularity the place or places to be searched. He is misguided. Attachment A to the NIT warrant states the NIT was "to be deployed on the computer server described below, obtaining information *from the activating computers described below*. . . . The activating computers are those of *any* user or administrator who logs into the TARGET WEBSITE by entering a username and password." ECF No. 14-1 at 2 (emphasis added). The attachment does not limit the warrant's applicability to "the computer of any user who resides in the Eastern District of Virginia." Rather, it authorizes the deployment of the NIT onto the computer of "any user," which encompasses users who reside inside and outside the district. *Id.* at 2. It further required those users to log into Website A with a username and password, which, as described above, *supra* pages 2–3, was nearly impossible to do by accident. Moreover, the affidavit accompanying the warrant application asked the magistrate to authorize the NIT to "cause an activating computer – *wherever located* – to send" information to the government. ECF No. 15 at 33–34 (emphasis added). "Wherever located" clearly contemplates more than just users and computers located within the Eastern District of Virginia. That the warrant encompassed a large number of possible computers potentially located in a large number of districts does not mean it suffered from a lack of particularity; it merely indicates the FBI suspected a large number of users would access Website A from all over the country.

Broy does not claim the particularity requirement was violated with regard to the things to be seized. Nor could he; attachment B of the warrant listed the seven specific pieces of information the NIT would gather from the activating computer and send back to the government computer in the Eastern District of Virginia. ECF No. 14-1 at 3. Thus, both the place and items to be seized were described with sufficient particularity so as not to render the warrant a general one.

B. Whether the NIT's Activation Constituted a Fourth Amendment Search

A threshold question in the Court's Fourth Amendment analyses is whether a defendant had a reasonable expectation of privacy in the things and places searched. A Fourth Amendment search occurs when "the government violates [the defendant's] subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *see Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). And "[a]lthough it has become an old saw that the Fourth Amendment protects people, not places, the starting point in the *Katz* inquiry generally 'requires reference to a place.'" *United States v. Cuevas-Perez*, 640 F.3d 272 (7th Cir. 2011) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (internal quotation marks omitted)). Indeed, *Rakas v. Illinois*, 439 U.S. 128 (1978), and *Rawlings v. Kentucky*, 448 U.S. 98 (1980), make clear that "a person can have a legally sufficient interest in a place other than his home so that the Fourth Amendment protects him from unreasonable governmental intrusion into that place." *Rakas*, 439 U.S. at 142–43, 148–49 (finding passengers of a car had a legally insufficient interest in a car in which they were riding). *See also*, *Rawlings*, 448 U.S. at 104–05 (finding defendant had a legally insufficient interest in his girlfriend's purse); *United States v. Chadwick*, 433 U.S. 1, 11 (1977) (finding defendant who placed marijuana in a double-locked footlocker could claim Fourth Amendment protection); *Katz*, 389 U.S. at 352 (finding defendant who entered a telephone booth, shut the door, and paid the toll to use the phone could claim Fourth Amendment protection). In 2010, the Seventh Circuit reiterated its reliance on a five-factor test, originally announced in *United States v. Peters*, 791 F.2d 1270 (7th Cir. 1986), used to determine whether a defendant had such a privacy interest:

> (1) whether the defendant had a possessory [or ownership] interest in the thing seized or the place searched, (2) whether he had the right to exclude others from that place, (3) whether he exhibited a subjective expectation

> that it would remain free from governmental invasion, (4) whether he took normal precautions to maintain his privacy, and (5) whether he was legitimately on the premises.

United States v. Carlisle, 614 F.3d 750, 758 (7th Cir. 2010) (quoting *Peters*, 791 F.2d at 1281).

The parties have dedicated much of their briefing to whether Broy had a reasonable expectation of privacy in his IP address. Indeed, many of the district courts that have considered the warrant at issue in this case have focused their Fourth Amendment analysis on this point. *See, e.g.*, *Acevedo-Lemus*, 2016 WL 4208436 at **4–6; *Werdene*, 2016 WL 3002376 at **7–10; *Michaud*, 2016 WL 337263 at *7. But the analysis should not and does not end there. Whether Broy had a reasonable expectation of privacy in his computer and its contents is equally as important as whether he had one in his IP address. This is so because the NIT was designed to yield more than just Broy's IP address. Rather, it was designed to enter Broy's computer and gather seven different pieces of information. Accordingly, the Court shall consider in turn whether Broy had a reasonable expectation of privacy in: (1) his IP address; and (2) his computer and its contents.

