IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, vs. DOMINIC C. DZWONCZYK, Defendant.	**4:15CR3134** **FINDINGS, RECOMMENDATION AND ORDER**

This matter is before the court on Defendant Dominic C. Dzwonczyk's Motion to Suppress evidence (Filing No. 37). For the reasons set forth below, the motion should be denied.

BACKGROUND

This case is one of many originating from a search warrant issued in the Eastern District of Virginia, each such case consisting of a similar fact pattern. In January of 2015, the Federal Bureau of Investigation ("FBI") received a warrant to seize a computer server. The server supported a website called "Playpen" which contained child pornography (referred throughout law enforcement affidavits as the "Target Website"). The Playpen website was operated on The Onion Router ("Tor network"). The Tor network is accessed only through Tor software available as "an add-on to the user's web browser or by downloading the free 'Tor: browser bundle' available at www.torproject.org." (Filing No. 40 at CM/ECF p. 16).

Websites on the Tor network typically cannot be accessed through traditional internet search means – e.g., the Playpen website could not be found through a traditional search engine like Google or Yahoo. As explained in the warrant application, a user must: a) have access to the Tor network, and b) know the Tor Network address for Playpen.

> Even after connecting the TOR network, however, a user must know the web address of the website in order to access the site. Moreover, TOR "hidden services" are not indexed like websites on the traditional internet. Accordingly, unlike the traditional internet, a user may not simply perform a Google search for the name of one of the websites on TOR to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from internet postings describing the sort of content available on the website, as well as the websites location. For example, there is a TOR "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to TOR "hidden services" that contain child pornography. The [Playpen] website is listed in that section.

(Filing No. 40 at CM/ECF p. 17, ¶10).

"The Tor software protects users' privacy online by bouncing their communications around a distributed network or relay computers run by volunteers all around the world, thereby masking the user's actual IP address[1] which could otherwise be used to identify a user." (Filing No. 40 at CM/ECF p. 16, ¶ 8). These relay computers are known as "nodes." "An exit node is the last computer through which a user's communications were routed." (Filing No. 39 at CM/ECF p. 16, ¶ 8). "When a user on the Tor network accesses a website . . . the IP address of a Tor 'exit node,' rather than the user's actual IP address, shows up in the website's IP log." Id.

The server seized in January of 2015 was moved to a Government facility in Newington, Virginia. The FBI then took administrative control over the server. Once the seized server was under FBI control, the FBI sought and received a warrant in the Eastern District of Virginia to deploy a Network Investigative Technique ("NIT") – a method

[1] An IP address or Internet Protocol Address "refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the Internet Service Provider (""ISP"") assigns a different unique number to a computer every time it accesses the Internet, IP addresses might also be "Static," if an ISP assigns user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers." Filing No. 40 at CM/ECF pp. 13-14, ¶5(m).

used to force a computer to send its actual IP address to the website in question. As described in the warrant application:

> In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display webpages on the user's computer. Under the NIT authorized by this warrant, the [Playpen website], which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the [Playpen website], located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in attachment B of this affidavit), and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

(Filing No. 40 at CM/ECF p. 29, ¶33).

The NIT allows law enforcement to gather information about users contacting the Playpen website. All of this information can assist the FBI with identifying the actual user of the website, thereby circumventing the masking effect of the Tor Network.

The warrant application submitted to Magistrate Judge Theresa Carroll Buchanan in the Eastern District of Virginia sought authorization for the NIT to "cause an activating computer – wherever located – to send to a computer controlled by or known to the government network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer . . . ." (Filing No. 40 at CM/ECF pp. 34-35, ¶ 46(a)). The "other" information included the computer's actual IP address, active operating system username, and the computer's Media Access Control ("MAC") address. The Magistrate Judge found probable cause and signed the warrant.

During the government's control and administration of the Playpen website, a user with the username "RebeckaBecka" accessed the Playpen website and was accessing images of child pornography. Though the use of the NIT, the FBI determined IP address 68.226.50.32 was assigned to "RebeckaBecka." Further investigation determined the IP address used by "RebeckaBecka" was assigned to Cox Communications, an internet service provider serving Bellevue, Nebraska. Law enforcement ascertained through Cox Communications that the IP address was assigned to defendant Dominic C. Dzwonczyk at a residence in Bellevue, Nebraska. Law enforcement requested and received a warrant in Nebraska (the "Nebraska Warrant") to search Dzwonczyk's residence. During execution of the Nebraska Warrant, law enforcement officers found evidence of child pornography on the computers located in Defendant's residence.

