IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA, v. GABRIEL WERDENE, *Defendant.*	CRIMINAL ACTION NO. 15-434

PAPPERT, J. **MAY 18, 2016**

MEMORANDUM

Gabriel Werdene ("Werdene") was indicted on September 17, 2015 on one count of possessing and attempting to possess child pornography pursuant to 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). The indictment was based on evidence obtained during a June 17, 2015 search of Werdene's Bensalem, Pennsylvania home, which was conducted in accordance with a warrant issued by a magistrate judge in this judicial district. The Federal Bureau of Investigation ("FBI") identified Werdene after a magistrate judge in Virginia issued a warrant permitting agents to deploy software that revealed the IP addresses of visitors to a child pornography website called Playpen.[1] FBI agents matched Werdene's Playpen username, "thepervert," to his IP address and then located his home in Bensalem based on that information.

Playpen's patrons accessed the website through software called "Tor," an acronym for "The onion router." Tor conceals the IP addresses of people who visit certain websites, in Werdene's case a website purveying child pornography. Otherwise stated, Tor enables people to use websites like Playpen to view, upload and share child pornography without being identified by traditional law enforcement investigative methods. To circumvent Tor, the FBI used a

[1] The parties refer to Playpen as "Website A," ostensibly to preserve the anonymity of the site during the continued investigation of its users and administrators. A number of published articles and judicial opinions, *see infra* Section I.E, have already identified "Website A" as Playpen, eliminating the need for any further efforts to conceal its identity.

Network Investigative Technique ("NIT"). The NIT caused software to be activated whenever a Playpen user logged into the website with his username and password. The software caused the Playpen user's computer to reveal its IP address to the FBI. The search warrant issued by the Virginia magistrate authorized the NIT.

Werdene moves to suppress the evidence seized from his home, arguing primarily that the magistrate judge in Virginia lacked jurisdiction under Federal Rule of Criminal Procedure 41 to authorize the NIT. Werdene contends that this violation of a procedural rule warrants suppression. While Rule 41 did not authorize the issuance of the warrant in Virginia, suppression is not the appropriate remedy. The magistrate judge's failure to comply with Rule 41 did not violate Werdene's Fourth Amendment rights because Werdene had no expectation of privacy in his IP address, and certainly not one that society would recognize as reasonable. Even if Werdene's constitutional rights were violated, the good faith exception to the exclusionary rule precludes suppression. Finally, any nonconstitutional violation of Rule 41 did not prejudice Werdene, as that term has been defined by the Third Circuit Court of Appeals in the Rule 41 context. The Court denies the motion.

I.

Playpen operated on the "dark web," a collection of websites that use anonymity tools to hide those websites' IP addresses and mask the identity of their administrators. Websites on the dark web can only be accessed using certain software such as Tor. (*See* Gov't. Mem. in Opp. to Def.'s Mot. to Suppress ("Gov't's Opp."), Ex. 1 ¶¶ 7–10, ECF No. 21.) Playpen, as its name connotes in this context, was "dedicated to the advertisement and distribution of child pornography, [and] the discussion of matters pertinent to child sexual abuse." (*Id.*, Ex. 1 ¶ 6.) The website's home page displayed an image of two partially clothed prepubescent females with

their legs spread. (*Id.*, Ex. 1 ¶ 12.) Upon arriving at the home page, a user was prompted to either register an account or login using his pre-existing username and password. (*Id.*) Prior to registering an account, a message was displayed which told the user, among other things, "NOT [to] . . . enter a real [email] address" and "[f]or your security you should not post information here that can be used to identify you." (*Id.*, Ex. 1 ¶ 13.) The message also stated that "[t]his website is not able to see your IP address and can not [sic] collect or send any other form of information to your computer except what you expressly upload." (*Id.*)

After successfully registering and logging into the site, the user reached a page which listed a number of "forums" or discussion boards on which users could post images, videos or text regarding various topics. The "forums" included "Jailbait – Boy," "Jailbait – Girl," "Preteen – Boy," "Preteen – Girl," "Jailbait Videos," "Jailbait Photos," "Pre-teen Videos," "Pre-Teen Photos," "Family – Incest" and "Toddlers." (*Id.*, Ex. 1 ¶ 14.) Within the pre-teen videos and photos forums were "subforums" titled "Girls [hardcore]," "Boys [hardcore]," "Girls [softcore/non-nude]" and "Boys [softcore/non-nude]."[2] (*Id.*) Each forum contained a topic with titles, an author and the number of replies and views. (*Id.*, Ex. 1 ¶ 16.) Upon accessing a topic, the original post appeared at the top of the page with all corresponding replies to the original post below. (*Id.*) Typical posts contained text, links to external sites, and/or images. (*Id.*)

Playpen also included features available to all users of the website referred to as "Playpen Image Hosting" and "Playpen Video Hosting." (*Id.*, Ex. 1 ¶ 23.) Those pages allowed users to upload images and videos of child pornography for other users to view. (*Id.*) Over 1,500 unique users visited Playpen daily and over 11,000 unique users visited the site over the course of a

[2] FBI Special Agent Douglas Macfarlane ("Agent Macfarlane") stated in his warrant application to employ the NIT that "jailbait refers to underage but post-pubescent minors." (Gov't's Opp., Ex. 1 ¶ 14 n.4.) Furthermore, "hardcore" typically depicts "penetrative sexually explicit conduct," "softcore" depicts "non-penetrative sexually explicit conduct," and "non-nude" depicts "subjects who are fully or partially clothed." (*Id.*, Ex. 1 ¶ 14 n.5.)

week. (*Id.*, Ex. 1 ¶ 19.) According to statistics on the website, by March 2015 Playpen contained a total of 117,773 posts, 10,622 total topics and 214,898 total members. (*Id.*, Ex. 2 ¶ 12.)

A.

Playpen operated on and was only accessible through Tor. (*Id.*, Ex. 1 ¶ 7.) Unlike a public website, a user could not reach Playpen through a traditional web search engine, such as Google. (*Id.*, Ex. 1 ¶ 10.) Rather, he could only access the website by using Tor and inputting the "particular . . . combination of letters and numbers that" matched Playpen's specific Tor-based web address. (*Id.*, Ex. 1 ¶¶ 9–10; Hr'g Tr. 38:9–13, ECF No. 29.)

Although the United States Naval Research Laboratory initially designed and implemented Tor for the primary purpose of protecting government communications, it is now "free software, [ ] available worldwide" to the public. (Gov't's Opp., Ex. 1 ¶ 7; Hr'g Tr. 7:13–17.) In order to access the Tor network, a user must take affirmative steps to install the software on his computer by either downloading an add-on to his web browser or downloading the Tor software available on its website. (Gov't's Opp., Ex 1 ¶ 7.)