i. Broy's IP Address

The Seventh Circuit has recently given guidance on whether a defendant has a reasonable expectation of privacy in his or her IP address. *United States v. Caira*, --- F.3d --- 2016 WL 4376472 (7th Cir. Aug. 17, 2016). In *Caira*, the DEA was monitoring a website through which the user of gslabs@hotmail.com was asking about buying sassafras oil, an ingredient in ecstasy. The DEA subpoenaed Microsoft Corporation (the owner of Hotmail), asking for basic information including, *inter alia*, the user's "IP Login history," which the user had necessarily and voluntarily communicated to both Microsoft and Comcast Corporation (the owner of the I.P. address commonly associated with the email

account). *Id.* at *1. Subsequent investigation and an additional subpoena led the DEA to determine the defendant was the user of the email address. The defendant made a motion to suppress the information gleaned from the subpoenas, which the district court denied. The Seventh Circuit held that sharing his IP address with a third party negated the defendant's reasonable expectation of privacy for Fourth Amendment purposes. *Id.* at *5. Indeed, the court noted that even if the defendant had a subjective expectation of privacy in such information, "once information is voluntarily disclosed to a third party, any such expectation is 'not one that society is prepared to recognize as reasonable.'" *Id.* at *2 (quoting *Smith v. Maryland*, 442 U.S. 735, 743 (1979)).

The government claims that, despite his attempts to conceal his identity, Broy had no reasonable expectation of privacy in his IP address because he communicated it to third parties. ECF No. 19-1 at 7. Broy, on the other hand, claims that he still had a reasonable expectation of privacy in his IP address because he was "not logging into an open commercial website, but using the anonymous Tor network, which as the government itself acknowledged, cloaks and scrambles a user's actual IP address." ECF No. 22 at 2. The Court finds Broy's distinction unpersuasive. The fact that Broy may have felt as if his identity was anonymous does not negate the fact that, in order to gain that feeling of anonymity, he voluntarily disclosed his IP address to the operator of the first Tor node. Moreover, the Court finds Broy should not be able to use the Tor network as both a shield to conceal his identity and a sword to claim a reasonable expectation of privacy such that accessing that information without a warrant would violate the Fourth Amendment. Accordingly, the Court holds Broy did not have a reasonable expectation of privacy in his IP address, and, thus, its discovery by the FBI was not a search that required a warrant under the Fourth Amendment.

ii. Broy's Computer

Broy further argues, albeit briefly, that he had a reasonable expectation of privacy in his computer itself, ECF No. 13 at 11, and the Court agrees. The Court begins by noting how, in the present case, it is possible that Broy may have had no reasonable expectation of privacy in his IP address, yet it was still unobtainable without a warrant. Considering the same warrant at issue in this case, the district court in *Adams* nicely framed the issue:

> 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 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. 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.

Adams, 2016 WL 4212079 at *4 (emphasis added) (internal citation omitted).

To determine whether Broy had a reasonable expectation of privacy in his computer, the Court relies on the five-factor *Peters* test and recent Supreme Court jurisprudence. All five *Peters* factors either point in Broy's favor or are unclear from the record. As noted *supra*, page 4 n. 2, the computer may have technically belonged to Broy's mother, but he certainly had a possessory interest in it. Along with that interest came the right to exclude people from its use.[3] Broy also had the subjective expectation that his computer would remain free from governmental invasion. The record is unclear as to whether he took normal precautions to maintain his *computer's* privacy, but if the steps Broy took to protect his IP address are indicative, the fourth factor points in his favor.

[3] It is possible that his mother also used the computer, but "the fact that others may have occasional access to the computer" does not necessarily extinguish any privacy expectations. *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (citing *Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001)).

Finally, he was legitimately on his computer. Thus, *Peters* suggests Broy had a legally sufficient interest in his computer such that the Fourth Amendment protected it from unreasonable, warrantless searches.

