IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

UNITED STATES OF AMERICA,	§	
	§	
v.	§	
	§	
ZACHARY AUSTIN HALGREN,	§	No. SA-16-CR-008-XR
	§	
Defendant.	§	
	§	
	§	
	§	

ORDER

Defendant is charged with receipt of child pornography and possession of child pornography. Defendant seeks to suppress the evidence in this case. The motion is denied.

Background

In December 2014, the Government became aware of a website named Playpen that contained child pornography. One of the servers for that website was in North Carolina. Ultimately the Government seized that server pursuant to a warrant, relocated the server to Virginia, and assumed the role of administrator. When the Government was unable to identify the identity of the approximate 150,000 members of the website, the Government obtained a warrant on February 20, 2015 to deploy Network Investigative Technique (NIT) malware. The warrant authorized the search for persons located in the Eastern District of Virginia. The malware, however, reached all computers accessing the website, including Defendant Halgren's computer in San Antonio, Texas.

Through the malware the Government discovered that a user named "Platch" accessed the site, and the Government discovered the IP address associated with "Platch." Defendant Halgren was the user associated with the IP address.

On December 15, 2016, the Government sought a search warrant for the Defendant's home, computers, and car. When the warrant was executed agents questioned Halgren and he gave incriminating statements in response to the questions. He was arrested eight days later.

Motion to Suppress

Defendant argues that the deployment of the NIT malware was a search for Fourth Amendment purposes and that the NIT warrant lacked particularity. The defendant argues that the NIT warrant should have described with particularity the place to be searched. The NIT warrant, however, captured information from thousands of computers in 120 countries.

Alternatively, Defendant argues that the NIT warrant was issued in violation of the Federal Magistrate Act and former Federal Rule of Criminal Procedure 41 because an Eastern District of Virginia warrant was used to search a computer located in the Western District of Texas. Defendant further argues that since the Magistrate Judge lacked jurisdiction to issue the NIT warrant, the NIT warrant was void from inception.

Further, Defendant argues that the affiant for the search warrant of his home made false statements in his affidavit.

Analysis

A. The NIT warrant did not lack particularity.

The Magistrate Judge signed a warrant that authorized in Attachment A (Place to be Searched) that a NIT be deployed on the computer server already seized by the Government ("The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL . . . ."). The Magistrate Judge further identified in Attachment A of her Warrant that the NIT was to be deployed to obtain information as that term was defined in Attachment B from "activating computers."

"Activating computers" was defined as "those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password." Attachment B of the Warrant authorized the seizure of any activating computer's actual IP address and other specific information that was evidence of any receipt, access, or distribution of child pornography.

As recognized by many courts, "Playpen operated on 'the onion router' or 'Tor' network." *United States v. Matish*, 193 F. Supp. 3d 585, 593 (E.D. Va. 2016). Individuals download the Tor browser from the Tor website. The "Tor network possesses two primary purposes: (1) it allows users to access the Internet in an anonymous fashion and (2) it allows some websites—hidden services—to operate only within the Tor network. Although a website's operator usually can identify visitors to his or her site through the visitors' Internet Protocol ("IP") addresses, Tor attempts to keep a user's IP address hidden." *Id.* at 593–94.

Regarding the Defendant's first argument that the warrant lacked particularity, this court agrees with the *Matish* court that the NIT Warrant did not violate the Fourth Amendment's particularity requirement. The warrant was not broader than the probable cause upon which it was based. There existed a fair probability that anyone accessing Playpen possessed the intent to view and trade child pornography. In the affidavit in support of the application for search warrant, the FBI Special Agent/affiant described how agents connected to the Tor browser and entered the URL address for the website suspected of storing and distributing child pornography. The affiant described how a user must know the exact URL address for a site, because the Tor network does not operate with traditional search engine sites, such as Google. He described that only registered users were allowed to access the Playpen website. If a user registered an account a warning was given not to enter a real address. After successfully registering, forums and sub-forums were available that described various "jailbait" and pre-teen videos and photos. Other

forums were also available that addressed rules, security, general discussion, kinky fetishes and fiction and non-fiction stories. The affiant described that upon entering the site agents found images and files of child pornography. Further, the warrant explicitly outlined the place to be searched—the computers of any user or administrator who logs into Playpen. The warrant also detailed the items to be seized. Therefore, the NIT Warrant met the Fourth Amendment's particularity requirements. *Id.* at 608–09; *see also United States v. Anzalone*, 208 F. Supp. 3d 358, 368 (D. Mass. 2016) ("Every court to consider this question has found the NIT search warrant sufficiently particular.").