Dzwonczyk has moved to suppress all evidence obtained from the search of his residence and the computers therein. He asserts: 1) the warrant from the Eastern District of Virginia (the "Virginia Warrant") was issued in violation of Fed. R. Crim. P. 41 and 28 U.S.C. § 636(a) because a Magistrate Judge does not have the power to issue a warrant to authorize the search of computers outside her district; 2) since information improperly seized through the invalid Virginia Warrant provides the probable cause basis for the Nebraska Warrant, the evidence found during the search of Defendant's Nebraska residence must be suppressed; and 3) the Virginia Warrant was void at the outset, so the Leon good faith exception is inapplicable.

ANALYSIS

Several district courts have ruled on similar motions to suppress evidence discovered in connection with the Virginia Warrant. See, e.g., United States v. Jean, case no. 5:15cr50087, 2016 WL 4771096 (W.D. Ark, Sept. 13, 2016); United States v. Henderson; case no. 15cr0565, 2016 WL 4549108 (N.D. Cal. September 1, 2016); United States v. Ammons, case no. 3:16cr00011, 2016 WL 4926438 (W.D. Ken. September 14, 2016); United States v. Levin, --- F. Supp. 3d ---, 2016 WL 2596010 (D. Mass. May 5, 2016); United States v. Weredene, --- F. Supp. 3d. ---, 2016 WL 3002376 (E.D. Penn. May 18, 2016); United States v. Matish, --- F. Supp. 3d ---, 2016 WL 3545776 (E.D. Vir. June 23, 2016); United States v. Darby, --- F. Supp. 3d ---, 2016 WL 3189703 (E.D. Vir. June 3, 2016); United States v. Michaud, case no. 3:15cr5351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). Although, the courts have employed different reasoning, the vast majority have held suppression of the evidence gained through the Virginia Warrant and various other local warrants was not appropriate.

Defendant's motion requests suppression for violation of his Fourth Amendment rights. As such, the threshold question is whether Defendant has a reasonable expectation of privacy in the location searched and/or the evidence obtained through execution of the Virginia Warrant. If Defendant can assert a privacy interest society is willing to recognize, then the court must decide whether using a NIT from a Virginia server to obtain an IP address from a Nebraska computer was a search beyond the borders of Virginia such that a warrant authorizing this activity was beyond the statutory and rule authority of the Virginia magistrate judge. Finally, even assuming Defendant has a privacy interest in his IP address and, as applied to computers outside Virginia, the Virginia magistrate judge exceeded her territorial authority when she issued the Virginia Warrant, the court must determine whether officers acted reasonably when they relied on

the Virginia and Nebraska warrants; that is, whether Defendant's motion must be denied under the Leon good faith exception.

1. Defendant's "Reasonable Expectation of Privacy" in the Property Searched.

The Fourth Amendment provides, in part, that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. "It is clear that a physical intrusion or trespass by a government official constitutes a search within the meaning of the Fourth Amendment." United States v. De L'Isle, 825 F.3d 426, 431 (8th Cir. 2016)(citing United States v. Jones, --- U.S. ---, 132 S.Ct. 945, 949, 181 L.Ed.2d 911 (2012)). But "[a] search is reasonable if the officer has a valid search warrant or if the search fits within a specific warrant exception." Id.

For a "search" to occur within the meaning of the Fourth Amendment, an individual must have a "reasonable expectation of privacy" in the place or thing subjected to search. United States v. Jones, --- U.S. ---, 132 S.Ct. 945, 950, 181 L.Ed.2d 911 (2012). "For this type of violation, the claimant must show both "an actual (subjective) expectation of privacy, and ... that the expectation [is] one that society is prepared to recognize as 'reasonable.'" DE L'Isle, 825 F.3d at 431 (internal quotations omitted). If a law enforcement official's search does not offend a person's reasonable expectation of privacy, the Fourth Amendment is not implicated. Id.