In *Riley v. California*, 134 S. Ct. 2473 (2014), the United States Supreme Court unanimously held police officers generally may not, without a warrant, search the digital information on cell phones seized from defendants during searches incident to arrest. *Id.* at 2485. The Court rejected the United States' contention that police could, at the very least, access the call log in arrestees' phones. *Id.* at 2492–93. The United States believed police had this authority based on *Smith*, where the Court found the use of a pen register did not constitute a Fourth Amendment search. *Id.* at 2492–93. *See also Smith*, 442 U.S. at 745–46. In *Riley*, however, the Court noted there was "no dispute" that officers engaged in a search of the defendants' cell phones. *Riley*, 134 S. Ct. at 2492–93. Thus, like the stolen vehicle in the garage, it was irrelevant that the defendants may not have had a reasonable expectation of privacy in some pieces of information in the phones so long as they had one in the phones more broadly. *Id.* at 2492–93.

As noted above, *supra* page 9, Broy did not have an expectation of privacy in his IP address. And while the Court does not decide whether he had a reasonable expectation of privacy in the other six specific pieces of information gathered and sent by the NIT, the Court finds Broy had a reasonable expectation of privacy in his computer more generally under *Riley*. Thus, the use of the NIT constituted a Fourth Amendment search.

The Court notes that at least two district courts which have considered both the warrant at issue in this case and whether the respective defendants had reasonable expectations of privacy in their *computers* have come to the conclusion that such privacy expectations existed. *See Adams*, 2016 WL 4212079 at *4; *Darby*, 2016 WL 3189703 at **5–6.

The opinion of one district court that decided differently, however, is worth mentioning. In *Matish*, the court found the defendant had no reasonable expectation of privacy in his computer. *Matish*, 2016 WL 3545776 at *21. The court first noted – this Court thinks incorrectly – that "the NIT only obtained identifying information; it did not cross the line between collecting addressing information and gathering the contents of any suspect's computer." *Id.* at *22. But while the "identifying information" may not have been images of child pornography, it was still part of the computer's code. Indeed, as the *Darby* court said, "[t]he 'contents' of a computer are nothing but its code." *Darby*, 2016 WL 3189703 at *6. Thus, the NIT did, in fact, gather the contents of the defendants' computers. Next, the *Matish* court, through a history of hacking, detailed society's changing view of the Internet and supposed corresponding diminished expectation of privacy in people's online posts and computers themselves. *Matish*, 2016 WL 3545776 at *22–23. It continued by referring to Justice Breyer's concurrence in *Minnesota v. Carter*, 523 U.S. 83 (1998). The *Matish* court concluded that just as "a police officer who peers through broken blinds does not violate anyone's Fourth Amendment rights, FBI agents who exploit a vulnerability in an online network do not violate the Fourth Amendment." *Matish*, WL 3545776 at * 23 (internal citation omitted). This Court rejects that comparison. Using the NIT to "exploit a vulnerability in the online network" is not akin to police merely peering through broken blinds; it is akin to the police breaking the blinds and then peering through them. The *Matish* court finally noted the severity of child pornography, likening it to an international crime. *Id.* at 23. While this Court appreciates the deplorable nature of child pornography, the crime itself is immaterial in deciding whether a defendant had a reasonable expectation of privacy in his computer.

Having concluded the use of the NIT constituted a Fourth Amendment search, the Court must now turn its attention to whether the warrant upon which the search was premised was valid.

C. Whether the Magistrate's Issuance of the NIT Warrant Violated the Federal Magistrate's Act and Rule 41(b)

The Federal Magistrate's Act, 28 U.S.C. § 636, specifically incorporates the Federal Rules of Criminal Procedure. Accordingly, the Court combines its analysis of the Federal Magistrate's Act and Rule 41(b) and finds the magistrate judge acted without authority to issue the warrant. Rule 41(b) provides that upon the request of a federal law enforcement officer or government attorney:

> (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 the 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 the 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(b). Subsections (b)(3) and (5) are clearly inapplicable to the present case. The government, however, argues subsections (b)(1), (2), and (4) all permit the magistrate's actions. Accordingly, the Court shall consider and reject each argument in turn.

i. 41(b)(1)

The government argues "it was reasonable" for the magistrate to issue the warrant because "the defendant entered the Eastern District of Virginia by accessing the Playpen server there, retrieved the NIT from that server, and the NIT sent his information back to a server in that district." ECF No. 15 at 43. Subsection (b)(1), however, is unconcerned with those activities. Rather, it allows a magistrate "to issue a warrant to search for and seize a person or property located within the district." While the NIT may have been deployed from the Eastern District of Virginia, the search it initiated took place in Broy's computer in Illinois. Furthermore, while Broy himself may have virtually entered the Eastern District of Virginia, he did not bring with him the information the NIT instructed the computer to transmit back to the government.[4] Thus, Rule 41(b)(1) did not authorize the magistrate to issue the warrant.

ii. 41(b)(2)

[4] There is a colorable argument that he brought with him his IP address, but the Tor network ensured the IP address he brought was not from the "activating computer." Furthermore, he certainly did not bring with him the other six pieces of information the NIT gathered and returned to the government. Those stayed in the computer in Illinois until the NIT accessed them.