B. The E.D. Va. Magistrate Judge was not authorized to sign the NIT warrant.

Former Federal Rule of Criminal Procedure 41(b)[1] and the Federal Magistrates Act, 28 U.S.C. Section 636, address the scope of a Magistrate Judge's authority.[2] In rejecting the

[1] Fed. R. Crim. P. 41(b)(6) was amended effective December 1, 2016. The amended rule

> provides that in two specific circumstances a magistrate judge in a 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 seize or copy electronically stored information even when that media or information is or may be located outside of the district.
>
> First, subparagraph (b)(6)(A) provides authority to issue a warrant to use remote access within or outside that district when the district in which the media or information is located is not known because of the use of technology such as anonymizing software.
>
> Second, (b)(6)(B) allows a warrant to use remote access within or outside the district in an investigation of a violation of 18 U.S.C. § 1030(a)(5) if the media to be searched are protected computers that have been damaged without authorization, and they are located in many districts. Criminal activity under 18 U.S.C. § 1030(a)(5) (such as the creation and control of "botnets") may target multiple computers in several districts. In investigations of this nature, the amendment would eliminate the burden of attempting to secure multiple warrants in numerous districts, and allow a single judge to oversee the investigation.

FED. R. CRIM. P. 41(b)(6) advisory committee's note to 2016 amendment.

[2] Courts across the country are split on the issue of whether the Magistrate Judge in the NIT warrant had authority to issue the warrant. *See United States v. Taylor*, No. 216CR00203KOBJEO1, 2017 WL 1437511, at *3–4 (N.D. Ala. Apr. 24, 2017) ("As of today, at least 44 district courts have ruled on motions to suppress the information seized pursuant to the NIT warrant. Twelve of these courts have found that the warrant did not violate § 636(a) of the Federal Magistrates Act and/or Rule 41 of the Federal Rules of Criminal Procedure. [citations omitted]. Twenty-two district courts have found that the warrant did violate § 636(a) and/or Rule 41(b), but that the violation did not warrant suppression. [citations omitted]. A few courts have declined to decide whether the statute and/or the Rule

argument advanced by the Government that defendants make a "virtual" trip to the Eastern District of Virginia to access child pornography and that investigators "installed" the NIT within that district, the Eighth Circuit has recently stated: "Although plausible, this argument is belied by how the NIT actually worked: it was installed on the defendants' computers in their homes [outside the Eastern District of Virginia]." *United States v. Horton*, 863 F.3d 1041, 1047–48 (8th Cir. 2017) (holding that the NIT warrant exceeded the magistrate judge's jurisdiction). This Court agrees with the Eighth Circuit and the majority of courts that have considered the issue.

Magistrate Judges have authority "within the district in which sessions are held by the court that appointed the magistrate judge . . . and elsewhere as authorized by law." 28 U.S.C. § 636(a). Former Rule 41 that was in effect in 2015 authorized a Magistrate Judge "to issue a warrant to search for and seize a person or property located within the district." FED. R. CRIM. P. 41(b)(1) (2015). The Former Rule 41 provided "exceptions to this jurisdictional limitation for property moved outside of the jurisdiction, for domestic and international terrorism, for the installation of a tracking device, and for property located outside of a federal district. None of these exceptions [in 2015] expressly allow[ed] a magistrate judge in one jurisdiction to authorize the search of a computer in a different jurisdiction." *Horton*, 863 F.3d at 1047 (footnote omitted); *But see United States v. Darby*, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016) ("Rule 41(b)(4) allows a magistrate judge to issue a warrant for a tracking device to be installed in the magistrate's district. Once installed, the tracking device may continue to operate even if the object tracked moves outside the district. This is exactly analogous to what the NIT Warrant authorized. Users of Playpen digitally touched down in the Eastern District of Virginia when

---

authorized the warrant but found that exclusion was unwarranted regardless. [citations omitted]. Four courts have suppressed the evidence. [citations omitted].").