The Eighth Circuit held that a person has no reasonable expectation of privacy in internet subscriber data, "including his IP address and name from third-party service providers." United States v. Wheelock, 772 F.3d 825, 828-29 (8th Cir. 2014)(internal citations omitted); see United States v. Laurita, case no. 8:13cr107, 2016 WL 4179365 (D. Neb. August 5, 2016)(Hon. Joseph F. Bataillon)("Generally, one has no reasonable

expectation of privacy in an IP address when using the internet")(citing United States v. Forrester, 512 F.3d 500, 509-11(9th Cir. 1999)). The lack of an expectation of privacy exists because an individual necessarily shares the IP address assigned to his computer to and from third parties, such as an Internet Service Provider ("ISP"). "A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." United States v. Miller, 425 U.S. 435, 442-44 (1976); see also United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010) (a person has "no reasonable expectation of privacy in his IP address" because the information is conveyed to and from third parties).

If the sole question was whether a Defendant has a reasonable expectation of privacy in his IP Address, applying Eighth Circuit law, the answer would simply be "No." But under the facts of this case, the issue is complicated by Defendant's use of the Tor Network to hide his IP address. And unlike the facts in the Eighth Circuit's holding in Wheelock, Defendant's IP address was obtained using a NIT which prompted Defendant's computer to reveal the actual IP address, and not through a subpoena served on a third-party internet service provider. Wheelock, 772 F.3d at 828-29 (finding the government's acquisition of the defendant's IP address through a third-party subpoena to an internet service provider did not violate the defendant's Fourth Amendment rights). Thus, the court must consider "whether the Tor user's expectation of privacy in his IP address may be stronger, or more legitimate, than that of an internet user who has taken no steps to conceal his IP address." Jean, 2016 WL 4771096 at *9.

As explained above, the Tor Network conceals a user's IP address prior to connecting with the end website. The main purpose of the Tor Network is for a user to avoid being identified. But even when using the Tor Network, an individual's IP address is disclosed to the first "node" in the Tor Network before being bounced to subsequent "nodes." "Using the Tor network does not strip users of all anonymity, because users accessing [Playpen] must still send and receive information, including IP addresses,

through another computer . . . at a specific location." Michaud, 2016 WL 337263 at *7. "[A] necessary aspect of Tor is the initial transmission of a user's IP address to a third-party." Werdene, --- F. Supp. 3d at ---, 2016 WL 3002376 at *8. "[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 communications can be directed toward their destinations." United States v. Farrell, 2016 WL 705197 at *2 (W.D. Wash. Feb. 23, 2016). The Tor project itself warns users: "Tor cannot solve all anonymity problems. It focuses only on protecting the transport of data. You need to use protocol-specific support software if you don't want sites you visit to see your identifying information."
See https://www.torproject.org/about/overview.html.en#stayinganonymous, last visited September 23, 2016.

With or without Tor, Defendant was sharing his IP address with others—total strangers, to potentially include law enforcement officers—with the hope and belief that the users of the first "node" computer would keep his IP address secret. While Defendant's choice to use Tor may be evidence of his "actual, (subjective) expectation of privacy" in his IP address, using Tor does not elevate that expectation to "one that society is prepared to recognize as 'reasonable.'" DE L'Isle, 825 F.3d at 431. Under the facts presented, like other courts, this court finds a user of the Tor network does not have a reasonable expectation of privacy in his IP address. See Werdene, --- F. Supp. 3d at ---, 2016 WL 3002376 at *9 ([Defendant] was aware that his IP address had been conveyed to a third party and he accordingly lost any subjective expectation of privacy in that information"); Michaud, 2016 WL 337263 at *7 ("Even though it was difficult for the Government to secure that information tying the IP address to [Defendant], the IP address was public information, like an unlisted telephone number, and eventually could have been discovered"). See also Jean, 2016 WL 4771096 at *7-10 (holding a search warrant to retrieve Defendant's IP address was unnecessary); Matish, --- F. Supp. 3d ---, 2016

WL 354776 at *22-24 (same); United States v. Acevedo-Lemus, case no. SACR 15-00137, 2016 WL 4208436 (C.D. Cal. August 8, 2008) (same).

The court must also decide whether a search occurred when the government deployed a NIT from the Target Server when contacted by Defendant's computer. While Defendant has no reasonable expectation of privacy in his IP address, he does have a privacy interest in his home and its contents. And absent exigent circumstances, law enforcement could not lawfully conduct a warrantless search of Defendant's home computer to obtain Defendant IP address.