The use of Tor thwarts traditional IP identification and investigative techniques. (*Id.*, Ex. 2 ¶ 23.) Under those traditional methods, FBI agents can review IP address logs after they seize a website to determine which IP addresses visited the site. (*Id.*, Ex. 1 ¶ 22.) They can then conduct a publicly available search to determine which internet service providers ("ISPs") owned the target IP address and issue a subpoena to the ISP to ascertain the identity of the user. (*Id.*)

The Tor software masks a user's IP address by "bouncing their communications around a distributed network of relay computers run by volunteers all around the world." (*Id.*, Ex. 1 ¶ 8.) As a result, "traditional IP identification techniques are not viable" because the last computer or

"exit node" is not the IP address of the actual user who visits the website. (*Id.*; *id.*, Ex. 2 ¶ 23.) It is also impossible to trace the IP address back to the originating computer. (*Id.*, Ex. 2 ¶ 23.) The Tor network "operates similarly to a proxy server—that is, a computer through which communications are routed to obscure a user's true location." (*Id.*, Ex. 1 ¶ 8.)

Tor also allows websites, such as Playpen, to operate as a "hidden service." (*Id.*, Ex. 1 ¶ 9.) Tor masks the website server's IP address and replaces it with a Tor-based web address. (*Id.*) The Tor-based address is usually a series of algorithm-generated characters such as "asdlk8fs9dflku7f" followed by the suffix ".onion." (*Id.*) The user may obtain Playpen's specific address from other users or through a link posted on one of Tor's "hidden services" pages dedicated to child pornography and pedophilia. (*Id.*, Ex. 1 ¶ 10.)

B.

In December 2014, a foreign law enforcement agency informed the FBI that it suspected a United States-based IP address was associated with Playpen. (*Id.*, Ex. 1 ¶ 28.) The FBI confirmed through a publicly available search that the IP address was owned by Centrilogic, a server hosting company headquartered in Lenoir, North Carolina. (*Id.*) The FBI subsequently obtained a search warrant for the server. (*Id.*) FBI agents examined the server and determined that it contained a copy of Playpen. They then stored the copy of the website on a computer server at a government facility in Newington, Virginia. Newington is located in the Eastern District of Virginia. (*Id.*)

Additional investigation revealed that a resident of Naples, Florida had administrative control of Playpen and the computer server in Lenoir. (*Id.*) On February 19, 2015 FBI personnel executed a court-authorized search of the suspected administrator's residence in Naples. (*Id.*, Ex. 1 ¶ 30.) The FBI arrested the suspect and assumed administrative control of Playpen. (*Id.*)

On February 20, 2015, Agent Macfarlane applied to a United States Magistrate Judge in the Eastern District of Virginia for a warrant to use the NIT while the FBI assumed administrative control of Playpen on a copy of its server in Newington. (*See generally id.*, Ex. 1.)

Agent Macfarlane stated in the warrant application that the NIT was necessary to overcome the obstacles presented by Tor's masking capabilities. (*Id.*, Ex. 1 ¶ 31.) He stated that "other investigative procedures that are usually employed in criminal investigations of this type have been tried and failed or reasonably appear to be unlikely to succeed if they are tried." (*Id.*) The agent represented that the search would aid the FBI in its investigation by revealing "information that may assist in identifying the user's computer, its location, and the user of the computer." (*Id.*, Ex. 1 ¶ 34.) He explained in the warrant application that the NIT would "augment" the normal content that websites send to its visitors with "additional computer instructions." (*Id.*, Ex. 1 ¶ 33.) Specifically, those instructions "are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government," including the "activating" computer's actual IP address.[3] (*Id.*, Ex. 1 ¶ 33, Attach. B.) The NIT would deploy "each time that any user or administrator log[ged] into Playpen by entering a username and password." (*Id.*, Ex. 1 ¶ 36.) The FBI could then link a username and its corresponding activity on the site with an IP address. (*Id.*, Ex. 1 ¶ 37.)

Agent Macfarlane explained that the "NIT may 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." (*Id.*, Ex. 1 ¶ 46 (emphasis

[3] Other information gathered from the NIT included: (1) a unique identifier generated by the NIT to distinguish data from that particular computer; (2) the type of operating system running on the computer; (3) information about whether the NIT has already been delivered to the "activating" computer; (4) the "activating" computer's host name; (5) the "activating" computer's active operating system username; and (6) the "activating" computer's media access control ("MAC") address. (Gov't's Opp., Ex. 1 Attach. B.)

added).) In Attachment A to the warrant application, which identified the "place to be searched," Agent Macfarlane stated that the NIT would be "deployed on the computer server. . . . located at a government facility in the Eastern District of Virginia." (*Id.*, Ex. 1 Attach. A.) It stated that the NIT would seek information from the "activating computers," which "are those of any user or administrator who logs into [Playpen] by entering a username and password." (*Id.*) On February 20, 2015, the magistrate judge issued the search warrant. (*Id.*, Ex. 1.)

C.

While monitoring activity on Playpen after seizing a copy of the server, FBI agents observed someone with the username "thepervert" posting occasionally on the website's forums. (*Id.*, Ex. 2 ¶¶ 25–27.) The profile page indicated that "thepervert" created his profile on January 26, 2015 and had been actively logged into the website for 10 hours and 18 minutes between that date and March 1, 2015. (*Id.*, Ex. 2 ¶ 26.) During that time, "thepervert" made approximately six postings on Playpen which included, among other things, hyperlinks to forums on both Playpen and external websites containing child pornography. (*Id.*, Ex. 2 ¶ 27.)

On February 28, 2015, after the NIT had already been deployed, "thepervert" logged into Playpen by entering his username and password. (*Id.*, Ex. 2 ¶ 28.) That triggered certain information on his computer, including his IP address, to be transmitted to the government. (*Id.*) During that browsing session, "thepervert" accessed forums depicting child pornography. (*Id.*, Ex. 2 ¶ 29.)

Using publicly available websites, FBI agents were able to determine that Comcast Cable ("Comcast") operated the suspect's IP address. (*Id.*, Ex. 2 ¶ 30.) They served upon Comcast an administrative subpoena/summons requesting information related to the IP address associated

with "thepervert." (*Id.*, Ex. 2 ¶ 31.) According to the information received from Comcast, the IP address was assigned to Werdene. (*Id.*, Ex. 2 ¶¶ 31–33.)

On June 17, 2015, FBI agents sought and obtained from a Magistrate Judge in the United States District Court for the Eastern District of Pennsylvania a warrant to search Werdene's home in Bensalem for "evidence, contraband, [and] fruits/instrumentalities" of child pornography. (*Id.*) On that same day, FBI agents searched Werdene's home and obtained a laptop, a USB drive contained in a safe and one DVD, all containing child pornography. (Gov't's Opp. at 8.) Werdene lived alone and was not home at the time of the search. (*Id.*) FBI agents later interviewed him, where he admitted to using and downloading the material on his laptop. (*Id.*) Werdene was indicted on September 17, 2015. (*Id.*)

D.

On February 11, 2016 Werdene filed a motion to suppress all physical evidence seized from his home and "all fruits therefrom," including any inculpatory statements he made. (Def.'s Mot. to Suppress at *1, ECF No. 19.) He argues that the government "knowingly circumvented" Federal Rule of Criminal Procedure 41, which "limits the authority of a magistrate judge to issue a warrant and "serves as a bulwark against the very type of sweeping dragnet searches and unrestrained government surveillance that occurred in this case." (Def.'s Mem. in Supp. of Mot. to Suppress ("Def.'s Mem.") at 9, ECF No. 19.) He argues that the violation of Rule 41 is "of constitutional magnitude" and the evidence seized pursuant to the NIT should be suppressed. (*Id.* at 15–16.) He further argues that even if the Court does not find a constitutional violation, suppression is warranted because he was prejudiced by the government's violation of the Rule. (*Id.* at 16–17.) Werdene also contends that the FBI acted with intentional and deliberate

disregard of Rule 41 because they misled the magistrate judge "with respect to the true location of the activating computers to be searched." (*Id.* at 17.)

The Government argues that "[t]he fact that Rule 41 does not explicitly authorize some procedure does not mean that those procedures are unlawful." (Gov't's Opp. at 17.) It argues that under these circumstances, Werdene's use of Tor made it impossible for FBI agents to comply with the requirements of Rule 41 because he "made sure that his location could not be found." (*Id.* at 18.) The Government further states that even if there was a violation of Rule 41, suppression is not the appropriate remedy because it was not of constitutional magnitude and there is no evidence that the FBI agents engaged in any conduct warranting application of the exclusionary rule. (*Id.* at 20–26.) The Court held a hearing on the motion on April 7, 2016. (ECF No. 27.)

E.

A number of federal courts have recently issued opinions in cases arising from the same NIT application and warrant issued in this case. *See United States v. Levin*, 15-cr-10271, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Arterbury*, 15-cr-182 (N.D. Okla. Apr. 25, 2016) (report and recommendation); *United States v. Epich*, 15-cr-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Stamper*, No. 15-cr-109 (S.D. Ohio Feb. 19, 2016); *United States v. Michaud*, 15-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). Similar to Werdene, the defendants in those cases lived outside of the Eastern District of Virginia and sought to suppress the evidence against them because of the Government's alleged violations of Rule 41.[4]

[4] The issue that the court addressed in *Stamper* was not suppression for violation of Rule 41, but instead suppression for violation of the Fourth Amendment.

Although the courts generally agree that the magistrate judge in Virginia lacked authority under Rule 41 to issue the warrant, they do not all agree that suppression is required or even appropriate. *Compare Michaud*, 2016 WL 337263, at *6–7 (finding violation of Rule 41(b) but suppression unwarranted because defendant was not prejudiced and FBI agents acted in good faith), *and Epich*, 2016 WL 953269, at *2 (rejecting Defendant's contention that Rule 41 was violated and finding suppression unwarranted even if it was), *with Levin*, 2016 WL 2596010, at *7–15 (finding suppression warranted because Rule 41 "implicates substantive judicial authority," Defendant was prejudiced even if the violation was technical, and the good faith exception to the exclusionary rule is not available because the warrant was void *ab initio*), *and Arterbury*, slip op. at 13–29 (same).

II.

Rule 41(b) describes five scenarios in which a magistrate judge has authority to issue a warrant. Subsection (b)(1) states the general rule that "a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district." FED. R. CRIM. P. 41(b)(1). The following four subsections provide that that a magistrate judge has authority to issue a warrant: (2) "if the person or property is located within the district but might move or be moved outside the district before the warrant is executed;" (3) if the magistrate judge sits in a district in which activities related to terrorism have occurred; (4) to install a tracking device within the district, though the magistrate judge may authorize the continued use of the device if the person or object subsequently moves or is moved outside of the district; and (5) where the criminal activities occur in the District of Columbia, any United States territory, or on any land or within any building outside of the country owned by the United States or used by a United States diplomat. FED. R. CRIM. P. 41(b)(2)–(5).

Werdene argues that the NIT warrant "is not authorized under any of these sections, and, therefore, plainly unlawful." (Def.'s Mem. at 11.) He contends that in this case the "actual 'place to be searched' was not the server, but the 'activating computers' that would be forced to send data to that server." (*Id.* at 13.) Accordingly, he contends that since his computer was located in Bensalem, outside the magistrate judge's jurisdiction in the Eastern District of Virginia, the magistrate judge did not have authority to issue the warrant under any of Rule 41(b)'s five subsections.

During the hearing, Werdene's counsel introduced as the lone defense exhibit a December 22, 2014 letter from United States Deputy Assistant Attorney General David Bitkower to Judge Reena Raggi, Chair of the Advisory Committee on Criminal Rules, regarding "Response to Comments Concerning Proposed Amendment to Rule 41."[5] (Def.'s Ex. 1.) The letter addresses various issues related to proposed amendments to Rule 41, including concerns regarding the Fourth Amendment's particularity and notice requirements, Title III wiretap orders, "remote search techniques" and, relevant to this case, new standards for obtaining a warrant "in cases involving Internet anonymizing technology." (Def.'s Ex. at 1–2.)

In a section titled "Concealed through technological means," the letter states that "[u]nder the proposed amendment, a magistrate judge in a district where activities related to a crime may have occurred will have authority to issue a warrant for a remote search if the location of the computer to be searched 'has been concealed through technological means.'" (*Id.* at 10.) Counsel for Werdene contends the letter is evidence of a Rule 41 violation in her client's case because "the law has not caught up with technology" and the evidence should be suppressed because "a violation is . . . a violation." (Hr'g Tr. 17:15, 18:8–9.) The Court need not address whether or not law enforcement has to cease its investigative efforts while the process to amend

[5] Judge Raggi sits on the United States Court of Appeals for the Second Circuit.

the Federal Rules of Criminal Procedure plays out. As explained *infra*, a violation of Rule 41 does not end the inquiry. The facts of this case compel the conclusion that suppression is unwarranted.

The Government does not contend that the NIT warrant falls within any specific subsection of Rule 41. (Gov't's Opp. at 15–20.) It instead argues that Rule 41 is flexible, and the failure of Rule 41 to "authorize some procedure does not mean that those procedures are unlawful." (*Id.* at 17.) The Government highlights the predicament with which the FBI agents were faced: the Defendant's use of Tor made it impossible for agents to know in which district it should seek a warrant, and they accordingly "sought [the] warrant in the only logical district—the one in which they had the server on which they would install the NIT." (*Id.* at 16.)

"Rule 41(b) is to be applied flexibly, not rigidly." *Michaud*, 2016 WL 337263, at *5 (citing *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992)). Even a flexible application of the Rule, however, is insufficient to allow the Court to read into it powers possessed by the magistrate that are clearly not contemplated and do not fit into any of the five subsections. *See id.* at *6 ("In this case, even applying flexibility to Rule 41(b), the Court concludes that the NIT Warrant technically violates the letter, but not the spirit, of Rule 41(b).").

Subsection (b)(1) states that a magistrate judge may issue a warrant "to search for and seize a person or property located within the district." The Government does not attempt to argue here, as it has done in similar cases in other districts, that the NIT targeted property in the Eastern District of Virginia because the Defendant initiated contact with the server in that location when accessing the website. *See Levin*, 2016 WL 2596010, at *5 ("[S]ince Levin . . . 'retrieved the NIT from a server in the Eastern District of Virginia, and the NIT sent [Levin's] network information back to the server in that district,' the government argues that the search . . .

can be understood as occurring within the Eastern District of Virginia."); *Michaud*, 2016 WL 337263, at *6 ("[A] cogent, but ultimately unpersuasive argument can be made that the crimes were committed 'within' the location of Website A, [the] Eastern District of Virginia, rather than on [a] personal computer located in other places under circumstances where users may have deliberately concealed their locations."). Rather, the Government argues for a flexible application of the Rule because "as is often the case, Congress has not caught up with the changes in technology." (Hr'g Tr. at 51:1–2.)

That Congress has "not caught up" with technological advances does not change the fact that the target of the NIT in Werdene's case was located outside of the magistrate judge's district and beyond her jurisdiction under subsection (b)(1). The property to be seized pursuant to the NIT warrant was not the server located in Newington, Virginia, but the IP address and related material "[f]rom any 'activating' computer" that accessed Playpen. (Gov't's Opp., Ex. 1 Attach. A.) Since that material was located outside of the Eastern District of Virginia, the magistrate judge did not have authority to issue the warrant under Rule 41(b)(1).

Subsections (b)(2)–(5) are also inapplicable to the NIT warrant: (b)(2) relates to a person or object located within the district at the time the warrant is issued but that the government has reason to believe might move or be moved outside the district; (b)(3) relates to terrorist activity; (b)(4) permits tracking devices to be installed on a person or property within the district; and (b)(5) allows the magistrate judge to issue a warrant when the activity occurs in certain territories outside of the district, none of which are applicable here. Subsections (b)(2) and (b)(4), the only provisions potentially applicable to this case, are both premised on the person or property being located within the district. It is uncontested that the computer information that the NIT targeted

was at all relevant times located beyond the boundaries of the Eastern District of Virginia. The magistrate judge was accordingly without authority to issue the NIT warrant under Rule 41.

III.

"There are two categories of Rule 41 violations: those involving constitutional violations, and all others." *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000) (citations omitted) (cited with approval in *United States v. Slaey*, 433 F. Supp. 2d 494, 498 (E.D. Pa. 2006) and *United States v. Sampson*, No. 07-cr-389, 2008 WL 919528, at *4 (M.D. Pa. Mar. 31, 2008)). Courts have described violations of Rule 41 as either: (1) "substantive" or "constitutional" violations; or (2) "ministerial" or "procedural" violations. *See United States v. Levin*, No. 15-cr-10271, 2016 WL 2596010, at *7 (D. Mass. May 5, 2016) (distinguishing between "substantive" and "procedural" violations of Rule 41); *see also United States v. Krueger*, 809 F.3d 1109, 1114 (10th Cir. 2015) (finding that the inquiry begins by determining whether the Rule 41 violation was of "constitutional import"); *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) (distinguishing between "substantive" and "procedural" violations of Rule 41); *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000) (distinguishing "constitutional" and "ministerial" violations of Rule 41).

A.

To demonstrate that the violation of Rule 41 was of constitutional magnitude, Werdene must show a violation of his Fourth Amendment rights. *See United States v. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988), *overruled on other grounds by United States v. Chapple*, 985 F.2d 729 (3d Cir. 1993). Specifically, he must articulate how the Government's failure to comply with Rule 41(b) caused a search or seizure prohibited by the Fourth Amendment. He cannot do so.

Werdene does not argue that the Government violated his Fourth Amendment rights by seeking a warrant without probable cause. (Hr'g Tr. 23:16–22.) Rather, as the Government asserts, his argument is that Agent Macfarlane applied for the NIT warrant in the wrong district. (Gov't's Opp. at 15.) Werdene contends rather circularly that the Government's "violation of Rule 41 is of constitutional magnitude because it did not involve mere ministerial violations of the rule." (Def.'s Mot. at 16 (citation omitted).) He argues that the Fourth Amendment protects his use of his computer inside the privacy of his own home and "[a]llowing the Government to ignore the limits imposed by the Rule will invite further violations and undermine the core constitutional requirement that warrants particularly describe the place or places to be searched." (*Id.* (citations omitted).)

The Supreme Court of the United States has "uniformly . . . held that 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 the government action." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (collecting cases). That inquiry is analyzed in two parts: (1) whether the individual, through his conduct, "exhibited an actual (subjective) expectation of privacy;" and (2) whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" *Id.* (citations omitted).

In *Smith*, the Supreme Court addressed whether petitioner Michael Lee Smith had a reasonable expectation of privacy in the telephone numbers he dialed. 442 U.S. at 738. The government had used a pen register to record the numbers dialed from Smith's home in order to determine if he made threatening phone calls to another individual. *Id.* at 737. The Court rejected Smith's argument that he had a "reasonable expectation of privacy" in the numbers that

he dialed and held that the use of the pen register was, in fact, not a search. *Id.* at 742. It reasoned that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone companies, since it is through telephone company switching equipment that their calls are completed." *Id.* It rejected Smith's argument that he attempted to keep the numbers he dialed private by dialing them from his home phone because such numbers were "convey[ed] . . . to the telephone company in precisely the same way" regardless of his location. *Id.* at 743. Further, it held that Smith's expectation of privacy was "not one that society is prepared to recognize as reasonable" because he voluntarily turned the information over to a third party, the telephone company. *Id.* at 743–44 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)) (internal quotation marks omitted).

The Third Circuit has similarly held that an individual has "no reasonable expectation of privacy in his IP address and so cannot establish a Fourth Amendment violation." *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (citations omitted). "[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including [internet service providers]." *Id.*; *see also In re Nickelodeon Consumer Privacy Litig.*, No. 12-cv-07829, 2014 WL 3012873, at *15 (D.N.J. July 2, 2014) ("Indeed, in the analogous Fourth Amendment context, email and IP addresses can be collected without a warrant because they constitute addressing information and do not necessarily reveal any more about the underlying contents of communications than do phone numbers, which can be warrantlessly captured via pen registers.") (citation and internal quotation marks omitted); *United States v. Forrester*, 512 F.3d 500, 509–10 (9th Cir. 2008) (comparing IP addresses to the outside of a letter and the monitoring of IP addresses to a pen register). The Third Circuit in *Christie* noted that "IP addresses are not merely passively conveyed through third party

equipment, but rather are voluntarily turned over in order to direct the third party's servers." 624 F.3d. at 574 (citations and internal quotation marks omitted).

Werdene had no reasonable expectation of privacy in his IP address. Aside from providing the address to Comcast, his internet service provider, a necessary aspect of Tor is the initial transmission of a user's IP address to a third-party: "in 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." *United States v. Farrell*, No. 15-cr-029, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016). The court in *Farrell* held that "[u]nder these circumstances Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network." *Id.*; *see also Michaud*, 2016 WL 337263, at *7 ("Although the IP addresses of users utilizing the Tor network may not be known to websites, like [Playpen], using the Tor network does not strip users of all anonymity, because users . . . must still send and receive information, including IP addresses, through another computer . . . .").[6]

That Werdene's IP address was subsequently bounced from node to node within the Tor network to mask his identity does not alter the analysis of whether he had an actual expectation of privacy in that IP address. In *Smith*, the petitioner argued that the numbers he dialed on his telephone remained private because they were processed through automatic switching equipment rather than a live operator. 442 U.S. at 745. The Court rejected that argument, finding that the

[6] In support of his argument, Werdene relies on *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). That case involved FBI agents seeking a warrant to install software on a computer whose location was not ascertainable. *Id.* at 755. The software could generate user records and take control of a computer's camera to generate photographs of the user. *Id*. The magistrate judge declined to issue the warrant because the jurisdictional requirements of Rule 41(b) were not met and because it violated the Fourth Amendment's particularity requirement and protections against intrusive video surveillance. *Id.* at 757–61. *In re Warrant* is distinguishable based on the intrusive and general nature of the information sought. Unlike the software in that case, the NIT targeted users who were accessing child pornography and revealed information in which they had no reasonable expectation of privacy.

telephone company's decision to use automatic equipment instead of a live operator did not "make any constitutional difference" in analyzing the petitioner's reasonable expectations of privacy. *Id.* Similarly, the type of third-party to which Werdene disclosed his IP address—whether a person or an "entry node" on the Tor network—does not affect the Court's evaluation of his reasonable expectation of privacy. He 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. *See Farrell*, 2016 WL 705197, at *2 ("[T]he Tor Project [communicates to users] that the Tor network has vulnerabilities and that users might not remain anonymous.").[7]

B.

Even if Werdene maintained a subjective expectation that his IP address would remain private through his use of Tor, that expectation is not "one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361. In *United States v. Stanley*, 753 F.3d 114 (3d Cir. 2014), Richard Stanley accessed his neighbor's wireless internet connection without permission to share child pornography. Police officers learned Stanley's IP address by analyzing the neighbor's router and located him by using a device known as a "MoocherHunter." *Id.* at 116. MoocherHunter is a mobile tracking software that is used with a directional antenna to locate a "mooching computer" by detecting the strength of the radio waves it is emitting. *Id.*

Stanley contended that the officers' use of MoocherHunter constituted a warrantless search and sought suppression of the evidence against him. *Id.* at 117. After the district court denied his motion, the Third Circuit affirmed, holding that the officers did not conduct a

[7] Werdene does not argue that he had a reasonable expectation of privacy in the other material gathered by the NIT, including the type of operating system running on the computer, his computer's active operating system username and his computer's MAC address. Nor does Werdene contend that any of that information was material to the investigation of his activities and his subsequent identification.

"search" within the meaning of the Fourth Amendment because Stanley did not have a reasonable expectation of privacy in his wireless internet signal. *Id.* at 119–22.

The Third Circuit reasoned that "while Stanley may have justifiably expected the path of his invisible radio waves to go undetected, society would not consider this expectation 'legitimate' given the unauthorized nature of his transmission." *Id.* at 120 (citing *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) ("[A] burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate.'")); *see also United States v. Jacobson*, 466 U.S. 109, 122 (1984) ("The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities."). Werdene's use of Tor to view and share child pornography is not only an activity that society rejects, but one that it seeks to sanction. *See, e.g.*, Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008, 42 U.S.C. §§ 17611, 17612 (authorizing the Attorney General to create a National Strategy for Child Exploitation Prevention and Interdiction and establishing a National Internet Crimes Against Children Task Force Program); *Stanley*, 753 F.3d at 121 (concluding that society would be unwilling to recognize Stanley's privacy interests as "reasonable" where "the purpose of [his] unauthorized connection was to share child pornography").

The Third Circuit further stated in *Stanley* that recognizing his expectation of privacy as "legitimate" would "reward him for establishing his Internet connection in such an unauthorized manner." 753 F.3d at 121. Here, Werdene seeks to "serendipitously receive Fourth Amendment protection" because he used Tor in an effort to evade detection, even though an individual who

does not conceal his IP address does not receive those same constitutional safeguards. *Id.* (citing *United States v. Broadhurst*, No. 11-cr-00121, 2012 WL 5985615, at *5 (D. Or. Nov. 28, 2012)). Since Werdene did not have a reasonable expectation of privacy in his IP address, the NIT cannot be considered a "search" within the meaning of the Fourth Amendment and the violation at issue is therefore not constitutional. *See Martinez-Zayaz*, 857 F.2d at 136.

IV.

Werdene is left to contend that suppression is warranted even if the Government's violation of Rule 41 was nonconstitutional, procedural or "ministerial." (Def.'s Mem. at 16–17.) He relies on the Tenth Circuit Court of Appeals's suppression standard in the context of a nonconstitutional Rule 41 violation. Specifically, in *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), the Tenth Circuit stated that it:

> consider[s] whether the defendant can establish that, as a result of the Rule violation (1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision of the Rule.

Id. at 1114.[8] Werdene claims he was prejudiced because the NIT "would not have occurred[] but for the Rule 41 violation." (Def.'s Mem. at 17.) He also contends that the Government "acted with intentional and deliberate disregard of Rule 41" as the Rule "simply does not permit remote, dragnet searches of computers outside of the authorizing district." (*Id.*)

[8] In *Krueger*, the Tenth Circuit adopted the Ninth Circuit's suppression standard for nonconstitutional violations of Rule 41 first articulated in *United States v. Stefanson*, 648 F.2d 1231, 1235 (9th Cir. 1981). Several other circuits also use the *Stefanson* test. *See, e.g.*, *United States v. Comstock*, 805 F.2d 1194, 1207 (5th Cir. 1986); *United States v. Loyd*, 721 F.2d 331, 333 (11th Cir. 1983); *United States v. Gitcho*, 601 F.2d 369, 372 (8th Cir. 1979), *cert. denied*, 444 U.S. 871 (1979); *United States v. Mendel*, 578 F.2d 668, 673–74 (7th Cir. 1978), *cert. denied*, 439 U.S. 964 (1978).

The Third Circuit defines prejudice differently than the Tenth Circuit.[9] In the Third Circuit, a nonconstitutional violation of Rule 41 warrants suppression when it "caused prejudice or was done with intentional and deliberate disregard of the rule's requirements." *United States v. Cox*, 553 F. App'x 123, 128 (3d Cir. 2014); *see also United States v. Slaey*, 433 F. Supp. 2d 494, 498 (E.D. Pa. 2006). Our Circuit defines prejudice "in the sense that it offends concepts of fundamental fairness or due process." *Hall*, 505 F.2d at 964; *see also United States v. Searp*, 586 F.2d 1117, 1125 (6th Cir. 1978) ("The Third Circuit has adopted a similar, but more restrictive 'prejudice' test, requiring suppression 'only when the defendant demonstrates prejudice from the Rule 41 violation . . . in the sense that it offends concepts of fundamental fairness or due process.'") (quoting *Hall*, 505 F.2d at 961); *United States v. Burka*, 700 F. Supp. 825, 830 (E.D. Pa. 1988) (articulating *Hall*'s prejudice standard). The Government's actions in this case do not offend notions of fundamental fairness or due process.

After assuming control of Playpen and moving its server to a government facility in Newington, Virginia, Agent Macfarlane sought and obtained a warrant to employ the NIT in the Eastern District of Virginia. (Gov't's Opp., Ex. 1 ¶¶ 28, 30.) Before activating the NIT, Agent Macfarlane did not—and could not—know that Werdene resided in the Eastern District of Pennsylvania. Indeed, the only way in which the Government could have procedurally complied with Rule 41 was either through sheer luck (*i.e.*, Werdene's location happened to be within the Eastern District of Virginia) or by applying for a warrant in every one of the ninety-four federal judicial districts. Agent Macfarlane's warrant application, which was approved by a neutral and

---

[9] The Government also argues that *Krueger*'s facts are distinguishable from this case. (Gov't's Opp. at 17.) In *Krueger*, Homeland Security Investigations ("HIS") agents sought and obtained a warrant from a magistrate judge in the District of Kansas to search properties in Oklahoma. *See United States v. Krueger*, 809 F.3d 1109, 1111 (10th Cir. 2015). There, it was clear in which district the HIS agents should have made their warrant request. Here, however, Werdene's use of Tor to mask his IP address obscured his location from FBI agents. Unlike *Krueger*, the FBI agents could not know Werdene's location prior to requesting the warrant.

detached magistrate judge, described the NIT process in copious detail. (*See generally* Gov't's Opp., Ex. 1.) The warrant application states that the NIT would deploy "each time that any user or administrator log[ged] into Playpen by entering a username and password." (*Id.*, Ex. 1 ¶ 36.) This enabled the FBI to link a username and its corresponding activity to an IP address. (*Id.*, Ex. 1 ¶ 37.) Agent Macfarlane specifically noted that the NIT could enable this process on users of Playpen "wherever located." (*Id.*, Ex. 1 ¶ 46.) The Government's nonconstitutional violation of Rule 41 does not offend concepts of fundamental fairness or due process and Werdene's motion to suppress cannot be granted on prejudice grounds. *See United States v. McMillion*, No. 08-cr-0205, 2011 WL 9110, at *4 (M.D. Pa. Jan. 3, 2011), *aff'd*, 472 F. App'x 138 (3d Cir. 2012).

B.

Werdene also contends that the Government acted with intentional and deliberate disregard of Rule 41 because the FBI misled the magistrate judge "with respect to the true location of the activating computers to be searched." (Def.'s Mem. at 17.) Werdene claims that this was "egregious[] because it is a deliberate flaunting of the Rule[.]" (Hr'g Tr. 33:2–3.) A review of the record, and specifically Agent Macfarlane's warrant application, shows no deception on the Government's part. The warrant request was candid about the challenge that the Tor network poses, specifically its ability to mask a user's physical location. (Gov't's Opp., Ex. 1 ¶¶ 28, 30.) Agent Macfarlane stated that the NIT would be deployed "each time" that "any user" logged into Playpen "wherever" they were "located." (*Id.*, Ex. 1 ¶ 46.) As discussed *infra*,

Section V.D., the Government did not mislead the magistrate judge but was instead up front about the NIT's method and scope.[10]

V.

Even if Werdene had a reasonable expectation of privacy in the information obtained by the NIT—rendering the Rule 41(b) violation constitutional in nature—suppression is not the appropriate remedy.

A.

When the Government seeks to admit evidence collected pursuant to an illegal search or seizure, the exclusionary rule operates to suppress that evidence and makes it unavailable at trial. *See United States v. Katzin*, 769 F.3d 163, 169 (3d Cir. 2014) (en banc), *cert. denied*, 135 S. Ct. 1448 (2015) (citing *Herring v. United States*, 555 U.S. 135, 139 (2009)). The exclusionary rule was developed "[t]o deter Fourth Amendment violations." *Id.*

Whether suppression is appropriate under the exclusionary rule is a separate question from whether a defendant's Fourth Amendment rights were violated. *See Hudson v. Michigan*, 547 U.S. 586, 591–92 (2006); *accord Herring*, 555 U.S. at 140. Exclusion is not a personal right conferred by the Constitution and was not "designed to 'redress the injury' occasioned by an unconstitutional search." *Davis v. United States*, 564 U.S. 229, 236 (2011) (quoting *Stone v. Powell*, 428 U.S. 465, 486 (1976)). Rather, the exclusionary rule is "a judicially created means of effectuating the rights secured by the Fourth Amendment." *Stone*, 428 U.S. at 482. The fact that a Fourth Amendment violation occurs does not mean that the evidence is automatically

---

[10] Werdene also argues that the Government violated Rule 41's notice requirement. (Def.'s Mem. at 18–20.) A careful reading of Agent Macfarlane's warrant application, however, shows that he requested the delay of any notice for up to 30 days under Rule 41(f)(3) and 18 U.S.C. § 3103(a)(b)(1) and (3) to avoid any tampering with Playpen while the investigation was ongoing. (Gov't's Opp., Ex. 1 ¶¶ 38–41.) He also noted that due to the anonymity of Playpen's users, "the investigation has not yet identified an appropriate person to whom such notice can be given." (*Id.*, Ex. 1 ¶ 40.) Regardless, even if the notice requirement was violated, suppression is not an appropriate remedy because he was not prejudiced by the violation. *See supra* Section IV.A.

suppressed. *See Katzin*, 769 F.3d at 170 (citing *Herring*, 555 U.S. at 140). Indeed, "exclusion 'has always been our last resort, not our first impulse.'" *Herring*, 555 U.S. at 140 (quoting *Hudson*, 547 U.S. at 591).

Application of the rule is instead "limited to those 'unusual cases' in which it may achieve its objective: to appreciably deter governmental violations of the Fourth Amendment." *Katzin*, 769 F.3d at 170 (quoting *Leon*, 468 U.S. at 909). "Real deterrent value" alone, however, is insufficient for the exclusionary rule to apply. *Id.* at 171 (quoting *Davis*, 564 U.S. at 237). The deterrent value must also outweigh the "substantial social costs" of exclusion. *Leon*, 468 U.S. at 907. Such costs "often include omitting 'reliable, trustworthy evidence' of a defendant's guilt, thereby 'suppress[ing] the truth and set[ting] [a] criminal loose in the community without punishment.'" *Katzin*, 769 F.3d at 171 (quoting *Davis*, 564 U.S. at 237). Because this result runs contrary to the truth-finding functions of judge and jury, "exclusion is a bitter pill, swallowed only as a last resort." *Id*. (citations and internal quotation marks omitted). Accordingly, exclusion is warranted "where the deterrent value of suppression . . . overcome[s] the resulting social costs." *Id*. (citing *Davis*, 564 U.S. at 237).

The good faith exception to the exclusionary rule "was developed to effectuate this balance and has been applied 'across a range of cases.'" *Id*. (quoting *Davis*, 564 U.S. at 238). *Leon* and its progeny highlight that "the deterrence benefits of exclusion 'var[y] with the culpability of the law enforcement conduct' at issue." *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 143). The deterrent value of suppression tends to outweigh the costs "[w]here officers exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights." *Id*. (quoting *Herring*, 555 U.S. at 144). When the police act with an "objectively reasonable good-faith belief" in the legality of their conduct, or when their conduct "involves

only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way." *Id*. (citations and internal quotation marks omitted). Accordingly, discerning "whether the good faith exception applies requires courts to answer the 'objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances.'" *Katzin*, 769 F.3d at 171 (quoting *Herring*, 555 U.S. at 145).

B.