The government also contends subsection (b)(2) authorized the magistrate to issue the warrant because the NIT was originally installed on a government server in the Eastern District of Virginia. ECF No. 15 at 42. The government again misses the point. Subsection (b)(2) allows a magistrate to issue a warrant for a person or property outside the district if that person or property is within the district when the warrant is issued but may move or be moved outside the district before the warrant is executed. It does not create methods by which to seize property that was never in the district. It is true that the NIT was in the district when the warrant was issued. But the property to be searched and seized, namely Broy's computer and its contents, remained in Illinois. The Court acknowledges the government's position is not an unreasonable one in the abstract, but it is weak given the mechanics of how the NIT operated.[5] Thus, subsection (b)(2) similarly did not authorize the magistrate's actions.

iii. 41(b)(4)

The government dedicates most of its Rule 41(b) analysis to subsection (b)(4), the "tracking device" subsection. As the government put it, "[i]nvestigators installed the NIT in the Eastern District of Virginia on the server that hosted [Website A]. When the defendant logged on and retrieved information from that server, he also retrieved the NIT. The NIT *then sent network information from the defendant's computer back to law enforcement*." ECF No. 15 at 39 (emphasis added). The government's own wording is fatal to its argument. Subsection (b)(4) allows the installation of a tracking device to track the *movement* of a person or property; it does not allow the installation of a device that searches for information that it then sends back to the government. The Court agrees with the court in *Adams*: "the NIT [did] not track; it searche[d]." *Adams*, 2016 WL

[5] If, for example, a suspect visited the Eastern District of Virginia with his computer but was likely to leave the district soon, this subsection may have authorized the magistrate's actions.

4212079 at *6. *But see Darby*, 2016 WL 3189703 at **11–12; *Matish*, 2016 WL 3545776 at **15–17. Thus, subsection (b)(4) did not authorize the magistrate to issue the warrant.

Because none of Rule 41(b)'s subsections authorized the magistrate's actions, the Court is left to conclude the issuance of the warrant violated Rule 41. By the government's own admission, because "the warrant was issued without lawful authority under Rule 41, it [was] void at the outset," or *ab initio*. ECF No. 15 at 28. *See also Levin*, 2016 WL 2596010 at *15. *But see Adams*, 2016 WL 4212079 at *6. As mentioned above, *supra* page 11, Broy had a reasonable expectation of privacy in his computer such that the use of the NIT was a Fourth Amendment search. The Court thus finds the government's actions ran afoul of Broy's Fourth Amendment protections. Accordingly, it is left to consider whether suppression is an appropriate remedy in this case.

D. Whether Suppression is an Appropriate Remedy

Broy argues that in the face of a violation of Rule 41(b) of constitutional magnitude, the Court should suppress the evidence discovered as a result of the Fourth Amendment violation. ECF No. 13 at 12–14. The government, on the other hand, argues suppression is not the proper remedy, any constitutional violation notwithstanding. ECF No. 15 at 34–36. The Court agrees with the government in this case.

"The fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009) (citing *Illinois v. Gates*, 462 U.S. 213, 223 (1983)). In fact, exclusion has always been considered a "last resort, not [a] first impulse." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006).

The Court in *United States v. Arterbury*, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091 (N.D. Okla. Apr. 25, 2016) on which Broy relies in part, pointed to relevant Seventh Circuit law which, in its opinion, would resolve any suppression question in the

Seventh Circuit. *Arterbury*, 2016 U.S. Dist. LEXIS 67091 at **15–17. *U.S. v. Cazares-Olivas*, 515 F.3d 726 (7th Cir. 2008), for example, says "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause." 515 F.3d at 730. Furthermore, "[t]he remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant would be 'wildly out of proportion to the wrong.'" *U.S. v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008) (quoting *Cazares-Olivas*, 515 F.3d at 730). While this Court believes these two cases are instructive, it notes that whether they control is not a certainty. Neither *Cazares-Olivas* nor *Berkos* involved warrants specifically determined to be void *ab initio*, as the warrant in this case has been.[6] In addition, the depth of the Rule 41 analyses in those cases is not as great as here. But regardless whether *Cazares-Olivas* and *Berkos* dictate a result, the Court still finds suppression inappropriate in the instant case under the good faith exception to the exclusionary rule.