But deploying the NIT to reveal the IP address was not a computer search. Defendant's IP address is not a "physical component" of the computer or a file residing on his computer like electronic documents or pictures. See Acevedo-Lemus, 2016 WL 4208436 at *5; Jean, 2016 WL 4771096 at *5. Rather, the IP address is assigned to a user by the ISP and typically is "maintained on the internet modem that connects an internet device to the internet." Jean, 2016 WL 4771096 at *5. Thus, the NIT essentially compelled Defendant's computer to produce its IP address (similar to a return address on an envelope) when the NIT instructed the computer to send other information identified in the Virginia Warrant. See Jean, 2016 WL 4208436 at *5. And the NIT was deployed only after Defendant sought out and visited the Playpen website. "The FBI did not come looking for Defendant. Instead it waited until he came to them and engaged in illicit activity by downloading content from Playpen." Acevedo-Lemus, 2016 WL 4208436 at *5. See also Matish, --- F. Supp. 3d ---, 2016 WL 3545776 at *22-24 (holding that with the prevalence of computer hacking and the "compromise of unprecedented amounts of data previously thought to be private," all individuals have a diminished expectation of privacy once they log onto the internet.)

This magistrate judge finds the government's act of deploying the NIT from the Target Server was not an authorized search of a home computer for the purposes of Fourth Amendment analysis, and it did not reveal information for which Defendant had a reasonable expectation of privacy. For these reasons alone, Defendant's motion to suppress should be denied.

2. Rule 41(b): Validity of the Virginia Warrant.

Assuming using a NIT from a Virginia server to obtain an IP address from a Nebraska computer was a search, the court must consider whether the Virginia warrant was valid. Defendant argues the Virginia Magistrate Judge exceeded the authority granted by statute and Rule 41 of the Federal Criminal Rules when she signed a warrant allowing officers to search computers outside the Eastern District of Virginia. Defendant argues that since the Virginia Warrant was void, the Nebraska Warrant, which relied on information obtained through the Virginia Warrant, is likewise void.

Rule 41(b) provides:

> 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.Crim.R. 41(b).

Defendant asserts the plain language of Rule 41 does not authorize a United States Magistrate Judge to issue a warrant to search property outside of her assigned district. Moreover, he argues subpart (4) does not apply because even if the NIT is a "tracking device," it was not installed in the magistrate judge's assigned district. The Government's argues the NIT is a "tracking device" and the magistrate judge's warrant was properly issued pursuant to Rule 41(b)(4).

Defendant relies heavily on Levin, --- F. Supp. 3d ---, 2016 WL 2596010 at *5-6. In Levin, the court determined the Virginia Warrant was not issued for searching or

seizing property only within the Eastern District of Virginia. The warrant was used to "obtain information" from various "activating computers" wherever located, including outside the district where the issuing Magistrate Judge was located. Levin determined the NIT technology was not akin to a tracking device. See also United States v. Croghan, --- F. Supp. 3d. ---, 2016 WL 4992105 (S.D. Iowa September 19, 2016); United States v. Henderson, case no. 15cr565, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016). Other courts have determined that even if it was a tracking device, the requirement of Rule 41(b)(4) was not fulfilled. That is, because the object of the search is a computer out of the district and that computer was never "physically located within the Eastern District of Virginia, law enforcement officers could not attach a tracking device to it while it was in the Eastern District of Virginia. See Mirchaud, 2016 WL 337263 at *6.

In contrast, other courts have found Magistrate Judge Buchanan was authorized by Rule 41(b)(4) to sign the Virginia Warrant. Darby, --- F. Supp. 3d ---, 2016 WL 3189703 at *12; Jean, 2016 WL 4771096 at *15-16; Matish, --- F. Supp. 3d ---, 2016 WL 3545776 at *17; see also United States v. Laurita, case no. 8:13cr107, 2016 WL 4179365 (D. Neb. August 5, 2016)(analogizing NIT to a pen register). Relying on the definitions set forth in Fed. R. Crim. P. 4, these courts have held the NIT operates as a "tracking device" for the purposes of Rule 41(b)(4), with installation of the tracking device occurring in the Eastern District of Virginia when a Defendant's computer contacts the Target Server located in Virginia.

Rule 41 defines a "tracking device" as any "electronic or mechanical device which permits the tracking of the movement of a person or object." Fed. R. Crim. P. 41(a)(2)(E)(cross-referencing 18 U.S.C. § 3117(b). Rule 41(b)(4) expressly authorizes the tracking of "property" "which is specifically defined to include the tracking of mere intangible 'information.'" Jean, 2016 WL 4771096 at *16 (citing Fed. R. Crim. P. 41(a)(2)(A)). As explained in Jean:

> Here, the government was essentially seeking authority to conduct a sting operation, whereby it would re-launch the Playpen website from its own server in Virginia, after which the FBI would then monitor the flow of electronic information as Playpen users accessed the website for allegedly unlawful purposes. Upon entering this "watering hole," a user—while still immersed—would become infected with the malware as it was deployed to the user's computer incident to the process of downloading child pornography.

Jean, 2016 WL 4771096 at *16. And consistent with the purpose of a tracking device, the NIT provides information which assists the FBI in locating those computers accessing the government-controlled Playpen website.

Defendant argues Defendant and his computer were never physically present in Virginia; that the NIT was "installed" in Nebraska—beyond the territorial limits of the Virginia magistrate judge's authority. But the FBI agents were also never physically present in Nebraska to "install" a tracking device. As with many technology based law enforcement measures, the NIT does not fit traditional notions of how tracking devices are installed or attached because "[i]nternet crime and surveillance defy traditional notions of place." Jean, 2016 WL 4771096 at *15.

Like Jean, I find that by logging into the Playpen website hosted on the Target Server in Virginia, Defendant's computer made a "virtual trip" to the Eastern District of Virginia. As explained in the Virginia Warrant application, once Defendant's computer contacted the Playpen website, that website sent information back to Defendant's computer which, in turn, installed the NIT on Defendant's computer. The NIT then transmitted location information (the IP address) being accessed by Defendant's computer to the FBI. Thus, even assuming the government's use of a NIT impacted Defendant's reasonable expectation of privacy sufficient to raise a Fourth Amendment claim, the officers acted pursuant to a warrant issued by a magistrate judge acting within the territorial boundaries of her authority under Fed. R. Crim. P. 41(b)(4).

Even assuming the Virginia magistrate judge acted beyond her authority under Rule 41(b), any such violation was not sufficiently fundamental to justify suppressing the evidence found.

> The Court's first step in this analysis is to determine whether the violation of Rule 41(b)—assuming such occurred—was either "fundamental" and rendered the search unconstitutional under traditional Fourth Amendment standards, or "non-fundamental." United States v. Freeman, 897 F.2d 346, 350 (8th Cir. 1990). A fundamental violation would require automatic suppression of the evidence, whereas a non-fundamental violation, where no constitutional error occurred, would not trigger automatic suppression. Id. A non-fundamental violation would only justify suppression where there was prejudice to the defendant, "in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed," or if the defendant were able to show that law enforcement and/or the magistrate judge demonstrated an "intentional and deliberate disregard of a provision in the Rule. Id.

Jean, 2016 WL 4771096, at *17.

In his reply brief, Defendant argues (for the first time) that the Virginia magistrate judge's violation of Rule 41 was not merely "procedural." But he does not explain how that alleged violation rose to a constitutional level. "[A] violation is 'fundamental' only where it, in effect, renders the search unconstitutional under traditional fourth amendment standards." Freeman, 897 F.2d at 346. "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. United States v. Ryan Anthony Adams, case no. 6:16cr11, 2016 WL 4212079, at *7 (M.D. Fla. Aug. 10, 2016)(citing Dalia v. United States, 441 U.S. 238, 255 (1979)); see also Bowling v. Rector, 584 F.3d 956, 967-68 (10th Cir. 2009).

"A warrant is supported by probable cause from the viewpoint of a reasonably prudent police officer acting in the circumstances of a particular case." United States v.

Reinholz, 245 F.3d 765, 776 (8th Cir. 2001). "The determination of whether or not probable cause exists to issue a search warrant is to be based upon a common-sense reading of the entire affidavit." United States v. Seidel, 677 F.3d 334, 338 (8th Cir. 2012)(internal quotations omitted). "To satisfy the particularity requirement of the fourth amendment, the warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized." United States v. Horn, 187 F.3d 781, 788 (8th Cir. 1999).

Defendant does not challenge the Virginia magistrate judge's neutrality in reviewing and signing the Virginia Warrant. And the Virginia Warrant was supported by sufficient probable cause and met the particularity requirements of the Fourth Amendment. The law enforcement officers provided Magistrate Judge Buchanan with more than enough information about the content of the Playpen website for her to make a finding there was a "fair probability that evidence of a crime would be found" if the NIT was deployed. Likewise, the particularity requirement was met: The Virginia warrant clearly states officers were allowed to obtain the IP addresses of individuals visiting the Playpen website for the purpose of viewing and/or distributing child pornography. Accordingly, even assuming the NIT is not a tracking device, the Virginia magistrate judge did not commit a "fundamental" violation of Rule 41 by signing the Virginia warrant. See, e.g., Darby, --- F. Supp. 3d at ---, 2016 WL 3189703 at * 8 (the affidavit provided probable cause for the warrant); Jean, 2016 WL 4771096 at *10-12 (finding the Virginia warrant met the probable cause and particularity requirements of the Fourth Amendment); Werdene, --- F. Supp. 3d at ---, 2016 WL 3002376 at *7-10 (Virginia warrant met Fourth Amendment requirements); Matish, --- F. Supp. 3d at ---, 2016 WL 3545776 at *9-10 (Virginia warrant was supported by probable cause); Michaud, 2016 WL 337263 at *3-4 (finding the Virginia warrant met the particularity requirement).

3. Any non-fundamental violation did not prejudice Defendant.

Defendant argues even if the violation of Rule 41 was not fundamental, the evidence should be suppressed because he was prejudiced by the search. Filing No. 30 at CM/ECF p. 9. Non-fundamental violations require suppression only if: 1) the search would not have occurred but for the violation of Rule 41, or 2) the investigators "recklessly disregarded proper procedure." United States v. Welch, 811 F.3d 275, 280-81 (8th Cir. 2016).

The search could have commenced even if the magistrate judge had determined Rule 41(b) prevented her from issuing the warrant. Levin, --- F. Supp. 3d at ---, 2016 WL 2596010 at *14; Jean, 2016 WL 4771096 at *18 ("both parties appear to agree . . . that an Article III judge in the Eastern District of Virginia could have authorized this particular search warrant.") "Section 636(a) and Rule 41(b) limit the territorial scope of magistrate judges – they say nothing about the authority of district judges to issue warrants to search property located outside their judicial district." Levin, --- F. Supp. 3d at ---, 2016 WL 2596010 at *14 (emphasis in original). Thus, had the FBI interpreted Rule 41 as prohibiting a Virginia magistrate judge from issuing the Virginia warrant, it could have presented the application to a district judge in the Eastern District of Virginia. Defendant's IP address would have still been revealed and the Nebraska warrant would still have been supported by probable cause.

I therefore find that assuming Defendant shows the initial requirement of standing to challenge the Virginia warrant, that magistrate judge who signed the warrant did not exceed the bounds of her jurisdictional authority under Rule 41(b), and committed no fundamental or non-fundamental violation of Rule 41. The evidence found upon execution of the Virginia Warrant should not be suppressed.

4. Good Faith Exception

Even assuming a Defendant can and has raised a valid Fourth Amendment challenge to a warrant, the evidence obtained from executing that warrant will not be suppressed if the executing officers relied 'in objective good faith on a search warrant.' " United States v. Hessman, 369 F.3d 1016, 1020 (8th Cir. 2004) (citing Leon, 468 U.S. 897, 922 (1984)). The purpose of suppression is two-fold:

> Two inseparable principles have emerged from the Supreme Court cases and each builds upon the underlying purpose of the exclusionary rule: deterrence. First, the exclusionary rule seeks to deter objectively unreasonable police conduct, i.e., conduct which an officer knows or should know violates the Fourth Amendment. See, e.g., Herring, 129 S.Ct. at 701-04; Krull, 480 U.S. at 348-49 . . . . Second, the purpose of the exclusionary rule is to deter misconduct by law enforcement officers, not other entities, and even if it was appropriate to consider the deterrent effect of the exclusionary rule on other institutions, there would be no significant deterrent effect in excluding evidence based upon the mistakes of those uninvolved in or attenuated from law enforcement.

United States v. McCane, 573 F.3d 1307, 1044 (10th Cir. 2009). This good-faith exception does not apply:

> (1) when the issuing judge is misled by information in the affidavit the affiant knows or should know is false;
>
> (2) when the issuing judge completely abandons his or her judicial role;
>
> (3) when the affidavit includes so little indicia of probable cause that official belief in its existence is entirely unreasonable; and
>
> (4) when the warrant is so facially deficient that the executing officer cannot reasonably presume it to be valid.

Hessman, 369 F.3d at 1020 (citing Leon, 468 U.S. at 923, 104 S.Ct. 3405; LaMorie, 100 F.3d at 555).

Defendant argues the Leon exception is inapplicable to the Virginia Warrant because the agents should have known that the warrant was facially void: "The Government could not have acted in good faith when it was clearly aware that there was no authority to issue a warrant seeking seizure of information outside its territorial limits." (Filing No. 38 at CM/ECF p. 10).

In considering whether the good-faith exception applies, the court must consider the totality of the circumstances, recognizing the judge as "the final reviewing authority . . . must shoulder the ultimate responsibility" for errors in a warrant application. United States v. Berry, 113 F.3d 121, 124 (8th Cir. 1997). The Eighth Circuit has held that even when a facially obvious error exists on a warrant, the Leon good-faith exception may still apply. Hessman, 369 F.3d at 1021.

There is no evidence that the FBI misled Magistrate Judge Buchanan when presenting the warrant application. To the contrary, the warrant application clearly states the Government-controlled Target Server was located in the Eastern District of Virginia and the NIT would obtain information from computers located outside that district when those computers accessed the Playpen website. The warrant application accurately described the facts to Magistrate Judge Buchanan.

And contrary to Defendant's assertions, there is no evidence Magistrate Judge Buchanan abandoned her judicial role by acting as a "rubber stamp" or an "adjunct law enforcement officer" in issuing the warrant. Leon, 468 U.S. at 914. There is no evidence Judge Buchanan did not read the warrant carefully, nor is the warrant full of boiler plate language. See United States v. Farlee, 910 F. Supp. 2d 1174, 1187 (D.S.D. 2012). Rather, the warrant application is replete with very specific information regarding the Playpen website and its connection with child pornography.

And while the Defendant argues the Magistrate Judge should have known Rule 41 "clearly" did not provide her with authority to issue the warrant, this court is certainly not convinced. Some courts have concluded Magistrate Judge Buchanan was authorized to sign the Virginia warrant: Other courts disagree. In and of itself, this divergence in judicial opinions provides ample evidence that under the facts of this case, there was nothing "clear" about the magistrate judge's authority, or lack thereof.

"For the Leon exception to apply when the warrant is based on evidence obtained through a Fourth Amendment violation, the detectives' prewarrant conduct must have been 'close enough to the line of validity to make the officers' belief in the validity of the warrant objectively reasonable.'" United States v. Cannon, 703 F.3d 407, 413 (8th Cir. 2013) (quoting United States v. Conner, 127 F.3d 663, 667 (8th Cir.1997)). "The Supreme Court's line of good-faith cases clearly indicates that the reach of the exclusionary rule does not extend beyond police conduct to punish the mistakes of others, be they judicial officers or employees. . . ." McCane, 573 F.3d at 1045 (10th Cir. 2009).

Here, Defendant has provided no evidence indicating the Virginia Warrant lacked a showing of probable cause or judicial authority such that a reasonable officer would not have relied upon it in conducting a search. The warrant application provided the magistrate judge with copious amounts of information linking the Playpen website to child pornography; the affiant officers did not conceal the fact that the NIT would deploy to computers located outside the Eastern District of Virginia; and law enforcement may reasonably rely upon the interpretation of the law by the magistrate judge issuing the warrant. Leon's aim is to deter officer misconduct. Excluding evidence due to a mistake of law attributable to the court, not the law enforcement officer, would undermine the purpose of the Leon good faith exception. See McCane, 573 F.3d at 1045.

Accordingly,

IT IS THEREFORE RECOMMENDED to the Honorable John M. Gerrard, United States District Judge, pursuant to 28 U.S.C. § 636(b), that the motion to suppress filed by Dominic C. Dzwonczyk, (Filing No. 37), be denied in all respects.

The parties are notified that failing to file an objection to this recommendation as provided in the local rules of this court may be held to be a waiver of any right to appeal the court's adoption of the recommendation.

IT IS ORDERED: A status conference to discuss defendant's pending motion for discovery is set for October 12, 2016 at 1:00 p.m. Counsel for the Government shall initiate the call.

Dated this 5th day of October, 2016

BY THE COURT:

s/ Cheryl R. Zwart
United States Magistrate Judge