Werdene relies on *United States v. Levin*, No. 15-cr-10271, 2016 WL 2596010 (D. Mass. May 5, 2016). In that case, the United States District Court for the District of Massachusetts addressed whether the NIT was a substantive or procedural violation of Rule 41 and whether the information obtained from the NIT should be suppressed. The court held, in relevant part, that: (1) the NIT warrant constituted a "substantive" or constitutional violation of Rule 41(b) in that it infringed on the defendant's Fourth Amendment rights; and (2) that the good faith exception was not available in this context, *i.e.*, where a magistrate judge issued a warrant without proper jurisdiction. *Id.*

In finding that the NIT warrant was a substantive violation of Rule 41(b), the *Levin* court reasoned that "the violation here involved 'substantive judicial authority' rather than simply 'the procedures for obtaining and issuing warrants.'" *Id*. at *8 (quoting *Krueger*, 809 F.3d at 1115). The court "assume[d] that [the defendant] had a reasonable expectation of privacy as to the information obtained through the execution of the various warrants." *Id*. at *1 n.1. The court in *Levin* held that because Rule 41(b) "did not grant [the magistrate] authority to issue the NIT warrant . . . [she] was without jurisdiction to do so." *Id*. at *8.

The court went further, concluding that this jurisdictional flaw rendered the warrant "void *ab initio*." *Id.* (citing, *inter alia*, *United States v. Master*, 614 F.3d 236, 241 (6th Cir. 2010)). It then stated that a warrant "void *ab initio*" was equivalent to "no warrant at all." *Id.* at *12. The court likened this situation to a "warrantless search" scenario which is "presumptively unreasonable" under the Fourth Amendment, and accordingly found a "substantive" or constitutional violation of Rule 41(b). *Id.* at *12 (citing *United States v. Curzi*, 867 F.2d 36 (1st Cir. 1989)).

The court also held that the good faith exception was not available in cases where a warrant was void *ab initio* and, therefore granted the motion to suppress. *Id.* at *10–13. In doing so, it relied on the Sixth Circuit Court of Appeals's decision in *United States v. Scott*, 260 F.3d 512 (6th Cir. 2001). The *Levin* court stated that while "the Supreme Court has expanded the good-faith exception to contexts beyond those *Leon* specifically addressed," none of those cases "involved a warrant that was void *ab initio*, and therefore none direct the conclusion that the good-faith exception ought apply to this case." *Levin*, 2016 WL 2596010, at *11.

C.

Levin's reliance on *Scott* was misplaced, particularly given the court's acknowledgement that "the Sixth Circuit effectively reversed [*Scott*]" in *United States v. Master*, 614 F.3d 236 (6th Cir. 2010).[11] *Id.* at *11; *see also United States v. Beals*, 698 F.3d 248, 265 (6th Cir. 2012) (recognizing that *Master* overruled *Scott*). In *Master*, the Sixth Circuit reexamined its holding in

[11] *Levin* later noted that "[e]ven in *Master* . . . the court acknowledged that the recent Supreme Court cases addressing the good-faith exception 'do [ ] not directly overrule our previous decision in *Scott*.'" *Levin*, 2016 WL 2596010, at *12 (citing *Master*, 614 F.3d at 243). It is therefore unclear whether or not *Levin* believed *Scott* was overruled. In any event, *Master* provided that "nothing in this opinion should cast doubt on the ultimate outcome in *Scott*. In that case, the officers made at best minimal attempts to find available, active magistrates before presenting the warrant to the retired judge." *Master*, 614 F.3d at 242 n.3. Thus, *Master* simply noted that the officers' actions in *Scott*, analyzed under the newly adopted good faith framework, fell below the standard necessary to apply the good faith exception to the exclusionary rule. To the extent *Levin* seeks to rely on *Master*'s footnote for the proposition that the good faith exception is inapplicable in this context, such a finding was clearly rejected by *Master*.

Scott—that the good faith exception could never apply where a warrant was void *ab initio*—in light of the Supreme Court's decisions in *Herring* and *Hudson*. 614 F.3d at 242–43. *Master* found *Herring*'s separation of the suppression and Fourth Amendment violation inquiries to be "contrary to a foundational assumption of the opinion in *Scott* that: 'Subject to a few exceptions, the exclusionary rule requires the suppression of evidence obtained in violation of the Fourth Amendment.'" *Id.* at 242 (quoting *Scott*, 260 F.3d at 514). The court stated:

> Whereas *Scott* effectively required the government to qualify for an exception to the general rule of suppression, the Supreme Court has since emphasized that the decision to exclude evidence is divorced from whether a Fourth Amendment violation occurred. The exclusionary rule's purpose is instead to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.

Id. (citations and internal quotation marks omitted). The Sixth Circuit accordingly found that the good faith exception *could* apply in situations where the warrant was void *ab initio*. *See id*. at 242–43.

Rather than rely on *Master*, the court in *Levin* instead deferred to *Scott*, stating that "[t]he *Master* court read the Supreme Court's recent good-faith cases too broadly." *Levin*, 2016 WL 2596010, at *12. The court explained its reasoning in a footnote, stating that while *Herring* "makes much of the connection between the exclusionary rule and the goal of deterrence and culpability of law enforcement . . . it says nothing about whether the same calculus ought apply where there was never jurisdiction to issue a valid warrant in the first place." *Id*. at *12 n.22. *Levin* apparently discounted *Master*'s reliance on *Herring* because *Herring* did not hold that the good faith exception applies where a warrant was void *ab initio*, *i.e.*, it never dealt with an issue that *Levin* admits was one of "first impression in this Circuit, and an unresolved question more broadly." *Id*. at *10. *But see United States v. Knights*, 534 U.S. 112, 117 (2001) (criticizing as "dubious logic" the argument "that an opinion upholding the constitutionality of a particular

search implicitly holds unconstitutional any search that is not like it"); *Arizona v. Evans*, 514 U.S. 1, 13 (1995) ("Subsequent case law has rejected [a] reflexive application of the exclusionary rule.") (citation omitted).

The Third Circuit has emphasized that courts "must be prepared to apply th[e] good-faith exception across a range of cases." *Katzin*, 769 F.3d at 178 (quoting *Davis*, 564 U.S. at 238) (internal quotation marks omitted). Indeed, the court in *Katzin* found that the good faith exception applied in the context of a warrantless search where the officers "acted . . . upon an objectively reasonable good faith belief in the legality of their conduct." *Id*. at 182. Moreover, it explicitly rejected the appellees' argument that it would be "fabricat[ing] a new good faith ground," stating that while "[t]he factual circumstances before us differ, [] we ground our application of the good faith exception in the same time-tested considerations." *Id*. at 178 n.11. In other words, the legal status of the warrant under the Fourth Amendment does not inform the decision of whether the good faith exception is available in a given case; that inquiry is separate and must be considered in light of the exclusionary rule's purpose and the officers' conduct at issue. *See Master*, 614 F.3d at 243.

Additionally, as *Master* indicates, "the exclusionary rule was crafted to curb police rather than judicial misconduct." *Id*. at 242 (citation omitted). Arguably, the magistrate judge's lack of authority to issue the warrant has no impact on police misconduct. *See id*. Applying the rule here without exception makes little sense where it was the magistrate, not the agents, who determined that she had jurisdiction. *See, e.g.*, *Emp'rs Ins. of Wausau v. Crown Cork & Seal Co.*, 905 F.2d 42, 45 (3d Cir. 1990) ("A federal court is bound to consider its own jurisdiction preliminary to consideration of the merits.") (quoting *Trent Realty Assocs. v. First Fed. Sav. & Loan Ass'n of Phila.*, 657 F.2d 29, 36 (3d Cir. 1981)); *In re Warrant to Search a Target*

Computer at Premises Unknown, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (declining to issue a warrant under Rule 41(b) because, *inter alia*, the court lacked jurisdiction). The good faith exception is not foreclosed in the context of a warrant that is void *ab initio* and the Court must now determine if it applies.

D.

The question is whether "the agents acted with a good faith belief in the lawfulness of their conduct that was 'objectively reasonable.'" *Katzin*, 769 F.3d at 182 (quoting *Davis*, 564 U.S. at 238). The Court must consider all of the circumstances and confine its inquiry to the "objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of that constellation of circumstances." *Katzin*, 769 F.3d at 182 (quoting *Leon*, 468 U.S. at 922 n.23) (internal quotation marks omitted).

The agents in this case acted upon an objectively reasonable good faith belief in the legality of their conduct. Attachment A to the warrant application is titled "Place to be Searched" and specifically authorizes deployment of the NIT to "activating computers." (Gov't Opp., Ex. 1 Attach A.) "Activating computers" are defined as "those of any user or administrator who logs into [Playpen] by entering a username and password." (*Id*.) Attachment A notes that the Eastern District of Virginia is where the NIT will be deployed. (*Id*.) Thus, an "objectively reasonable" reading of the warrant gave the agents "authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia." *United States v. Michaud*, No. 15-cr-05351, 2016 WL 337263, at *4 (W.D. Wash. Jan. 28, 2016).

Werdene claims that the Government acted with intentional and deliberate disregard of Rule 41 because the FBI misled the magistrate judge "with respect to the true location of the activating computers to be searched." (Def.'s Mem. at 17.) This argument is belied by both the warrant and warrant application. Agent Macfarlane stated in the warrant application that the "NIT may 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." (Gov't Opp., Ex. 1 ¶ 46 (emphasis added).) With this information, the magistrate judge believed that she had jurisdiction to issue the NIT warrant. Contrary to Werdene's assertion, this is not a case where the agents "hid the ball" from the magistrate or misrepresented how the search would be conducted. *See, e.g.*, *Illinois v. Gates*, 462 U.S. 213, 264 (1983) ("Similarly, the good-faith exception would not apply if the material presented to the magistrate or judge is false or misleading.") (citing *Franks v. Delaware*, 438 U.S. 154 (1978)).

While the *Levin* court found the good faith exception foreclosed in this scenario, it alternatively held that if the exception did apply, suppression was nonetheless appropriate. *See Levin*, 2016 WL 2596010, at *13. The court reasoned that "it was not objectively reasonable for law enforcement—particularly a veteran FBI agent with 19 years of federal law enforcement experience—to believe that the NIT Warrant was properly issued considering the plain mandate of Rule 41(b)." *Id*. (citations and internal quotation marks omitted). Noting that "the conduct at issue here can be described as systemic error or reckless disregard of constitutional requirements," the court found suppression appropriate. *Id*. (citations and internal quotation marks omitted).

The court in *Levin* did not analyze the "costs" associated with suppression. The Supreme Court has stated that these costs are "substantial," *Leon*, 468 U.S. at 907, given that suppression "often excludes 'reliable, trustworthy evidence' of a defendant's guilt, 'suppress[es] the truth and set[s] [a] criminal loose in the community without punishment.'" *Katzin*, 769 F.3d at 186 (quoting *Davis*, 564 U.S. at 237). The court in *Levin* also did not address what deterrent effect, if any, suppression would have in this case. While the court found that the agents' conduct constituted "systemic error or [a] reckless disregard of constitutional requirements," it failed to address why that is the case. *Levin*, 2010 WL 2596010, at *13. *Levin* seemed to overlook the Supreme Court's directive that "the exclusionary rule is not an individual right and applies only where it result[s] in appreciable deterrence." *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 909).

Further, to the extent a mistake was made in this case, it was not made by the agents in "reckless . . . disregard for Fourth Amendment rights." *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 144). Rather, it was made by the magistrate when she mistakenly issued a warrant outside her jurisdiction. The agents consulted with federal attorneys before preparing the warrant application. (Gov't's Opp. at 24.) *See e.g.*, *Katzin*, 769 F.3d at 181 (stating that "[w]e have previously considered reliance on government attorneys in our good faith calculus and concluded that, based upon it in combination with other factors, '[a] reasonable officer would . . . have confidence in [a search's] validity'") (quoting *United States v. Tracey*, 597 F.3d 140, 153 (3d Cir. 2010)). They presented the magistrate judge with all relevant information to allow her to make a decision as to whether Rule 41(b) permitted her to issue the warrant. The FBI agents did not misrepresent how the search would be conducted or, most importantly, where it would be conducted.

A magistrate judge's mistaken belief that she had jurisdiction, absent any indicia of reckless conduct by the agents, does not warrant suppression. The Supreme Court has stated:

> To the extent . . . proponents of exclusion rely on its behavioral effects on judges and magistrates in these areas, their reliance is misplaced . . . . [T]here exists no evidence suggesting that judges and magistrates are inclined to ignore or subvert the Fourth Amendment or that lawlessness among these actors requires application of the extreme sanction of exclusion . . . . And, to the extent that the rule is thought to operate as a "systemic" deterrent on a wider audience, it clearly can have no such effect on individuals empowered to issue search warrants. Judges and magistrates are not adjuncts to the law enforcement team; as neutral judicial officers, they have no stake in the outcome of particular criminal prosecutions. The threat of exclusion thus cannot be expected significantly to deter them.

Leon, 468 U.S. at 916–17. Exclusion of the evidence in this case would only serve to "punish the errors of judges and magistrates" and would not have any "appreciable" effect on law enforcement. *Id.* at 909, 916.

Had the agents lied to the magistrate and told her that all the information being sought would be gathered only in the Eastern District of Virginia, the Court's analysis would likely change because suppression deters misrepresentations made to the Court. *See, e.g.*, *Franks*, 438 U.S. at 171 (finding exclusion appropriate where there is proof of "deliberate falsehood or of reckless disregard for the truth"). In this case, however, the agents provided the magistrate with all the information she needed to "satisfy [herself] of [her] jurisdiction before proceeding . . . ." *Packard v. Provident Nat'l Bank*, 994 F.2d 1039, 1049 (3d Cir. 1993) (citations omitted). Once the warrant was issued, albeit outside the technical bounds of Rule 41(b), the agents acted upon an objectively reasonable good faith belief in the legality of their conduct. *Cf. Leon*, 468 U.S. at 921 ("In the ordinary case, an officer cannot be expected to question the magistrate's . . . judgment that the form of the warrant is technically sufficient . . . . Penalizing the officer for the

magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations.").

Here, as in *Katzin*, "the Government's evidence against [the defendant] is substantial, and it is uncontested that the Government would have no case without it." *Katzin*, 769 F.3d at 186. The "cost" of suppression, therefore, would be letting a "guilty and possibly dangerous defendant[] go free—something that 'offends basic concepts of the criminal justice system.'" *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 908). Absent any appreciable deterrent effect on law enforcement, suppression would only serve to "exact[] a heavy toll on both the judicial system and society at large." *Davis*, 564 U.S. at 237.

An appropriate order follows.

BY THE COURT:

/s/ Gerald J. Pappert
GERALD J. PAPPERT, J.