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. The magistrate judge did not violate Rule 41(b) in issuing the NIT Warrant.")[3]

C. However, even if the E.D. Va. Magistrate Judge lacked authority to sign the NIT warrant, the Defendant lacked a reasonable expectation of privacy in his IP address when using the Internet and accessing the Playpen website.

Given that the Defendant's IP address was required to be disclosed to various third parties and Playpen to access the website, any subjective expectation of privacy the Defendant may have possessed was not objectively reasonable. *See United States v. Weast*, 811 F.3d 743, 747 (5th Cir.), *cert. denied*, 137 S. Ct. 126 (2016) (adopting the holding that "[f]ederal courts have uniformly held that subscriber information provided to an internet provider, including IP addresses, is not protected by the Fourth Amendment's privacy expectation because it is voluntarily conveyed to third parties." (internal quotations omitted)); *Matish*, 193 F. Supp. 3d at 616.[4]

Defendant asserts that the NIT malware also intercepted his user name and that he had a reasonable expectation of privacy in that piece of information. Because the Court concludes that the *Leon* exception will apply in this case, the Court does not reach any conclusion regarding whether a reasonable expectation of privacy existed in the user name.

D. *Leon* exception applies.

[3] *But see United States v. Levin*, 186 F. Supp. 3d 26, 34 (D. Mass. 2016) (holding that neither the Federal Magistrates Act nor former Rule 41(b) authorized the issuance of the NIT Warrant).

[4] Some courts have found to the contrary finding that individuals have a reasonable expectation of privacy in the data stored on their personal computers. Respectfully, while there should be little disagreement on that point, this is not the fundamental issue. The issue is once a person voluntarily transmits his IP address to a third party, does that person retain that reasonable expectation of privacy?

Alternatively, even if Defendant had a reasonable expectation of privacy in his IP address and the Magistrate Judge lacked authority to sign the NIT warrant, suppression of this evidence is not required because the *Leon* good faith exception applies in this case. The agents' reliance on the NIT Warrant was objectively reasonable, and the agents acted in good faith. An experienced and neutral Magistrate Judge reviewed the warrant application and concluded that there existed probable cause to issue the NIT Warrant. *United States v. Workman*, 863 F.3d 1313, 1317 (10th Cir. 2017) (motion to suppress reversed; even if the warrant had been invalid, the *Leon* exception would still apply); *Horton*, 863 F.3d at 1052 (applying the *Leon* exception despite the warrant being void ab initio); *Matish*, 193 F. Supp. 3d at 593; *Darby*, 190 F. Supp. 3d at 536; *Anzalone*, 208 F. Supp. 3d at 372 ("Even if the magistrate judge in the Eastern District of 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."); *but see Levin*, 186 F. Supp. 3d at 44 (NIT Warrant was issued without jurisdiction and thus was void ab initio and the good-faith exception is inapplicable). This Court disagrees with *Levin* and the three or four other courts that have ordered suppression. If a judge signed a warrant without the necessary probable cause determination that warrant was akin to being void. But if an officer reasonably relies upon that signing and acts in good faith, *Leon* holds that the evidence seized should not be suppressed.

E. Affidavit used to establish probable cause for the search of Halgren's residence did not contain misrepresentations.

In the 33-page affidavit in support of the application for a search warrant, FBI Special Agent Jeffrey Allovio stated that individuals must download software to access the Tor network,

and that once an individual has done so, a user must know the exact address of the website he wants to access because the Tor network does not perform traditional Google-type searches. He further stated that the Tor network attempts to conceal a user's IP address "by bouncing their communications around a distributed network of relay computers . . . ." Docket no. 42-2 at 31. He restated how one of the Tor servers had been seized and, pursuant to the NIT warrant, law enforcement officials became aware of a user known as "Platch." He also stated that the main page for Playpen consisted of "two images depicting partially clothed prepubescent girls with their legs spread apart, along with text underneath stating, 'No cross-board reposts . . . .'" *Id.* Det. Allovio stated that no "cross-board" referred to a prohibition against material that is posted on other websites from being re-posted to Playpen. The Playpen main page also contained a warning that only registered members were allowed access and a login was required. Det. Allovio also stated that if an individual was registering an account for the first time, Playpen warned individuals not to post information that can be used to identify a user. Det. Allovio proceeded to detail the images of children being sexually abused, posed nude or partially nude, or lasciviously exposing their genitals that were found once a user entered various sections, forums, and sub-forums. Det. Allovio stated that it had been determined that "Platch" had accessed the Playpen site between January 27, 2015 and March 4, 2015. Through the NIT deployment, an IP address associated with "Platch" had been discovered, "Platch" used the Playpen logon name of "SaintRoshi", and "Platch" had accessed images of a nude prepubescent female in sexually suggestive positions and images of her being sexually assaulted by an adult male. Det. Allovio further stated that Patch's IP address was operated by Time Warner Cable, an Internet Service Provider, and that the account belonged to Pht RITTIMAN LLC at 5710 Industry Park Drive, San Antonio, Texas. The location was a Travel Inn. Agents uncovered that

the name "Saint Roshi" had been used on social networking sites by Zachary Austin Halgren. When law enforcement officials attempted to locate Halgren, they became aware he no longer resided at the Travel Inn, but they uncovered his telephone number. A tracking warrant was issued for the telephone number and it was uncovered that the phone number was routinely being operated from 8302 Morning Grove, Converse, Texas. Surveillance was then conducted at the premises and it was established that Halgren was residing there. Based upon this information the Magistrate Judge signed a search and seizure warrant that authorized the search of 8302 Morning Grove, a 1997 Chevrolet pick-up truck being used by Halgren, and Halgren's phone.

Defendant argues that Det. Allovio falsely misrepresented that evidence of "Platch" would be found on his computer. He argues that based upon how Tor worked Det. Allovio knew that it was unlikely that there would exist any evidence of Halgren's activity on the Playpen site.

As stated recently by the Fifth Circuit in *United States v. Ortega*, "a search warrant must be voided if the defendant shows by a preponderance of the evidence that the affidavit supporting the warrant contained a false statement made intentionally or with reckless disregard for the truth and, after setting aside the false statement, the affidavit's remaining content is insufficient to establish probable cause." 854 F.3d 818, 826 (5th Cir. 2017) (citing *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978)). The *Franks* inquiry requires the court to ask three questions:

> First, does the affidavit contain a false statement? *See, e.g.*, *States v. Singer*, 970 F.2d 1414, 1416–17 (5th Cir. 1992) (affirming denial of motion to suppress because affidavit's statement was not false). Second, was the false statement made intentionally or with reckless disregard for the truth? *See, e.g.*, [*United States v. Looney*, 532 F.3d 392, 394–95 (5th Cir. 2008)] (affirming denial of motion to suppress because affiant officer did not intentionally or recklessly include the false statement). And third, if the false statement is excised, does the remaining content in the affidavit fail to establish probable cause?

Id. at 826.

"In determining whether probable cause exists without the false statements a court must 'make a practical, common-sense decision as to whether, given all the circumstances set forth in the affidavit [minus the alleged misstatements], there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Id*. at 828.

Because there was evidence that Halgren accessed the Playpen site, even if the affidavit incorrectly stated evidence of access to Playpen could be found on Halgren's computer, there was a practical, common-sense decision that there was a fair probability that Halgren likely downloaded images or videos of child pornography to his computer.

F. Suppression of incriminating statements.

Defendant argues that since the Virginia warrant should never have been issued, any incriminating statements he later made in San Antonio should be suppressed. Inasmuch as the Court concludes that the *Leon* exception applies in this case, this argument is also rejected.

Conclusion

Defendant's motion to suppress (docket no. 42) is denied.

SIGNED this 30th day of August, 2017.

XAVIER RODRIGUEZ
UNITED STATES DISTRICT JUDGE