In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court announced its "good-faith exception" to the exclusionary rule and held suppression is not warranted when officers act in reasonable reliance on a search warrant issued by a detached and neutral magistrate. 468 U.S. at 913, 925–26. It found suppression "should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." *Id.* at 918. The primary purpose of the exclusionary rule is, of course, "to safeguard Fourth Amendment rights generally through its deterrent effect." *Id.* at 906 (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)). The good faith exception to the exclusionary rule turns on "objective reasonableness." *Id.* at 924.

[6] The Court sees no other way of reading *Cazares-Olivas*, however, where the Seventh Circuit noted "[t]he agents had judicial approval, based on probable cause, but they did not have a warrant." 515 F.3d 726, 729. The same scenario presents itself in the current case.

It appears to be an unsettled question whether the *Leon* exception applies to warrants that are void *ab initio*. Broy points to the *Levin* court, which held Supreme Court precedent did not require the *Leon* exception be applied to searches pursuant to warrants that are determined to be void *ab initio*. ECF No. 18 at 12–13. *See also Levin*, 2016 WL 2596010 at *12–13. Broy further points to *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), where the Tenth Circuit recently affirmed a district court's order granting the defendant's motion to suppress because suppression would "further[] the purpose of the exclusionary rule by deterring law enforcement from seeking and obtaining warrants that clearly violate" Rule 41(b). *Krueger*, 809 F.3d at 1117. His argument that *Krueger* is applicable in this case boils down to his assertion that the government was not merely negligent, but rather that they made "purposeful misrepresentations" to the magistrate judge, thus foreclosing any possibility of objective reasonableness. ECF No. 18 at 15. Broy claims *Herring*, 555 U.S. 135 (2009), is inapplicable here for this same reason. The Court need not decide whether the government was even negligent, however, as it finds Broy is mistaken as to *Herring*'s applicability.

In *Herring*, Chief Justice Roberts wrote that in order "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." 555 U.S. at 144. He noted Supreme Court cases "require any deterrence to be weighed against the substantial social costs exacted by the exclusionary rule." *Id.* at 144 n.4 (internal quotations omitted). Here, while Broy claims the FBI having two different judges issue warrants is evidence of deliberateness and culpability, this is nothing but rank speculation in which the Court cannot engage. In fact, the Court finds no indication in this record of any false or misleading statements made to the magistrate in the warrant application that could support an inference of bad faith. On the contrary, the

government's efforts in establishing probable cause and obtaining the NIT warrant were unusually detailed and specific. Such efforts are to be lauded, not deterred.

Moreover, the only benefit to suppression in this case would be ensuring magistrate judges are more careful about issuing NIT warrants in the future, but two reasons limit the effect of such a benefit. First, the benefit would not last for long. On April 28, 2016, the Supreme Court approved an amendment to Rule 41(b) which, when it takes effect on December 1, 2016, will empower magistrate judges to issue warrants which authorize remote searches of computers wherever located if the computer's location has been concealed through technological means.[7] Second, and more importantly, the exclusionary rule is designed to control the conduct of *law enforcement*, not the conduct of federal judges. *E.g.*, *Leon*, 468 U.S. at 906–08. As mentioned above, law enforcement exhibited laudable conduct in this case. The Court further notes that, in any event, Broy was not prejudiced by the Rule 41(b) violation. The record contains no indication of any impediment or legal barrier that would have arisen to prevent a district judge from issuing the NIT warrant. Thus, the Court finds *Herring* counsels against suppression. Overall, then, the *Leon* exception to the exclusionary rule applies. Suppression is not an appropriate remedy in this case.

Conclusion

For the reasons set forth herein, Broy's Motion to Suppress Evidence (ECF No. 12) is DENIED.

ENTERED this 21st day of September, 2016.

s/ Michael M. Mihm
Michael M. Mihm
United States District Judge

[7] The full amendment can be found at https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf.