United States v. Anzalone

United States District Court for the District of Massachusetts

September 22, 2016, Decided; September 22, 2016, Filed

Criminal Action No. 15-10347-PBS

Reporter
2016 U.S. Dist. LEXIS 129735

UNITED STATES OF AMERICA, v. VINCENT ANZALONE, Defendant.

Core Terms

user, site, website, child pornography, magistrate judge, probable cause, logged, network, suppression, search warrant, computers, deploy, reasonable expectation of privacy, activating, visited, server, good faith, accessing, homepage, hidden, images, warrant application, tracking device, void ab initio, downloaded, triggering, partially, clothed, girls, district court

Counsel: **[*1]** For Vincent C. Anzalone, also known as Vincent Anzalone, Defendant: Timothy G. Watkins, LEAD ATTORNEY, Federal Public Defender Office, District of Massachusetts, Boston, MA.

For USA, Plaintiff: David G. Tobin, LEAD ATTORNEY, United States Attorneys Office, Boston, MA.

Judges: Patti B. Saris, Chief United States District Judge.

Opinion by: Patti B. Saris

Opinion

MEMORANDUM AND ORDER

Saris, C.J.

INTRODUCTION

Defendant Vincent Anzalone is charged with one count of possession of child pornography in violation of *18 U.S.C. § 2252A(a)(5)(B)* and one count of receipt of child pornography in violation of *18 U.S.C. § 2252A(a)(2)(A)*. The government also seeks forfeiture of any child pornography images in the defendant's possession.

This case arises from an FBI investigation into users of Playpen, a child pornography website. Playpen operates on the Tor network, which enables anonymous internet browsing. In February 2015, the government acquired control of Playpen's server. For two weeks, the government operated the website. To obtain the IP addresses of the site's users, the government applied for and received a search warrant from a magistrate judge in the Eastern District of Virginia. The search warrant allowed the FBI to deploy a Network Investigative Technique (NIT) on users' **[*2]** computers. The NIT caused users' computers to transmit identifying information, including IP addresses, to the government. The defendant asserts the government unreasonably searched his computer by using the NIT in violation of the *Fourth Amendment*. Specifically, the defendant contends that the warrant lacked probable cause, that the magistrate judge in the Eastern District of Virginia did not have the authority to authorize a search in the District of Massachusetts, and that suppression is required. The defendant moves to suppress all evidence gathered by the NIT as well as all fruits of the allegedly unconstitutional search.

For the reasons set forth below, the defendant's

motion to suppress (Docket No. 47) is **DENIED**.

FACTUAL BACKGROUND

The following facts are undisputed unless otherwise noted. The Court has not held an evidentiary hearing. The facts are primarily drawn from FBI Special Agent Douglas Macfarlane's affidavit in support of the February 20, 2015 search warrant application. The defendant initially requested a Franks hearing, but later withdrew that request. See Docket No. 65 at 5 n.4. The Court requested the parties to supplement the record with more information about the NIT, which the **[*3]** Court considered.

I. The Tor Network

Special Agent Macfarlane has worked as an FBI Special Agent for two decades. At the time of the investigation at issue, he was assigned to the FBI's Violent Crimes Against Children Section. On February 20, 2015, Macfarlane submitted a search warrant application to Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia. Macfarlane appended his affidavit to that application. The statements contained in the affidavit were based on information provided by other federal and foreign law enforcement agents, information obtained from subpoenas, the results of physical and electronic surveillance, forensic computer analysis, and Macfarlane's own experience and training as a special agent.

In his affidavit, Agent Macfarlane described the mechanics of the Tor network. The Tor network, also known as The Onion Router, is an anonymity network that masks a user's IP address. Designed by the U.S. Naval Laboratory to protect government communications, Tor is now available to the public. To access the Tor network, a user must download an add-on to the user's existing browser or download the Tor browser bundle. To ensure anonymity for its users, **[*4]** the Tor network bounces communications through various relay computers. When a user accesses a website, the IP address of the last computer in that chain is displayed, rather than the user's IP address. The network therefore "prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked." Macfarlane Aff. ¶ 8, Docket No. 48, Ex. 2.

Within the Tor network, sites can be designed as "hidden services." Hidden services are only accessible if the user is using the Tor network. Hidden services allow websites and other servers to hide their location. Like traditional websites, these sites "are hosted on computer servers that communicate through IP addresses." Id. ¶ 9. Unlike such websites, however, the "IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters" followed by the suffix ".onion." Id.

II. The Playpen Website

Playpen operated as a hidden service on the Tor network. The site was only accessible via the Tor network. **[*5]** According to Agent Macfarlane, even then, a user was required to know the site's address: "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." Id. ¶ 10. To learn Playpen's unique .onion address, a user might communicate directly with others on Tor or he might consult another site that lists links to child pornography hidden service sites. Agent Macfarlane concluded that accessing Playpen "therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon [Playpen] without understanding its purpose and content." Id.[1]

[1] The defendant counters that Tor search engines do exist and that even hidden service sites are indexed: "All a user need do is enter search terms for sexually oriented sites, chat rooms, or a host of

Agent Macfarlane described Playpen's homepage as it appeared on February 18, 2015, two days before he signed the affidavit. At the top left corner of the page, the name Playpen was prominently displayed. On either side of the site name were images depicting partially clothed prepubescent girls with their legs spread apart. Below these images, the site stated: "No cross-board reports, .7z preferred, encrypt filenames, include preview." Id. ¶ 12. Agent Macfarlane explained that "no-cross-board reports" was an instruction to users not to post material appearing on other sites. Id. The ".7z preferred" statement referred to a method of compressing large files for distribution. Id. At the top right corner, to the right of the site name, users could enter a username and password, and select a session length. A login button **[*7]** appeared to the right of those login fields.

Below the site name, the image of the two partially clothed girls, and the login fields was a textbox that read: "Warning! Only registered members are allowed to access this section. Please login below or 'register an account' with Playpen." Id. The "register an account" text was hyperlinked to the site's registration page. Another set of login fields appeared below this warning, asking users to enter their username, password, minutes to stay logged in, and whether they wanted to permanently remain logged in.

When a prospective user clicked the "register an account" hyperlink, the user saw a message from the forum operators. The message explained that the forum required new users to enter an email address and that the software "checks that what you enter looks approximately valid." Id. ¶ 13. However, the forum operators encouraged users to enter fake email addresses: we "do NOT want you to enter a real address, just something that matches the xxx@yyy.zzz pattern. No confirmation will be sent. This board has been intentionally configured so that it WILL NOT SEND EMAIL, EVER." Id. The message further cautioned new users: "For your security you **[*8]** should not post information here that can be used to identify you." Id. The forum operators further emphasized the site's focus on anonymity: "The website is not able to see your IP and can not collect or send any other form of information to your computer except what you expressly upload," explaining that only a text file with the user's username and password reside in the browser's cache. Id.

The defendant and the government agree that one aspect of the homepage changed between February 18, 2015, when Agent Macfarlane last visited the Playpen site, and February 20, 2015, when Agent Macfarlane signed his affidavit and submitted the search warrant application. As of February 3, 2015, the homepage featured the two photos of the partially clothed prepubescent girls described above. Sometime after February 3, 2015, Agent Macfarlane learned that the site's URL had changed. On February 18, 2015, he visited the Playpen site at its new URL. He confirmed that its content had not changed. However, on February 19, 2015, the logo on Playpen's site changed. Instead of two prepubescent, partially clothed girls with their legs spread, the site featured one young girl (age unclear) wearing a short **[*9]** dress and black stockings with her legs crossed. Agent Macfarlane did not know of this change when he signed the affidavit on February 20, 2015. Therefore, the affidavit incorrectly described the homepage.

After logging into Playpen with a username and password, visitors to the site had access to various forums, many of which contained child pornography. The table of contents included nearly fifty topics, including "pre-teen photos," "pre-teen videos," "jailbait photos," "jailbait videos," "kinky

---

other content not related to child pornography to find sites like Playpen." Docket No. 48 at 22. The defendant cites ahmia.fi as an example of a Tor search engine. However, Playpen and other child pornography websites **[*6]** are banned by ahmia.fi. See Hidden Service Blacklist — Ahmia, *https://ahmia.fi/blacklist* (last visited Aug. 31, 2016) ("Ahmia blacklists sites containing child abuse material from its index."); Ahmia search after GSoC development, *https://blog.torproject.org/category/tags/ahmiafi* (last visited Aug. 31, 2016) ("We have decided to filter any sites related to child porn from our search results. Ahmia is removing everything related to these websites.").

fetish," "webcams," and "family -- incest." Id. ¶ 14. Agent Macfarlane noted in the affidavit that "jailbait" refers to underage, but post-pubescent minors. Id. ¶ 14 n.4. He also explained that the photos and videos were denominated as "HC" or "SC/NN." Id. ¶ 14 n.5. Agent Macfarlane stated that "HC" stands for hardcore and depicts "penetrative sexually explicit content," "SC" stands for softcore and includes "depictions of non-penetrative sexually explicit conduct," and "NN" stands for non-nude and depicts "subjects who are fully or partially clothed." Id. Agent Macfarlane provided various examples of photos and videos depicting child pornography within these forum sections.

Agent Macfarlane **[*10]** described other features of the site that allowed for the dissemination of child pornography: a private messaging function; an image hosting feature, which allowed users to upload links to images of child pornography; a file hosting feature, which allowed users to upload videos of child pornography; and a chat feature, which allowed those logged into the chat service to view and post images of child pornography. For each of these components of the website, Agent Macfarlane identified specific examples of child pornography being posted or transmitted.

III. The Network Investigative Technique

In December 2014, a foreign law enforcement agency alerted the FBI of an IP address connected with Playpen. The FBI identified the server hosting company that owned this IP address. The FBI then obtained a search warrant and seized a copy of the server assigned to the IP address at issue. After reviewing the server copy, FBI agents determined that it contained a copy of Playpen. Further investigation revealed that Playpen's suspected administrator lived in Naples, Florida. On February 19, 2015, the FBI executed a search warrant at the administrator's Florida residence. As of February 19, 2015, the **[*11]** FBI assumed control of Playpen. The government operated the website for the following two weeks.

While operating Playpen, the government sought permission from a magistrate judge in the Eastern District of Virginia to deploy the NIT. Because Playpen resided on the Tor network, Agent Macfarlane explained in his affidavit that the NIT was necessary to identify the site's users and administrators. Macfarlane stated that other methods typically used in criminal investigations "have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried." Id. ¶ 31.

The search warrant requested the authority to deploy the NIT at the point when a user accesses Playpen, enters a username and password, and logs into the site. Agent Macfarlane noted that, despite a request to deploy the NIT at this stage, "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation, in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users," such as those who post most often or those who visit those forum sections dedicated solely to child pornography. Id. ¶ 32 n.8.

Agent Macfarlane detailed the technical **[*12]** aspects of the NIT deployment. He explained that the NIT would deploy from the Eastern District of Virginia. Macfarlane stated that generally, when a user visits a website, the computer downloads content that is used to display web pages on the user's computers. The NIT "would augment that content with additional computer instructions." Macfarlane Aff. ¶ 33, Docket No. 48, Ex. 2. "When a user's computer successfully downloads those instructions from [Playpen], located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government." Id.

The affidavit enumerated the seven categories of information that would be transmitted back to the government and would help identify Playpen users: the activating computer's IP address, a unique

identifier generated by the NIT to distinguish data from other activating computers, the type of operating system running on the activating computer, information about whether the NIT had previously been delivered to the activating computer, the activating computer's Host Name,[2] the activating computer's **[*13]** active operating system username, and the activating computer's media access control (MAC) address.[3] These seven pieces of information were to be transmitted to the government every time a user logged into Playpen. In addition, when accessing Playpen, a user sends "request data" to the website. The government recorded that data and paired it with the data collected separately by the NIT so that the government could determine which pages a user accessed and how long the user was logged into Playpen during the two-week period in which the government operated the site.

On February 20, 2015, Magistrate Judge Theresa Carroll Buchanan granted the NIT warrant. The next day, the defendant visited Playpen and the NIT was deployed. According to the government, **[*14]** the defendant was actively logged into Playpen for twelve hours, one minute, and twenty-four seconds during the two weeks the government controlled the site.

On October 20, 2015, Magistrate Judge Judith Dein of the District of Massachusetts issued a search warrant of the defendant's residence. Members of the FBI Child Exploitation Task Force executed the warrant on October 21, 2015. Inside the residence and after the defendant waived his Miranda rights, law enforcement agents recorded an interview with him. During the interview, the defendant allegedly admitted to possessing child pornography, stating that he downloaded it three to four times a week for five or six years. He purportedly estimated that he had between 50 and 100 gigabits of child pornography on his computer.

IV. Procedural Background

On November 12, 2015, the defendant was indicted on one count of possession of child pornography in violation of *18 U.S.C. § 2252A(a)(5)(B)* and one count of receipt of child pornography in violation of *18 U.S.C. § 2252A(a)(2)(A)*. On May 13, 2016, the defendant moved to suppress the evidence gathered by the NIT and all fruits of this search, including the evidence gathered during the subsequent search of the defendant's home.

DISCUSSION

I. Reasonable [*15] Expectation of Privacy

The government contends that the "most critical piece of information obtained by the NIT warrant -- Defendant's IP address -- is information that ordinarily would have been publicly available over which the defendant cannot claim a reasonable expectation of privacy." Docket No. 58 at 30. The defendant responds that the NIT gathered more than the IP address and that the defendant had a reasonable expectation of privacy in the contents of his personal computer.

The *Fourth Amendment* provides that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." *U.S. Const. amend. IV*. "Intrusions upon personal privacy do not invariably implicate the *Fourth Amendment*. Rather, such intrusions cross the constitutional line only if the challenged conduct infringes upon some reasonable expectation of privacy." *Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174, 178 (1st Cir. 1997)*. "Whether a defendant has a reasonable expectation of privacy in a particular place is a two-pronged inquiry. We consider 'first, whether the movant has exhibited an actual, subjective, expectation of privacy; and second, whether such

[2] "A Host Name is a name assigned to a device connected to a computer network that is used to identify that device in various forms of electronic communication, such as communications over the Internet." Macfarlane Aff. ¶ 34, Docket No. 48, Ex. 2.

[3] A MAC address is a unique identifying number assigned to a network adapter, which is equipment that connects a computer to a network. The MAC address does not change and is intended to be unique. Id.

subjective expectation is one that society is prepared to recognize as objectively reasonable.'" **[*16]** *United States v. Werra, 638 F.3d 326, 331 (1st Cir. 2011)* (quoting *United States v. Rheault, 561 F.3d 55, 59 (1st Cir. 2009)*).

The NIT caused a user's computer to transmit to the government seven pieces of information, including the user's IP address. The government also collected information about a user's activities on Playpen -- such as the particular pages visited and the amount of time logged into the site -- and matched that data to the user's IP address. Some courts have found that an individual lacks a reasonable expectation of privacy in one's IP address. See, e.g., United States v. Caira, No. 14-1003, 2016 WL 4376472, at *5 (7th Cir. Aug. 17, 2016) ("Because [the defendant] voluntarily shared his I.P. addresses with Microsoft, he had no reasonable expectation of privacy in those addresses.").

A number of district courts have found that law enforcement therefore did not require a search warrant before deploying the NIT. See United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *3 (C.D. Cal. Aug. 8, 2016) ("The Court concludes that the FBI's acquisition of the key piece of information here -- Defendant's IP address -- was not a search under the meaning of the *Fourth Amendment*, and therefore did not require a warrant."); United States v. Matish, No. 4:16CR16, 2016 WL 3545776, at *19 (E.D. Va. June 23, 2016) ("Defendant possessed no reasonable expectation of privacy in his computer's IP address, so the Government's acquisition of the IP address did not represent a prohibited **[*17]** *Fourth Amendment* search."); United States v. Werdene, No. CR 15-434, 2016 WL 3002376, at *10 (E.D. Pa. May 18, 2016) ("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* . . . .").

Other district courts have cautioned against the narrow scope of this inquiry, asking "whether the IP address should be the focus of this analysis or whether Defendant's expectation of privacy in his computer is the proper subject of this analysis." United States v. Adams, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016). These district courts have concluded that, because the "NIT searches the user's computer to discover the IP address associated with that device," the user'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." Id. If "an individual has a reasonable expectation of privacy in the contents of his or her personal computer, as he or she does, and the deployment of the NIT invades that privacy, then the NIT is a search." United States v. Darby, No. 2:16CR36, 2016 WL 3189703, at *6 (E.D. Va. June 3, 2016). It "is irrelevant that Defendant might not have a reasonable expectation of privacy in some of the information searched and **[*18]** seized by the government. The government's deployment of the NIT was a *Fourth Amendment* search." Id.

The Court finds that the defendant had a reasonable expectation of privacy in his personal computer and that the government's use of the NIT constituted a *Fourth Amendment* search. While the most critical piece of information obtained by the NIT warrant may have been the IP address, the NIT afforded the government access to six other pieces of identifying information that were not readily available to law enforcement, as well as the ability to pair a user's actions on Playpen with the user's IP address. Even if the defendant did not have a reasonable expectation of privacy in these discrete pieces of information, he did have a reasonable expectation of privacy in the computer that housed this data and that was instructed by the NIT to transmit the data back to the government.

II. Probable Cause

The defendant argues that the site's illegal purpose was not readily apparent from the homepage as described in the affidavit and that a visitor could

log into the site unaware of its content. The government retorts that users had to take a number of affirmative steps to access the site, that the homepage alerted users that the **[*19]** site contained illicit material, and that the registration process further signaled the unlawful nature of the site.

"A warrant application must demonstrate probable cause to believe that (1) a crime has been committed -- the 'commission' element, and (2) enumerated evidence of the offense will be found at the place to be searched -- the so-called 'nexus" element.'" *United States v. Feliz, 182 F.3d 82, 86 (1st Cir. 1999)*. Probable cause "does not demand certainty, or proof beyond a reasonable doubt, or even proof by a preponderance of the evidence -- it demands only 'a fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Rivera, 825 F.3d 59, 63 (1st Cir. 2016)* (quoting *Illinois v. Gates, 462 U.S. 213, 235, 238 (1983)*). "All that is needed is a 'reasonable likelihood' that incriminating evidence will turn up during a proposed search." *United States v. Clark, 685 F.3d 72, 76 (1st Cir. 2012)* (quoting *Valente v. Wallace, 332 F.3d 30, 32 (1st Cir. 2003)*).

"A magistrate's 'determination of probable cause should be paid great deference by reviewing courts.'" *Gates, 462 U.S. at 236* (quoting *Spinelli v. United States, 393 U.S. 410, 419 (1969)*). The inquiry "is whether the magistrate had a 'substantial basis' for concluding that probable cause existed." *Feliz, 182 F.3d at 86* (quoting *United States v. Taylor, 985 F.2d 3, 5 (1st Cir. 1993)*).

Agent Macfarlane's affidavit establishes a fair probability that an individual who downloaded a Tor browser, located the Playpen site, entered an email address and password, and logged in[4] did so with the purpose **[*20]** of accessing child pornography. See United States v. Eure, No. 2:16CR43, 2016 WL 4059663, at *6 (E.D. Va. July 28, 2016) ("[T]here was probable cause to search the computers of those who registered and logged into the website even after the change to the website."); Matish, 2016 WL 3545776, at *11 (finding that it was reasonable to "find that Playpen's focus on anonymity, coupled with Playpen's suggestive name, the logo of two prepubescent females partially clothed with their legs spread apart (or, as discussed below, the one scantily clad minor), and the affidavit's description of Playpen's content, endowed the NIT Warrant with probable cause."); Darby, 2016 WL 3189703, at *8 ("In sum, the information in the affidavit provided substantial evidence in support of the magistrate's finding that there was probable cause to issue the NIT Warrant. . . . Although it is not beyond possibility that some of those who logged into Playpen did so without intention of finding child pornography, probable cause requires a fair probability that a search will uncover evidence, not absolute certainty."); United States v. Epich, No. 15-CR-163-*PP, 2016 WL 953269, at *1 (E.D. Wis. Mar. 14, 2016)* ("[A]nyone who ended up as a registered user on the web site was aware that the site contained, among other things, pornographic images of children.").

The defendant maintains that, even if the affidavit as presented to the magistrate judge established probable cause for the NIT, the magistrate judge would have ruled differently if she had been presented with an accurate description of the Playpen homepage. Specifically, the defendant emphasizes that the homepage depicted a single image of a scantily clad girl with her legs crossed, as opposed to two partially clothed prepubescent girls with their legs spread apart. Initially, the defendant requested a Franks hearing on these

[4] In supplemental briefing, the **[*21]** government informed the Court that, despite what the warrant authorized, the FBI did not deploy the NIT in this case until the defendant accessed a forum section that explicitly referenced the child pornography content therein. Docket No. 70 at 1-2. The defendant responds that the probable cause inquiry focuses on what the warrant permitted, not when the officers chose to deploy the NIT. Docket No. 74 at 1. Because the Court finds that there was probable cause to deploy the NIT when a user logged into Playpen, the Court need not address how, if at all, the timing of the NIT deployment in this particular case affects the probable cause analysis.

misstatements. **[*22]** Docket No. 48 at 24. Because the government concedes that the images on the website changed in the two days prior to Agent Macfarlane submitting the search warrant application, the defendant no longer seeks a Franks hearing. See Docket No. 65 at 5 n.4. However, the defendant continues to assert that the affidavit should be reformed to account for the incorrect description of the site's appearance and that probable cause should be assessed with respect to the reformed affidavit. See Docket No. 65 at 5.

The defendant has not proven that the affiant knowingly or recklessly included the incorrect description of the homepage. As other district courts have noted, Agent Macfarlane visited the website two days prior to submitting the warrant application and he verified that the site appeared as described in his affidavit. Macfarlane was not reckless in failing to check the site again in the hours prior to presenting the application to the magistrate judge. See Matish, 2016 WL 3545776, at *12 ("The Court also finds that it was not reckless for the affiant not to examine the website one more time on the day he sought the warrant's authorization, as he had recently examined the website and confirmed that nothing had changed."); **[*23]** Darby, 2016 WL 3189703, at *9 ("There is nothing reckless about relying on a visit to the website on February 18, 2015 when describing the website for a warrant signed and executed on February 20, 2015.").

Nor has the defendant demonstrated that probable cause would have been lacking had the affidavit described the site as it appeared on February 20, 2015. See Matish, 2016 WL 3545776, at *12 (holding that 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, 2016 WL 3189703, at *9 ("[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.").

III. Particularity

The defendant argues that the search warrant was a general warrant and that it was insufficiently particular. The government responds that the **[*24]** search warrant amply described both the places to be searched and the items to be seized.

"We begin with the basic proposition that the Warrant Clause of the *Fourth Amendment* prohibits the issuance of a warrant, except one 'particularly describing the place to be searched, and the persons or things to be seized.'" *United States v. Tiem Trinh, 665 F.3d 1, 15 (1st Cir. 2011)* (quoting *U.S. Const. amend. IV*). "Any search intruding upon that privacy interest must be justified by probable cause and must satisfy the particularity requirement, which limits the scope and intensity of the search." *United States v. Bonner, 808 F.2d 864, 867 (1st Cir. 1986)*.

Every court to consider this question has found the NIT search warrant sufficiently particular. See Acevedo-Lemus, 2016 WL 4208436, at *7 n.4 ("Defendant's alternative argument -- that the NIT Warrant failed the *Fourth Amendment's* particularity requirement -- is without merit. That argument has been rejected, as near as the Court can tell, by every federal court to consider it."). This Court agrees and finds that the warrant is "sufficiently particular as it specifies that the NIT search applies only to computers of users accessing the website, a group that is necessarily actively attempting to access child pornography." United States v. Henderson, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at *4 (N.D. Cal. Sept. 1, 2016).

IV. Anticipatory Warrant

The defendant contends that the warrant was an

anticipatory warrant in which **[*25]** the triggering event did not occur. The defendant defines the triggering event as accessing the Playpen website as it was described in the affidavit, with the images of two partially clothed girls. The government counters that the triggering event was simply the act of logging into the site.

For "a conditioned anticipatory warrant to comply with the *Fourth Amendment's* requirement of probable cause, two prerequisites of probability must be satisfied." *United States v. Grubbs, 547 U.S. 90, 96 (2006)*. "It must be true not only that if the triggering condition occurs 'there is a fair probability that contraband or evidence of a crime will be found in a particular place,' but also that there is probable cause to believe the triggering condition will occur." *Id. at 96-97* (quoting *Gates, 462 U.S. at 238*). "The supporting affidavit must provide the magistrate with sufficient information to evaluate both aspects of the probable-cause determination." *Id. at 97*.

The Court concludes that "logging into Playpen -- which the warrant application identified by its URL -- represents the relevant triggering event." Matish, 2016 WL 3545776, at *15. When a user opened a Tor browser, located the Playpen site, created an account and password, and logged on, the triggering condition was satisfied as there was a fair probability that the user sought **[*26]** to access child pornography. The anticipatory warrant complied with the *Fourth Amendment*.

V. *Rule 41(b)*

The defendant urges the Court to find that, even if there was probable cause for the NIT search warrant, the magistrate judge in the Eastern District of Virginia lacked authority under *Rule 41(b)* to issue it. The government responds that the magistrate judge had the power to issue the warrant under subsections (b)(1), (b)(2), and (b)(4).

Federal Rule of Criminal Procedure 41(b) states in relevant part:

> At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> . . .
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize **[*27]** use of the device to track the movement of a person or property located within the district, outside the district, or both;

Fed. R. Crim. P. 41(b)(1)-(2), (4).

Rule 41(b)(1) is inapposite. The defendant's computer was not in the Eastern District of Virginia, where the magistrate judge issued the warrant. *Rule 41(b)(2)* does not apply either because the defendant and his property were not within the district when the warrant was issued.

Rule 41(b)(4) presents a closer call. See Henderson, 2016 WL 4549108, at *3 ("There is a stronger argument that the NIT Warrant is permissible under *Rule 41(b)(4)* . . . ."). Agent Macfarlane stated that the NIT "would augment" the content that a user downloads from the Playpen website, which was located on a server in the Eastern District of Virginia, "with additional computer instructions." Macfarlane Aff. ¶ 33, Docket No. 48, Ex. 2. After the defendant downloaded those instructions from the server in Virginia to his home computer in

Massachusetts, the NIT would instruct the defendant's computer to transmit certain identifying information back to the government.

Some district courts have found that the NIT constituted a tracking device and the magistrate judge was within her authority under *Rule 41(b)(4)* to issue the warrant. See Matish, 2016 WL 3545776, at *17; Darby, 2016 WL 3189703, at *12 ("Users of Playpen digitally touched down in the **[*28]** Eastern District of Virginia when they logged into the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government about their location."); see also United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *6 (D. Neb. Aug. 5, 2016) ("*Rule 41(b)(4)* authorizes the magistrate judge to issue a warrant such as the NIT warrant issued in this case. That provision authorizes the use of a tracking device and the NIT is analogous to a tracking device.").

However, other courts have found the NIT warrant does not satisfy *Rule 41(b)(4)*. See Henderson, 2016 WL 4549108, at *3. These courts have either concluded that the NIT was installed outside of the Eastern District of Virginia or that it functionally differed from a tracking device in that it did not merely relay location data. See *id. at *4* ("The NIT . . . falls outside the meaning of a 'tracking device' as contemplated by the rule. Further, the NIT was installed outside of the district, at the location of the activating computers, not within the district as required by *Rule 41(b)(4)*."); Adams, 2016 WL 4212079, at *6 ("Moreover, the NIT does not track; it searches. As discussed above, the NIT is designed to search the user's computer for certain information, including **[*29]** the IP address, and to transmit that data back to a server controlled by law enforcement.").

Because the NIT relays more than just the location of a user's computer, the Court concludes the NIT is probably not a tracking device within the meaning of *Rule 41(b)(4)*, but it is certainly similar to a tracking device. Because this is such a close call, the Court ultimately concludes that the good faith exception applies even if issuance of the search warrant did not comply with *Rule 41(b)*.

VI. Good Faith Exception

As a preliminary matter, the First Circuit has not decided whether a failure to comply with *Rule 41(b)* is a ministerial, technical violation -- as the government argues -- or if it rises to the level of a constitutional violation -- as the defendant claims.

If the violation is merely technical, suppression is not warranted unless the defendant can demonstrate prejudice. *United States v. Burgos-Montes, 786 F.3d 92, 109 (1st Cir.)*, cert. denied, *136 S. Ct. 599 (2015)* (finding that a violation of subsection (e) is ministerial and stating that suppression requires prejudicial error); *Bonner, 808 F.2d at 869* (finding that a violation of subsection (f)(1)(C) is ministerial and stating that suppression requires prejudicial error). Other circuits have adopted a similar rule. See *United States v. Krueger, 809 F.3d 1109, 1113 (10th Cir. 2015)* ("[W]e typically proceed by determining whether that specific *Rule 41* violation rises to **[*30]** the level of a *Fourth Amendment* violation. . . . Unless the defendant can establish prejudice or intentional disregard of the Rule, a non-constitutional violation of *Rule 41* will not, by itself, justify suppression."); *United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000)* (internal citations omitted) ("There are two categories of *Rule 41* violations: those involving constitutional violations, and all others. The violations termed 'ministerial' in our prior cases obviously fall into the latter category."). If the violation is constitutional, no additional prejudicial showing is required. Even constitutional violations, however, do not merit suppression in all cases. *Herring v. United States, 555 U.S. 135, 140 (2009)* ("The fact that a *Fourth Amendment* violation occurred -- i.e., that a search or arrest was unreasonable -- does not necessarily mean that the exclusionary rule applies.").

Most courts have found that, even if the magistrate judge violated *Rule 41(b)* in issuing the NIT warrant, there was no constitutional infirmity. See Henderson, 2016 WL 4549108, at *4 ("The NIT Warrant's violation of *Rule 41* is technical because the Warrant complies with the *Fourth Amendment* requirements of probable cause and particularity."); Adams, 2016 WL 4212079, at *6 ("The Court views a *Rule 41(b)* violation to be a technical or procedural violation."); United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016) ("[T]he NIT Warrant did not fail for constitutional reasons, **[*31]** but rather was the product of a technical violation of *Rule 41(b)*.").

