IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

MITCHELL JOHNSON,

Defendant.

REPORT AND RECOMMENDATION

16-cr-76-wmc

On August 24, 2016, a grand jury in this district returned a one-count indictment charging defendant Mitchell Johnson with possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). *See* dkt. 1. Johnson is one of many defendants across the country who was caught in the FBI's sting of a internet child pornography website called Playpen. *See, e.g.*.,https://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346.

The FBI's investigation began in early 2015 when the bureau received a lead from a foreign law enforcement agency about a child pornography site named "Playpen." Playpen was ensconced in the internet's "dark web" and was accessible only through the anonymous Tor network. Subsequently, the FBI seized control of a computer server hosting the site. Rather than shut down Playpen immediately, the FBI continued to operate it for two weeks in order to identify users of the site. Toward this end, on February 20, 2015, the agency sought and obtained from a magistrate judge in the United States District Court for the Eastern District of Virginia a warrant that authorized the FBI to deploy a Network Investigative Technique (NIT) on the server for a limited time period. The NIT caused computers that logged into Playpen to

reveal their concealed Internet Protocol (IP) addresses, which would allow the FBI to discover the residences where these computers were located.

Among the IP addresses identified as having logged into Playpen was one associated with Mitchell Johnson's residence in this judicial district. On August 14, 2015, the government obtained a search warrant for Johnson's home that targeted the computers located on the premises. Dkt. 20-2. Execution of this warrant led to discovery of the child pornography images charged against Johnson in this prosecution.

Johnson has moved to suppress the evidence derived from information obtained from execution of the NIT warrant. Dkt. 17. Johnson contends that the NIT warrant is invalid for five reasons: (1) it was not supported by probable cause; (2) it issued only after the FBI intentionally and recklessly misled the issuing court; (3) it is an impermissible general warrant; (4) it was contingent on a "triggering event" that did not occur; and (5) it was void *ab initio*, because the magistrate judge did not have authority to issue it. These challenges to the NIT warrant already have been presented to and considered by other federal courts in Playpen prosecutions across the country; most courts have rejected them and declined to suppress evidence.[1]

---

[1] For a sampling of cases, *see United States v. Allain*, No. 15-CR-10251, 2016 WL 5660452, at **4-7 (D. Mass. Sept. 29, 2016) (NIT search warrant supported by probable cause); *United States v. Anzalone*, 15-CR-10347, 2016 WL 5339723, at **6-7 (D. Mass. Sept. 22, 2016) (same); *United States v. Vortman*, No. 16-CR-210, 2016 WL 7324987, at **7-8 (N.D. Cal. Dec. 12, 2016) (same); *United States v. Owens*, No. 16-CR-38, 2016 WL 7079609, at **3-4 (E.D. Wisc. Dec. 5, 2016) (same); *United States v. Tippens*, No. 15-CR-387 (W.D. Wash. Nov. 30, 2016) (same); *United States v. McLamb*, No. 16-CR-92, 2016 WL 6963046, at **3-5 (E.D. Va. Nov. 28, 2016) (same); *United States v. Mascetti*, No. 16-CR-308 (M.D.N.C. Oct. 24, 2016) (same); *United States v. Matish*, No. 16-CR-16, 2016 WL 3545776, at **9-11 (E.D.Va. June 23, 2016) (same); *United States v. Tran*, No. 16-CR-10010, 2016 WL 7468005, at **6-7 (D. Mass. Dec. 28, 2016) (No substantial showing to justify *Franks* hearing); . *Owens*, 2016 WL 7079609, at **5-7 (E.D. Wis. Dec. 5, 2016); *Allain*, 2016 WL 5660452, at **7-8 (same); *Matish*, 2016 WL 3545776, at **5-7 (same); *United States v. Michaud*, No. 15-CR-05351, 2016 WL 337263, at **4-5 (W.D. Wash. Jan. 28, 2016) (NIT search warrant was not overbroad and did not lack particularity); *Vortman*, 2016 WL 7324987, at *9; (same); *Owens*, 2016 WL 7079609, at **7-8 (same); *Allain*, 2016 WL 5660452, at **8-9 (same); *Anzalone*, 2016 WL 5339723, at * 7 (finding

Johnson fares no better here. Having reviewed the opinions issued by other courts and having considered the parties' competing arguments for and against suppression in the instant case, I am recommending that this court should deny Johnson's motion to suppress. I agree with the courts that have found that the NIT warrant was supported by probable cause, was sufficiently particular and was not tainted by any false or misleading statements. As for Johnson's argument that the magistrate judge who issued the NIT warrant lacked authority to issue it, I find that even if the magistrate judge exceeded the authority granted by Fed. R. Crim. P. 41(b), suppression is not an appropriate remedy.

Johnson, by counsel, has submitted the affidavit for the NIT warrant. Def.'s Exh. B, NIT Warrant Application, dkt. 17-2. The affidavit speaks for itself, but I will summarize it for the reader's convenience:[2]

I. THE NIT WARRANT APPLICATION

The 31-page NIT search warrant affidavit was sworn to by Douglas Macfarlane, an FBI special agent with 19 years of federal law enforcement experience and particular training and experience investigating child pornography and the sexual exploitation of children. Def.'s Ex. B, dkt. 17-2, ¶1. The affidavit included: a three-page explanation of the offenses under investigation, ¶4; a seven-page section setting out definitions of technical terms used in the

---

that "[e]very court to consider this question has found the NIT search warrant sufficiently particular."); *Matish*, 2016 WL 3545776, at **13-14 (same); McLamb, 2016 WL 6963046, at *5 (triggering event that activated the search warrant occurred); *Mascetti*, No. 16-CR-308 (same); *Owens*, 2016 WL 7079609, at *8 (same); *Matish*, 2016 WL 3545776, at *15 (same); *Anzalone*, 2016 WL 5339723, at *8 (same).

[2] This summary is taken in large part (and sometimes verbatim) from the government's brief, dkt. 20.

affidavit, ¶5; and a three-page explanation of the Tor network, how it works, and how users could find a hidden service such as Playpen, which is identified in the warrant application as the "TARGET WEBSITE." ¶¶ 7-10.

According to paragraphs 7-10 of the affidavit, Playpen operated on the anonymous Tor network. Tor was created by the U.S. Naval Research Laboratory as a means of protecting government communications. It is now available to the public. Use of the Tor network masks the user's actual IP address, which could otherwise be used to identify a user. Tor does this by bouncing user communications around a network of relay computers run by volunteers. To access the Tor network, users must install Tor software either by downloading an add-on to their web browser or the free "Tor browser bundle," available at www.torproject.org. Users can also access Tor through "gateways" on the open internet that do not provide users with the full anonymizing benefits of Tor. When a Tor user visits a website within Tor, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address, and Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node. Accordingly, traditional IP-address-based identification techniques used by law enforcement on the open internet will fail on the Tor network.

Within the Tor network itself, certain websites, including Playpen, operate as "hidden services." Like other websites, they are hosted on computer servers that communicate through IP addresses. They operate the same as other public websites with one critical exception: the IP address for the server is hidden and is replaced with a Tor-based web address, which is a series of sixteen algorithm-generated characters followed by the suffix ".onion." A user can only reach a "hidden service" by using the Tor client and by operating in the Tor network. Unlike an open

internet website, it is not possible to use public lookups to determine the IP address of a computer hosting a "hidden service."

A "hidden service" on the Tor network does not reside on the traditional or "open" internet and can be accessed only through the Tor network. Even after connecting to the Tor network, users must know the exact web address of a "hidden service" in order to access it. As Agent Macfarlane explained:

> Even after connecting to 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 on 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 website's 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. [Playpen] is listed in that section.
>
> ¶10.

Thus, Macfarlane continued, "[a]ccessing [Playpen] . . . requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content." ¶10.

Between September 16, 2014 and February 3, 2015, FBI agents operating in the District of Maryland connected to the internet via the Tor Browser and were able to access Playpen and review its contents. ¶11. Statistics as of February 3, 2015 showed that the site—which was believed to have been in existence since August of 2014—contained 158,094 members, 9,333 message threads, and 95,148 posted messages. ¶11. By gaining access to the site, agents

determined that it "appeared to be a message board website whose primary purpose is the advertisement and distribution of child pornography." In paragraphs 11-30 of his affidavit, Agent Macfarlane described the features and content of the site that led to this conclusion.

It started with the site's main page, which Agent Macfarlane described as follows: "[O]n the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." ¶12. The following text appeared beneath those images: "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Agent Macfarlane explained that, based on his training and experience, the phrase "no cross-board reposts" referred to a "prohibition against material that is posted on other websites from being 're-posted'" to Playpen and that ".7z" referred to a "preferred method of compressing large files or sets of files for distribution." ¶12.

The affidavit also explained that users were required to register an account by creating a username and password before they could access the site. Users clicking on the "register an account" hyperlink on the main page were required to accept registration terms, the entire text of which was included in Agent Macfarlane's affidavit. ¶¶12-13. Playpen repeatedly warned prospective users to be vigilant about their security and the potential of being identified, explicitly stating, "the forum operators do NOT want you to enter a real [e-mail] address," users "should not post information [in their profile] that can be used to identify you," "it is impossible for the staff or the owners of this forum to confirm the true identity of users," "[t]his website is not able to see your IP," and "[f]or your own security when browsing or [*sic*] Tor we also recommend that you turn off javascript and disable sending of the 'referer' header." ¶13. Once a user accepted these terms and conditions, a user was required to enter a username, password, and e-mail address. ¶14. Upon successful registration, all of the sections, forums, and

sub-forums, along with the corresponding number of topics and posts in each, were observable. *Id*.

Paragraph 14 of the affidavit recited verbatim this table of contents. *Id*. Within the site's "Chan" forum were individual sub-forums for "jailbait" or "preteen" images of boys and girls. There were separate forums for "Jailbait videos" and "Jailbait Photos" featuring boys and girls. The "Pre-teen Videos" and "Pre-teen Photos" forums were each divided into four sub-forums by gender and content, with "hardcore" and "softcore" images/videos separately categorized for boys and girls.[3] A "Webcams" forum was divided into girls and boys sub-forums. The "Potpourri" forum contained sub-forums for incest and toddlers.

Reviewing the topics within these various forums, Agent Macfarlane determined that "the majority contained discussions, as well as numerous images that appeared to depict child pornography ('CP') and child erotica of prepubescent females, males, and toddlers." ¶18. Agent Macfarlane described examples of particular child pornography that were available to all registered users of Playpen, including images of prepubescent children being sexually abused by adults. ¶18. Agent Macfarlane stated that "[w]hile the entirety of [Playpen] is dedicated to child pornography," he then listed the site's sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." ¶27.

The affidavit further explained that Playpen contained a private messaging feature that allowed users to send messages directly to one another. The affidavit specified that "numerous"

[3]The words "hardcore" and "softcore" do not appear on the table of contents, but are abbreviated as "HC" and "SC." Agent Macfarlane averred that, based on his training and experience, he knows that "HC" means hardcore and "SC" means softcore. NIT Warrant Aff., n.5.

site posts referenced private messages related to child pornography and exploitation, including an example where one user wrote to another, "I can help if you are a teen boy and want to fuck your little sister, write me a private message." ¶21. Based on his training and experience and law enforcement's review of the site, Agent Macfarlane stated his belief that the site's private message function was being used to "communicate regarding the dissemination of child pornography." ¶22. He also noted that Playpen included multiple other features intended to facilitate the sharing of child pornography, including an image host, a file host, and a chat service. ¶¶23-25. All of those features allowed site users to upload, disseminate, and access child pornography. Agent Macfarlane stated that FBI agents had observed images of prepubescent child pornography disseminated by site users through each one of those features. *Id*. His verbal description of these images made clear that they constituted child pornography. *Id*.

The NIT warrant affidavit contained a detailed and specific explanation of the NIT, its necessity, how and where it would be deployed, what information it would collect, and why that information constituted evidence of a crime. Specifically, the affidavit noted that without the use of the NIT, "the identities of the administrators and users of [Playpen] would remain unknown" because any IP address logs of user activity on Playpen would consist only of Tor "exit nodes," which "cannot be used to locate and identify the administrators and users." ¶29. Further, because of the "unique nature of the Tor network and the method by which the network . . . route[s] communications through multiple other computers, . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed." ¶ 31. Agent Macfarlane determined that "using a NIT may help FBI agents locate the administrators and users" of Playpen. ¶¶ 31-32. Indeed, he explained, based on his training and experience and that of other officers and

forensic professionals, the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the actual location and identity" of Playpen users who were "engaging in the federal offenses enumerated" in the warrant. ¶31.

As for the how the NIT functioned, Agent Macfarlane explained that when a user's computer downloads site content in the normal course of operation, the NIT would augment that content with additional computer instructions. ¶33. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would cause a user's computer to transmit specified information to a government-controlled computer. *Id*. The discrete pieces of information to be collected were detailed in the NIT warrant and accompanying Attachment B, along with technical explanations of the terms. Specifically, the FBI wanted to collect: (1) the actual IP address assigned to the user's computer; (2) a unique identifier to distinguish the data from that collected from other computers; (3) the operating system running on the computer; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's Host Name; (6) the computer's active operating system username; and (7) the computer's Media Access Control (MAC) address. ¶ 34.

Agent Macfarlane explained why the information "may constitute evidence of the crimes under investigation, including information that may help to identify the . . . computer and its user." ¶35. For instance:

> the actual IP address of a computer that accesses [Playpen] can be associated with an ISP [*internet service provider*] and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the

> computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.
>
> ¶35.

The warrant affidavit specifically requested authority for the FBI to deploy the NIT each time any user logged into Playpen with a username and a password. ¶36. However, the affidavit disclosed to the magistrate judge that, "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation," the FBI might "deploy the NIT more discretely against particular users," including those who "attained a higher status" on the site or "in particular areas of [Playpen]" such as the sub-forums with the most egregious activity, which were described elsewhere in the affidavit. ¶32 n.8. Finally, the affidavit requested authority for the NIT to "cause an activating computer - wherever located - to send to a computer controlled by or known to the government . . . messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." ¶46(a).

As noted above, among the things described in the NIT warrant affidavit was Playpen's site logo: "on the main page of the site, located to either side of the site name, were two images depicting partially clothed prepubescent females with their legs spread apart." ¶12; *see also* dkt. 20-3, Govt. Ex. C (showing image of home page). Sometime before February 18, 2015, Playpen's administrator changed the URL (the site address). In his affidavit, Agent Macfarlane stated that he had accessed Playpen in an undercover capacity at its new URL on February 18, 2015 (two days before obtaining the warrant) and confirmed that the content had not changed. ¶11 n.3. This included the site logo.

On February 19, 2015, the FBI executed a search at the Florida home of the Playpen administrator and apprehended him. ¶30. At that point, the FBI also assumed control of Playpen. Postings by the administrator from earlier in the day show that a few hours before his arrest, the administrator changed Playpen's site logo, replacing the images described above with a single image showing a prepubescent girl, wearing a short dress and black stockings, reclined on a chair with her legs crossed and posed in a sexually suggestive manner. Dkt. 20-4, Govt. Ex. D (showing image of new home page). The text described in the affidavit as part of the logo, "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview," remained unchanged. *Compare* NIT Warrant Aff., ¶12 and Govt. Ex. C *with* Govt. Ex. D. The NIT warrant was sworn to and authorized at 11:45 a.m. on February 20, 2015, the day after the logo change. The affidavit did not reference this change.

II. ANALYSIS

A. The Warrant is Supported by Probable Cause

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." It further provides that "no Warrants shall issue, but upon probable cause." Probable cause is established when, based on the totality of the circumstances, the affidavit to the judge sets forth sufficient evidence to induce a reasonably prudent person to believe that a search will uncover evidence of a crime." *United States v. Scott*, 731 F.3d 659, 665 (7th Cir. 2013) (quotation omitted), cert. denied ___ U.S. ___, 134 S.Ct. 1806 (2014). "[P]robable cause is far short of certainty—it requires only a probability or substantial chance of criminal activity, not an actual showing of such activity, and not a probability that exceeds 50 percent (more likely than not), either." *United States v.*

Seiver, 692 F.3d 774, 777 (7th Cir. 2012) (quotation and citation omitted). *See also Gutierrez v. Kermon*, 722 F.3d 1003, 1008 (7th Cir. 2013)(probable cause is a practical, common sense standard that requires only the type of fair probability on which reasonable people act). A reviewing court owes "great deference" to the probable cause conclusion of the judge who issued the search warrant, and must uphold a finding of probable cause so long as the issuing judge had a substantial basis to conclude that the search was reasonably likely to uncover evidence of wrongdoing. *United States v. Reichling*, 781 F.3d 883, 886 (7th Cir.), cert. denied, ___ U.S. ___, 136 S. Ct. 174 (2015) (quotation and citations omitted).[4]

Because there was no particularized information in the warrant application about Playpen members, the application needed to establish probable cause to believe that every person who logged into Playpen was doing so for the purpose of viewing or distributing child pornography. This depended, in part, on establishing that Playpen was a child pornography site. Agent Macfarlane's affidavit clearly does this. Although Johnson makes a number of arguments suggesting that the site had innocent as well as illegal purposes, his arguments are unpersuasive. For example, he cites sections listed as "artwork" and "stories" and "general discussion" which he contends could refer to innocent, legal activities. Dkt. #17, at 10. However, Johnson fails to mention that the reference to "artwork" follows a listing for "toddlers," which follows a listing

[4] Although the government argues in conjunction with its Rule 41(b) argument that Johnson did not have a reasonable expectation of privacy in his IP address, it appears to concede that he had a reasonable expectation of privacy in the contents of his computer. Accordingly, the use of the NIT to execute that search constituted a search for Fourth Amendment purposes. *Accord United States v. Owens*, 2016 WL 7053195, *4-5 (E.D. Wis. Dec. 5, 2016) (use of NIT constituted Fourth Amendment search because defendant had reasonable expectation of privacy in contents of his computer); *United States v. Adams*, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016) ("The NIT searches the user's computer to discover the IP address associated with that device. Therefore, one's expectation of privacy in that device is the proper focus of the analysis, not one's expectation of privacy in the IP address residing in that device.").

for "Family Playpen – Incest," which follows several listings for webcams of "boys" and "girls," which follow several listings for "pre-teen photos" of "girls [hardcore]" and "boys [hardcore]." NIT Warrant Aff., ¶14. No reasonable judge reading the entirety of Agent Macfarlane's affidavit would conclude that Playpen was anything other than a website dedicated to the dissemination of child pornography.

Even so, contends Johnson, to establish probable cause that each person visiting Playpen was doing so knowing the site's illicit purpose and content, the warrant application had to establish that each visitor would be able to discern from the site's home page that Playpen was a child pornography forum. Johnson argues that Playpen's illegal purpose was not apparent from the home page (as it was described in the warrant application), and therefore there was no probable cause to support the NIT warrant.

In support of his argument, Johnson relies primarily on the First Circuit's decision in *United States v. Wilder*, 526 F.3d 1 (1st Cir. 2008). In *Wilder*, the First Circuit found probable cause to search the defendant's residence based in part on defendant's subscription to a pay-for-membership website called "Lust Gallery." The First Circuit found that "[t]he entrance page of the [Lust Gallery] website, as described, was plainly designed and written to attract persons interested in viewing child pornography." 526 F.3d at 6. As a result, "it was a fair inference from [defendant's] subscription to the Lust Gallery website . . . that downloading and preservation in his home of child pornography might very well follow." *Id*. The First Circuit noted that the preview page for the website showed naked female children identified as being under fourteen years old. *Id*. at 3. Furthermore, the preview page stated that "everyone understands there are reasons not to reveal everything right here." *Id*. Based on the appearance of the website, which "vividly indicated that child pornography was a featured product," as well

as the fact that Wilder had previously been convicted for possession of child pornography, the First Circuit upheld the finding of probable cause that Wilder had accessed child pornography and that it could be found at his home. *Id*. at 6–7.

Johnson contends that, compared to Lust Gallery, Playpen's home page was much more benign: Playpen's name was not overtly associated with child pornography, and there were no images, advertisements or representations made on the home page that clearly indicated that images of child pornography would be found on the site. Although Johnson concedes that Agent Macfarlane's description of the site logo as depicting "partially clothed prepubescent females with their legs spread apart," is accurate [5], he argues that this is not enough from which to infer that Playpen was a child pornography site. He notes further that the affidavit did not claim that the images of the young girls on the home page met the legal definition of "lascivious" pornography (*see* 18 U.S.C. § 2256(2)(1)) nor did the warrant application include a copy of the home page for the magistrate judge to review.

Johnson's arguments are unpersuasive. Lascivious or not, the Playpen site logo described in the warrant application clearly was suggestive of the content one would find upon visiting the site. More importantly, the logo was only one of several factors establishing that a person visiting the site probably intended to view or share child pornography. In addition to the images, the home page contained instructions associated with compressing large files for distribution and told users to encrypt file names and avoid "cross-board reposts." Further, the NIT did not deploy when a visitor merely landed on the home page, but only after he actually

[5] Elsewhere in his motion, Johnson contends that the description of Playpen's homepage was false. This contention will be addressed in the next section. For purposes of his probable cause challenge to the warrant, Johnson asserts that even assuming everything in the affidavit is accurate, it still failed to establish probable cause.

logged into the site, an act that required him first to enter a username and password. Even *before* doing that, the visitor would have to accept Playpen's registration terms, which told the prospective registrant that: Playpen's operators "do NOT want you to enter a real [e-mail] address"; that he "should not post information [in their profile] that can be used to identify you"; "it is impossible for the staff or the owners of this forum to confirm the true identity of users"; "[t]his website is not able to see your IP"; and "[f]or your own security when browsing or Tor we also recommend [*sic*] that you turn off javascript and disable sending of the 'referer' header." *Id*. at ¶13. It defies common sense for Johnson to suggest that a "casual visitor" landing on a site called "Playpen" that featured images of scantily clad young girls with their legs spread, that provided instructions referring to methods for compressing and encrypting files, and that imposed registration "terms" strongly suggesting the site was illicit, would nonetheless proceed to establish a user name and password without ever realizing that he was entering a child porn site.

But let's back up a step: the affidavit made clear that innocent web-surfers were unlikely ever to land on Playpen's home page in the first place. To access the site, a user first would have to install the Tor browser software to gain access to the "dark web," and then somehow locate the site, which was a "hidden service" on the Tor network. This second step would be difficult to accomplish unless the user knew right where to look. Although Johnson suggests that one can easily find "hidden services" on the Tor network merely by installing a search engine that operates much like Google does on the traditional internet, he offers nothing to support his assertion other than a link to a website that purports to offer such a tool.[6] Johnson's speculation

[6] Johnson refers to a Tor search engine called "ahmia.fi." As the government points out, "ahmia.fi" has a content-filtering policy that would remove pages containing child abuse (for which

is not enough to call into question Agent Macfarlane's statement in the warrant application that it would be "extremely unlikely that any user could simply stumble upon [Playpen] without understanding its purpose and content." I agree with the court in *United States v. Allain*, No. 15-CR-10251, 2016 WL 5660452, at *6 (D. Mass. Sept. 29, 2016), which found:

> Playpen was in fact a website devoted to child pornography, and the fact that users found it and then logged into it is indicative of criminal intent. While there may be legitimate reasons to use the Tor network other than masking illicit activity, the clandestine nature of the website and the challenges of finding it on the Tor Network suggests that those who logged into Playpen likely knew the purpose of the website and were entering it to access child pornography.

Considering all of the circumstances, the reviewing magistrate judge had ample evidence before her to conclude that deploying the NIT onto the computer "of any user or administrator who logs into [Playpen] by entering a username and password" was reasonably likely to uncover evidence of criminal conduct. The appearance and content of Playpen, its clandestine location on the Tor network and its registration terms sufficiently establish that users logging into the site likely knew the purpose and content of the site and were entering it for the purpose of viewing or sharing child pornography. Although it is hypothetically possible that some Playpen was visited by ingenuous registrants did not intend to access child pornography, this is improbable. In any event, probable cause does not demand certainty, only probability. *United States v. Funches*, 327 F.3d 582, 587 (7th Cir. 2003) ("the mere existence of innocent explanations does not necessarily negate probable cause"). That standard was easily met by the NIT warrant application.

Playpen would certainly qualify). See Welcome to the ahmia wiki! available at: https://github.com/juhanurmi/ahmia/wiki (last visited May 4, 2017).

B. A *Franks* Hearing Is Not Required

Johnson argues that Agent Macfarlane made material omissions or deliberate misstatements in his search warrant affidavit that unfairly skewed the probable cause analysis in favor of the government. Specifically, Johnson alleges that:

> 1) the agent misrepresented in Attachments A and B that the property to be searched was in the Eastern District of Virginia, when in fact the search had no geographic limitation, dkt. 23, at 3;
>
> 2) the agent stated in paragraph 27 of his affidavit that the "entirety" of Playpen was "dedicated to child pornography," when in fact he was aware that the site had a mix of legal and illegal content, *id*. at 4;
>
> 3) the agent did not accurately describe the site's logo on the home page as it appeared on the day he sought the warrant, dkt. 17, at 18;
>
> 4) the agent overstated how difficult it was to find the site on the Tor Network, dkt. 17, at 19; and
>
> 5) the agent improperly suggested that features such as image uploading capabilities and messaging service are indicative of criminality, dkt. 20.

According to Johnson, these errors and misstatements entitle him to an evidentiary hearing under *Franks v. Delaware*, 438 U.S. 154, 171 (1978). I disagree.[7]

There is a "presumption of validity with respect to the affidavit supporting the search warrant." *Franks*, 438 U.S. at 171. In *Franks*, the Supreme Court established the limited circumstances in which a defendant is entitled to an evidentiary hearing regarding the accuracy of a warrant application. The defendant must make a substantial preliminary showing that: (1)

[7] Upon a preliminary review of the briefs in regards to the *Franks* issue, I determined on February 15, 2017 that no hearing on Johnson's motion was necessary. This report supplements the reasoning I provided on the record at a telephonic hearing with the parties. See dkts. 25, 27.

the warrant affidavit contained false statements, (2) these false statements were made intentionally or with reckless disregard for the truth, and (3) the false statements were material to the finding of probable cause. *United States v. Hancock*, 844 F.3d 702, 708 (7th Cir. 2016). This rule applies to omissions as well as affirmative misrepresentations. *Id*. If, in spite of affiant's alleged errors, the affidavit contains sufficient allegations to establish probable cause, then a hearing is unnecessary. *United States v. Mullins*, 803 F.3d 858, 862 (7th Cir. 2015). Because this burden is so high, *Franks* hearings are rarely held, *see United States v. Swanson,* 210 F.3d 788, 790 (7th Cir. 2000).

Johnson has not made the substantial preliminary showing that would entitle him to a *Franks* hearing. I already have rejected his second and fourth arguments, which are not based upon "inaccuracies" per se but on alleged mischaracterizations. Johnson's first argument fails because it mischaracterizes the language of Attachment A. He implies that Attachment A listed the place to be searched as the "Target Website"–which was located in the Eastern District of Virginia– and disguised the fact that the search would occur on activating computers located well beyond that district. *See* dkt. 17 at 7, dkt. 23, at 3. Actually, Attachment A states at the outset "This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below." NIT Warrant Aff., dkt. 17-2, Att. A. Attachment A then defines the "target website," including its location in the Eastern District of Virginia, and defines the "activating computers" as those of any user or administrator who logs into the target website by entering a username and password. *Id*. As other district courts have found, "[a] complete, contextual reading of the warrant demonstrates . . . that the warrant was not geographically limited to activating computers in the Eastern District of Virginia." *United States*

v. Tran, ___ F. Supp. 3d ___, 2016 WL 7468005, at *5 (D. Mass. Dec. 28, 2016). *See also United States v. Levin*, 186 F.Supp.3d 26, n.8 (D. Mass. May 5, 2016) ("That the cover page of the NIT Warrant application indicated that the property to be searched was located in the Eastern District of Virginia does not alter this conclusion."); *United States v. Michaud*, 2016 WL 337263 at *4 (W.D. Wash. Jan. 28, 2016) ("Mr. Michaud's argument requires an overly narrow reading of the NIT Warrant that ignores the sum total of its content. While the NIT Warrant cover sheet does explicitly reference the Eastern District of Virginia, that reference should be viewed within context ....").

Johnson's fifth argument—that Agent Macfarlane used "misleading technical jargon" to make commonplace technologies such as image and video hosting and message boards seem criminal—likewise misses the mark. Agent Macfarlane did not say that such technologies were used "only" to exchange child pornography. Instead, he made clear that, based on his review of the site and his training and experience, he believed that these features were actually being used by Playpen users to disseminate child pornography. He supported this belief by citing graphic examples of child pornography that actually were distributed via these technologies. That an individual may also be able to use upload and link capabilities to post innocent images is an obvious fact that has no bearing on the probable cause analysis.

This leaves Johnson's claim that the affidavit inaccurately described Playpen's home page on the date the warrant was issued. Johnson is correct: the description was inaccurate. The site's logo changed between the time Agent Macfarlane completed the affidavit and the time the magistrate judge issued the warrant. Nonetheless, no *Franks* hearing is necessary because this outdated description of the images of the two prepubescent girls was not necessary for the court to find probable cause. As discussed in the preceding section, other factors supported the

issuance of the warrant and they would suffice even if the court redacts Agent Macfarlane's incorrect description of the home page. *Accord Tran*, 2016 WL 7468005, *7 ("the new logo would not have changed the probable cause analysis"); *Matish*, 193 F. Supp. 3d at 606 (the "logo change lacks significance because the probable cause rested not solely on the site's logo but also on the affiant's description that the entire site was dedicated to child pornography, Playpen's suggestive name, the affirmative steps a user must take to locate Playpen, the site's repeated warnings and focus on anonymity, and the actual contents of the site"); *Darby*, 190 F. Supp. 3d at 534 ("[C]ontrary to the repeated emphasis of Defendant, the images of two prepubescent females described in the warrant application were not necessary to the finding of probable cause. There was an abundance of other evidence before the magistrate judge that supported her finding that there was probable cause to issue the warrant."); *Owens*, 2016 WL 7079609, at 5-7 ("[E]ven if the affiant had accurately described the homepage, there would have been probable cause for the search."); *Allain*, 2016 WL 5660452, at 7-8.

C. Overbreadth

The Fourth Amendment prohibits general search warrants and requires that a warrant describe with particularity the place to be searched and the persons or things to be seized. U.S. Const. amend. IV. The purpose of the particularity requirement is to "protect persons against the government's indiscriminate rummaging through their property" and to "[prevent] the searching for and seizure of items that there is no probable cause to believe are either contraband or evidence of a crime." *United States v. Jones*, 54 F.3d 1285, 1289–90 (7th Cir. 1995) (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement

ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *United States v. Vitek Supply Corp.*, 144 F.3d 476, 481 (7th Cir. 1998) ("This requirement . . . ensures that the scope of a search will be confined to evidence relating to a specific crime that is supported by probable cause."). Put in more practical terms, "[i]f you are looking for an adult elephant, searching for it in a chest of drawers is not reasonable." *Platteville Area Apartment Ass'n v. City of Platteville*, 179 F.3d 574, 579 (7th Cir. 1999).

Johnson argues that the NIT warrant was "the Internet age equivalent of a general warrant," in that it allowed the FBI to deploy an NIT search based merely on a user's having accessed Playpen's home page, regardless whether that user engaged in a chat, viewed pictures or otherwise participated in activities on the site. According to Johnson, the issuing court should have required the FBI to narrow deployment of the NIT to only "those people who 'clicked' on particular sub-directories with illegal content or particular pictures or links" contained in the site's sub-directories. Dkt. 17, at 21-22. Johnson points out that the warrant as framed allowed the FBI to search "tens of thousands of computers."

Johnson cites no case for the proposition that the mere fact that the warrant authorized the search of a potentially large number of suspects renders it constitutionally infirm. Whether it could have been more narrowly tailored to reach potentially fewer suspects is not the operative question. The question posed by the particularity requirement is merely whether the warrant described with particularity the places to be searched and the items to be seized, and whether there was probable cause to believe the searched-for items would be located in the area to be searched.

That standard is easily met in this case. Attachments A and B defined with precision where agents could look and for what. As already discussed, the issuing court was presented with numerous facts and circumstances indicating that it was reasonably likely that *any* user or administrator who logged in to Playpen from an activating computer by entering a user name and password was likely doing so for the purpose of viewing or sharing child pornography. The warrant was not overbroad. *Anzalone*, 2016 WL 5339723, at * 7 ("Every court to consider this question has found the NIT search warrant sufficiently particular.").

D. Anticipatory Warrant

As Johnson points out, the warrant in this case was anticipatory in that deployment of the NIT was not triggered until someone logged into Playpen by entering a user name and password. Johnson argues that the act of logging in to Playpen was not an appropriate triggering event because it was not indicative of criminal activity. Dkt. 17, at 23 ("In this case, there was probable cause to search the computers of everyone who signed into Playpen (the triggering event) only if the site so unabashedly announced that it was dedicated to child pornography that it would be inescapable that illegal content was within."). This argument just repackages Johnson's probable cause and *Franks* arguments. Logging into Playpen was a sufficient triggering event for the reasons set forth in previous sections. This is not a basis to quash the warrant.

E. Rule 41(b)

Finally, Johnson argues that, because the Virginia warrant was not limited in geographic scope—in other words, because the NIT could and did capture data about users who physically might be located all over the world—it violated the territorial limitations of the Federal

Magistrates Act, specifically 28 U.S.C. § 636(a), as well as Federal Rule of Criminal Procedure 41(b). As a result, Johnson argues, the warrant was void at its inception and the evidence seized pursuant thereto must be suppressed.

A few courts have accepted this argument, but most have rejected it.[8] Although there is disagreement within the majority view whether Rule 41(b) was violated, all of these courts agree that even if it was, suppression is not an appropriate remedy. I share this view.

Section 636(a) provides, in relevant part, as follows:

> (a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—(1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts . . .

---

[8] *See United States v. Austin*, 2017 WL 496374, at *3–4 (M.D. Tenn. Feb. 2, 2017); *Michaud*, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016); *United States v. Epich*, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Werdene*, 188 F. Supp. 3d 431 (E.D. Pa. 2016); *United States v. Acevedo–Lemus*, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Adams*, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016); *United States v. Henderson*, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *United States v. Torres*, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016); *United States v. Ammons*, 207 F. Supp. 3d 732, (W.D. Ky. Sept. 14, 2016); *United States v. Knowles*, 207 F. Supp. 3d 585, 607-08 (D.S.C. Sept. 14, 2016); *United States v. Broy*, 209 F.Supp.3d 1045, (C.D. Ill. Sept. 21, 2016); *Anzalone*, 208 F. Supp. 3d at 371-72; *Allain*, ––– F.Supp.3d ––––, 2016 WL 5660452; *United States v. Scarbrough*, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016); *United States v. Stepus*, 2016 WL 6518427 (D. Mass. Oct. 28, 2016); *Owens*, 2016 WL 7053195 (E.D. Wis. Dec. 5, 2016); *United States v. Duncan*, 2016 WL 7131475 (D. Or. Dec. 6, 2016); *United States v. Dzwonczyk*, 2016 WL 7428390 (D. Neb. Dec. 23, 2016). *United States v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016); *United States v. Matish*, 193 F. Supp. 3d 585 (E.D. Va. 2016); *United States v. Eure*, 2016 WL 4059663 (E.D. Va. July 28, 2016); *United States v. Laurita*, 2016 WL 4179365 (D. Neb. Aug. 5, 2016); *United States v. Jean*, 207 F. Supp. 3d 920, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); *United States v. Johnson*, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016); *United States v. Lough*, ––– F.Supp.3d ––––, 2016 WL 6834003 (N.D. W.Va. Nov. 18, 2016); *McLamb*, ––– F.Supp.3d ––––, 2016 WL 6963046 (E.D. Va. Nov. 28, 2016); *United States v. Sullivan*, 2017 WL 201332 (N.D. Ohio Jan. 18, 2017). Four courts have granted suppression: *United States v. Arterbury*, No. 15–CR–182 (N.D. Okla. April 25, 2016); *United States v. Workman*, 205 F. Supp. 3d 1256 , 1265-67 (D. Colo. Sept. 6, 2016); *United States v. Croghan*, 209 F. Supp. 3d 1080, 1090-91 (S.D. Iowa Sept. 19, 2016) *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. May 5, 2016) (appeal pending).

Rule 41(b) of the Federal Rules of Criminal Procedure, in turn, sets out territorial limits on a magistrate judge's authority to issue a search warrant. It authorizes magistrate judges to issue warrants authorizing: (1) the "search for and seize a person or property located within [the judge's] district"; (2) the search for and seize a person or property located outside the judge's 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) the search for and seize a person or property located outside the judge's district if the investigation relates to terrorism; (4) installation within the judge's district a tracking device to track the movement of a person or property located within the district, outside the district, or both; and (5) the search for and seizure of a person or property outside the judge's district but within a United States territory, possession, commonwealth, or premises used by a United States diplomat or consular mission.

Effective December 1, 2016, Rule 41(b) was amended to add Subsection (6), which provides:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

The government argues that the magistrate judge had authority to issue the warrant under Fed. R. Crim. P. 41(b)(4) because the NIT was equivalent to a "tracking device" under. *See* Br. in Opp., dkt. 20, at 41-45. This is a fair argument but it is unpersuasive. Even accepting

the government's argument that the NIT was "installed" on Johnson's computer while he was making a "digital trip" to the Eastern District of Virginia, the NIT did more than merely "track movement" of illegal child pornography content through the internet. The NIT was "designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government," including "information that may assist in identifying the user's computer, its location and the user of the computer." NIT Warrant App, dkt. 17-2, at ¶¶ 33-34. Thus, "the NIT does not track; it searches." *Adams*, 2016 WL 4212079, *6. Moreover, the recent amendment to Rule 41(b)—which plainly would have authorized the magistrate judge to issue the NIT warrant—strongly suggests that such authority was lacking at the time the warrant issued. *Accord Owens*, 2016 WL 7053195, *6 (finding same).

But even if Rule 41(b) was violated, I agree with the government that suppression is not the appropriate remedy for the violation. It is now well-settled that even if a Fourth Amendment violation occurs, application of the exclusionary rule does not necessarily follow. *Davis v. United States*, 564 U.S. 229, 236 (2011); *Herring v. United States*, 555 U.S. 135, 137 (2009). The exclusionary rule is neither a "personal constitutional right" nor a mechanism to "redress the injury" caused by an unconstitutional search; it is a court-made doctrine designed solely to deter future Fourth Amendment violations. *Davis*, 564 U.S. at 236-37. Thus, courts are to apply the exclusionary rule as a "last resort" only where it results in appreciable deterrence that outweighs the substantial social costs that result from allowing some guilty and possibly dangerous defendants to go free. *Herring*, 555 U.S. at 140-41. Moreover, the rule is aimed to deter police misconduct, not judicial misconduct. *United States v. Leon*, 468 U.S. 897, 917 (1984). Generally speaking, "when an officer acting with objective good faith has obtained a search warrant from

a judge or magistrate and acted within its scope . . . there is no police illegality and thus nothing to deter." *Leon*, 468 U.S. at 920.

Relying on *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. May 5, 2016) (appeal pending, 1st Cir. Case No. 16-1567), Johnson argues that *Leon*'s good faith exception is not available in the case of a warrant issued by a magistrate lacking authority to do so. In *Levin*, 186 F. Supp. 3d at 39, the court observed that neither *Leon* nor the Supreme Court's later cases expanding the good faith doctrine involved a warrant that was void *ab initio*. The court found persuasive a handful of state and federal district court cases concluding that a warrant issued by a judge with no authority to issue it is akin to no warrant at all, and therefore the good faith exception does not apply. *Id*. at 40-41. Three district courts in other circuits have followed *Levin's* reasoning and have declined to apply the good faith exception to the NIT warrant. *United States v. Arterbury*, No. 15–CR–182 (N.D. Okla. April 25, 2016); *United States v. Workman*, 205 F. Supp. 3d 1256 , 1265-67 (D. Colo. Sept. 6, 2016); *United States v. Croghan*, 209 F. Supp. 3d 1080, 1090-91 (S.D. Iowa Sept. 19, 2016).

District courts in the Seventh Circuit, however, have found *Levin* unpersuasive. (Obviously, that court's opinion has no precedential authority). As the court observed in *Owens*, 2016 WL 7053195, *7-8, *Levin*'s holding is inconsistent with Seventh Circuit precedent strongly suggesting if not directly holding that a Rule 41(b) violation does not trigger the exclusionary rule. In *United States v. Berkos*, 543 F.3d 392 (7th Cir. 2008), the defendant challenged the authority of a magistrate judge sitting in the district where the crime was being investigated to issue a search and production of electronic evidence directed to an out-of-district internet service provider. Noting that the defendant's argument "presents the question of whether a violation of Federal Rule of Criminal Procedure 41(b), which discusses authority to issue search warrants,

merits invoking the exclusionary rule," *id*. at 396, the court reaffirmed this circuit's previous holdings that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause and with advance judicial approval." *Id*. at 396 (quoting *United States v. Cazares–Olivas*, 515 F.3d 726, 730 (7th Cir. 2008), and *United States v. Trost*, 152 F.3d 715, 722 (7th Cir. 1998)). Quoting from its decision in *Cazares–Olivas*, 515 F.3d at 730, the *Berkos* court observed that "[t]he remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant would be 'wildly out of proportion to the wrong.'" *Id*. Although the court found that "[t]his alone merits affirming the district court's denial of Berkos's first motion to suppress," *id*., it noted that the government had not raised this argument in its brief or at oral argument and therefore had waived it. *Id*.

In the *Owens* court's view, *Berkos* compelled the conclusion that the exclusionary rule did not apply to Rule 41(b) violations. *Owens*, 2016 WL 7053195, *8. *See also United States v. Epich*, 2016 WL 953269, *2 (E.D. Wis. Mar. 14, 2016) (adopting magistrate judge's report and recommendation finding suppression not warranted for Rule 41(b) violation under *Berkos*). As the court observed in *United States v. Broy*, 209 F. Supp. 3d 1045, 1057 (C.D. Ill. 2016), however, whether *Berkos* controls is not a certainty: the court's statements regarding the impropriety of exclusion for a Rule 41(b) violation arguably are dicta given the government's waiver in that case. Moreover, *Cazares-Olivas*, 515 F.3d 726, the case cited in *Berkos*, did not involve a Rule 41(b) violation.

Even if these cases are not controlling, I still conclude that suppression would be an inappropriate remedy under the Court's holdings in *Leon* and *Herring*. "The exclusionary rule should be limited to those situations where its remedial objectives are best served, i.e., to deter illegal police conduct, not mistakes by judges and magistrates." *United States v. Burgos–Montes*,

786 F.3d 92, 109 (1st Cir. 2015) (quoting *United States v. Bonner*, 808 F.2d 864, 867 (1st Cir. 1986)). There is no evidence of any misconduct by the FBI. Before conducting the search at issue, the FBI obtained a judicial determination that the facts set forth in Agent Macfarlane's meticulous affidavit established probable cause to deploy the NIT. The FBI's application and affidavit did not contain material misstatements or omit any material facts. The FBI did not hide the fact that it was seeking authorization to search the contents of computers located outside the judicial district as noted earlier, this was plainly stated in the application and the attachments. Thus, the agents presented the magistrate judge with all the facts she needed to satisfy herself of her jurisdiction before proceeding to issue the warrant. Although Johnson asserts that "law enforcement agents were keenly aware that the warrant they obtained patently exceeded the Magistrate Judge's jurisdiction," Br. in Supp., dkt. 17, at 28, the record does not support this assertion.

As other courts have found, "[t]he FBI agents can hardly be faulted for failing 'to understand the intricacies of the jurisdiction of federal magistrates.'" *United States v. Ammons*, 207 F. Supp. 3d 732, 744–45 (W.D. Ky. 2016) (quoting *Darby*, 190 F.Supp.3d at 538, 2016 WL 3189703, at *14; *cf. Leon*, 468 U.S. at 921, 104 S.Ct. 3405 ("In the ordinary case, an officer cannot be expected to question the magistrate's . . . judgment that the form of the warrant is technically sufficient."). As observed above in note 7, there is disagreement among reasonable jurists on this exact question. "The fact that courts are presently divided over" whether the NIT warrant "even violated Rule 41 is compelling evidence that the FBI did not . . . deliberately violate the Rule by seeking the warrant in the first instance." *Acevedo–Lemus*, 2016 WL 4208436, at *7. *See also Anzalone*, 208 F. Supp. 3d at 371–72 ("Given the closeness of the question and the absence of any evidence of reckless disregard of the strictures of the Fourth

Amendment by law enforcement, the Court finds that the agents here acted in 'objectively reasonable reliance' on the NIT warrant."); *Michaud*, 2016 WL 337263, at *7 ("Because reliance on the NIT Warrant was objectively reasonable, the officers executing the warrant acted in good faith, and suppression is unwarranted."); *Darby*, 190 F. Supp. 3d at 452 ("[T]here is no evidence that any failure by the FBI to understand the intricacies of the jurisdiction of federal magistrates was deliberate."); *Werdene*, 188 F. Supp. 3d at 452 ("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.").

Even assuming, *arguendo*, that the FBI's conduct in obtaining the challenged warrant was in some way blameworthy, at worst this would amount to "simple, isolated negligence," for which the deterrence rationale of the exclusionary rule loses much of its force. *Davis*, 564 U.S. at 238-39 (internal citations and quotations omitted). In light of all the circumstances, including Johnson's acknowledgment that the NIT Warrant could have been lawfully issued by any Article III judge sitting in the same courthouse as the magistrate judge, the minimal deterrence benefits of suppression do not come close to outweighing its heavy costs. This court should deny Johnson's motion to suppress.

RECOMMENDATION

Pursuant to 28 U.S.C. § 636(b)(1)(B), I respectfully recommend that the motion of Mitchell Johnson to suppress evidence, dkt. 17, be DENIED.

Entered this 14th day of June, 2017.

BY THE COURT:

/s/

STEPHEN L. CROCKER
Magistrate Judge

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN
120 N. Henry Street, Rm. 540
Madison, Wisconsin 53703

Chambers of
STEPHEN L. CROCKER
U.S. Magistrate Judge

Telephone
(608) 264-5153

June 14, 2017

All Counsel of Record

Re: United States v. Mitchell Johnson
Case No. 16-cr-76-wmc

Dear Counsel:

The attached Report and Recommendation has been filed with the court by the United States Magistrate Judge.

The court will delay consideration of the Report in order to give the parties an opportunity to comment on the magistrate judge's recommendations.

In accordance with the provisions set forth in the memorandum of the Clerk of Court for this district which is also enclosed, objections to any portion of the report may be raised by either party on or before June 30, 2017, by filing a memorandum with the court with a copy to opposing counsel.

If no memorandum is received by June 30, 2017, the court will proceed to consider the magistrate judge's Report and Recommendation.

Sincerely,

/s/

Susan K. Vogel for Connie A. Korth
Secretary to Magistrate Judge Crocker

Enclosures

MEMORANDUM REGARDING REPORTS AND RECOMMENDATIONS

Pursuant to 28 U.S.C. § 636(b), the district judges of this court have designated the full-time magistrate judge to submit to them proposed findings of fact and recommendations for disposition by the district judges of motions seeking:

(1) injunctive relief;

(2) judgment on the pleadings;

(3) summary judgment;

(4) to dismiss or quash an indictment or information;

(5) to suppress evidence in a criminal case;

(6) to dismiss or to permit maintenance of a class action;

(7) to dismiss for failure to state a claim upon which relief can be granted;

(8) to dismiss actions involuntarily; and

(9) applications for post-trial relief made by individuals convicted of criminal offenses.

Pursuant to § 636(b)(1)(B) and (C), the magistrate judge will conduct any necessary hearings and will file and serve a report and recommendation setting forth his proposed findings of fact and recommended disposition of each motion.

Any party may object to the magistrate judge's findings of fact and recommended disposition by filing and serving written objections not later than the date specified by the court in the report and recommendation. Any written objection must identify specifically all proposed

findings of fact and all proposed conclusions of law to which the party objects and must set forth with particularity the bases for these objections. An objecting party shall serve and file a copy of the transcript of those portions of any evidentiary hearing relevant to the proposed findings or conclusions to which that party is objection. Upon a party's showing of good cause, the district judge or magistrate judge may extend the deadline for filing and serving objections.

After the time to object has passed, the clerk of court shall transmit to the district judge the magistrate judge's report and recommendation along with any objections to it.

The district judge shall review de novo those portions of the report and recommendation to which a party objects. The district judge, in his or her discretion, may review portions of the report and recommendation to which there is no objection. The district judge may accept, reject or modify, in whole or in part, the magistrate judge's proposed findings and conclusions. The district judge, in his or her discretion, may conduct a hearing, receive additional evidence, recall witnesses, recommit the matter to the magistrate judge, or make a determination based on the record developed before the magistrate judge.

NOTE WELL: A party's failure to file timely, specific objections to the magistrate's proposed findings of fact and conclusions of law constitutes waiver of that party's right to appeal to the United States Court of Appeals. ***See United States v. Hall,*** **462 F.3d 684, 688 (7th Cir. 2006).**