As explained above, the Court finds that there was probable cause to issue this warrant and that the warrant was sufficiently particular. There was no *Fourth Amendment* violation here and suppression is not warranted. Even if *Rule 41(b)* was violated and even if that violation was of the constitutional variety, the Court concludes that the good faith exception would apply. See *United States v. Leon, 468 U.S. 897, 922 (1984)* ("We conclude that the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion.").

"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." *Burgos-Montes, 786 F.3d at 109* (quoting *Bonner, 808 F.2d at 867*). "Indeed, exclusion 'has always been our last resort, not our first impulse.'" *Herring, 555 U.S. at 140* (quoting *Hudson v. Michigan, 547 U.S. 586, 591 (2006)*). The Supreme Court has "repeatedly rejected the argument that exclusion is a necessary consequence of a *Fourth Amendment* violation." *Id. at 141*. For the exclusionary rule to apply, "the benefits of deterrence must outweigh the costs." Id.

The Court has already found that it is a close call whether **[*32]** this warrant complied with *Rule 41(b)*. See also Michaud, 2016 WL 337263, at *6 ("The Court must conclude that the NIT Warrant did technically violate *Rule 41(b)*, although the arguments to the contrary are not unreasonable and do not strain credulity."). 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. See *Leon, 468 U.S. at 922*. Most district courts to consider this question have reached this same conclusion. See 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, 2016 WL 3189703, at *14 ("[T]here is no evidence that any failure by the FBI to understand the intricacies of the jurisdiction of federal magistrates was deliberate."); Werdene, 2016 WL 3002376, at *15 ("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 defendant contends that exclusion is warranted because the warrant here was void ab initio, arguing **[*33]** that Leon's good faith exception only applies to a "subsequently invalidated" search warrant. See *Leon, 468 U.S. at 922*. The defendant relies principally on United States v. Levin, No. CR 15-10271-WGY, 2016 WL 2596010, at *10 (D. Mass. May 5, 2016) (Young, J.). The Levin court concluded that the magistrate judge did not have authority to issue the NIT warrant and that it was void ab initio. *Id. at *15*. Noting that whether "the good-faith exception applies where a warrant was void is a question of first impression in [the First Circuit], and an unresolved question more broadly," the court concluded that the exception did not apply. *Id. at *10*. At least three other district courts have subscribed to the Levin court's reasoning and

found the good faith exception inapplicable to a warrant deemed void ab initio. See United States v. Croghan, No. 1:15-CR-48, 2016 WL 4992105, at *6 (S.D. Iowa Sept. 19, 2016) ("For the same reasons asserted in Levin, however, the Court finds that Leon is inapplicable to issuance of the NIT Warrant because the NIT Warrant was issued without jurisdiction and was, therefore, void ab initio."); United States v. Workman, 15-cr-00397-RBJ, slip op. at 12-15 (D. Colo. Sept. 6, 2016); United States v. Arterbury, No. 15-CR-182-JHP, slip op. at 25 (N.D. Okla. Apr. 25, 2016).

The Court holds that the warrant here was not void ab initio. See Adams, 2016 WL 4212079, at *6. Even if the magistrate judge in the Eastern District of **[*34]** Virginia lacked the authority to issue a warrant that allowed the FBI to deploy the NIT outside of that district, the magistrate judge did have authority to issue a warrant in which the NIT deployed in that district. The warrant was not void at its issuance. Even if it had been, the Court concludes that the good faith exception would apply and that suppression would not be warranted. See *Herring, 555 U.S. at 144* ("To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system."); *United States v. Master, 614 F.3d 236, 241-42 (6th Cir. 2010)* (stating that the court's earlier holding that the good faith exception did not apply to warrants that were void ab initio was no longer "viable in light of more recent Supreme Court cases" such as Herring); United States v. Ammons, No. 3:16-CR-00011-TBR-DW, 2016 WL 4926438, at *8 (W.D. Ky. Sept. 14, 2016) ("The Court holds that the good-faith exception is not foreclosed where the warrant relied upon is void ab initio."); Eure, 2016 WL 4059663, at *8 ("[E]ven if *Rule 41(b)* did not allow the magistrate judge to issue the NIT warrant, suppression would not be justified because the actions of the law enforcement officers in this case were not sufficiently culpable."); Werdene, 2016 WL 3002376, at *14 ("The good **[*35]** faith exception is not foreclosed in the context of a warrant that is void ab initio . . . .").

ORDER

The defendant's motion to suppress (Docket No. 47) is **DENIED**.

/s/ PATTI B. SARIS

Patti B. Saris

Chief United States District Judge

End of Document