UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 4:16-cr-00018-TWP-VTW
	)	
ADRIAN GRISANTI (01),	)	
	)	
Defendant.	)	

ENTRY ON MOTION TO SUPPRESS

This matter is before the Court on Defendant Adrian Grisanti's ("Grisanti") Motion to Suppress (Filing No. 27). Grisanti is charged with two counts of Receipt of Child Pornography in violation of 18 U.S.C. § 2252A(a)(2)(A), seven counts of Knowing Access with Intent to View Child Pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), one count of Knowing Possession of material containing Child Pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), and one count of Destruction of Evidence in violation of 18 U.S.C. § 1519. (Filing No. 1.) Grisanti petitions the Court to suppress any and all evidence obtained from a search of a computer located at his place of employment, Our Place Drug and Alcohol Services ("Our Place"), through the Federal Bureau of Investigation's ("FBI") deployment of a Network Investigative Technique ("NIT"). He asserts the evidence collected should be suppressed because the magistrate judge overstepped her authority in issuing the warrant and there was no probable cause for the search warrant. For the reasons set forth below, the Court **DENIES** the Motion to Suppress.

I. BACKGROUND

In September 2014, the FBI began an investigation into a global online forum called "Playpen" which was dedicated to the advertisement, distribution, receipt and collection of child

pornography through which registered users advertised, distributed, received, or accessed illegal child pornography. (Filing No. 35-6 at 16.) The scale of child sexual exploitation that occurred on the site contained more that 150,000 total members who collectively engaged in tens of thousands of postings related to child pornography. *Id.* Playpen, was hosted on The Onion Router ("TOR") network. TOR uses technology that provides anonymity to Internet users by masking user data, hiding Internet Protocol ("IP") addresses, and bouncing user communications around a distributed network of relay computers (called "nodes") (Filing No. 27 at 2). Playpen was set up as a "hidden service" within the TOR network. (Filing No. 35 at 5.) Thus, users could only reach "hidden services" if the user was using the TOR client software and operating in the TOR network. *Id.* Because the Playpen web server was hidden, in order to access the site a user would need to know Playpen's exact TOR-based web address, consisting of a series of algorithm-generated characters.

In February 2015, the FBI seized Playpen from its web-hosting facility in North Carolina and interdicted the site allowing it to continue to operate at a government facility located in the Eastern District of Virginia during a two-week period between February 20, 2015 and March 4, 2015. *Id.* at 7. During that time, the FBI obtained a warrant from a magistrate judge in the United States District Court for the Eastern District of Virginia, to monitor and identify anonymous site users through the use of NIT technology. (Filing No. 35-6.) The NIT consisted of computer instructions which, when downloaded (along with the other content of Playpen) by a registered user's computer, were designed to cause the user's computer to transmit a limited set of information. (Filing No. 35 at 8.) This information allowed the FBI to capture the computer's true IP address and other computer related data that would assist in identifying the computer used to access Playpen and its user. The Playpen investigation and execution of the NIT warrant resulted

in the identification and arrest of many individuals on child pornography-related crimes nationwide. *United States v. Brooks*, No. 16-CR-6028L, 2017 WL 3835884 at *9 (W.D. NY August 31, 2017).

In March 2015, the FBI filed an administrative subpoena on AT&T for an IP address belonging to Playpen registered user "THISISMEE222", which revealed that it belonged to a computer at Grisanti's place of employment, Our Place, located at 400 East Spring Street, New Albany, Indiana 47150. (Filing No. 27 at 2.) According to user profile records, this user was logged into Playpen for more than 9 hours and 13 minutes between January 28, 2015 and February 24, 2015. (Filing No. 35 at 9.) The FBI contacted the management at Our Place and learned that Grisanti was the sole user of the computer repeatedly accessing Playpen. On August 18, 2015, the FBI obtained a search warrant from the United States District Court for the Southern District of Indiana for Grisanti's work computer (Filing No. 35 at 10). The computer's unique Media Access Control ("MAC") address, a feature of internal hardware, matched the one observed on Playpen. *Id*. The FBI conducted a search after business hours on August 18, 2015, but agents were only able to complete a limited forensic analysis using a triage search tool. The next day, August 19, 2015, the FBI obtained additional search warrants from this District and the Western District of Kentucky to search not only Grisanti's work computer, but also his person, residence, and vehicle. (Filing No. 35-3; Filing No. 35-4; Filing No. 35-5.) Upon returning, the FBI found the computer in Grisanti's car trunk with the hard drive missing. *Id.* The FBI also found a smashed thumb drive in the dumpster of the business. *Id*. Subsequent forensic analysis found child pornography on the devices recovered from Grisanti's residence, including common files found between THISISMEE222 user's activity records and his work computer (Filing No. 35 at 10). Thereafter, Grisanti was indicted for receiving child pornography from Playpen in violation of 18 U.S.C. §

2252A(a)(2)(A), and one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). *Id.*

II. LEGAL STANDARD

The Fourth Amendment provides,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. "If the search or seizure was effected pursuant to a warrant, the defendant bears the burden of proving its illegality." *United States v. Longmire*, 761 F.2d 411, 417 (7th Cir. 1985). In reviewing the issuance of a search warrant:

> a magistrate's determination of probable cause…should be overruled only when the supporting affidavit, read as a whole in a realistic and common sense manner, does not allege specific facts and circumstances from which the magistrate could reasonably conclude that the items sought to be seized are associated with the crime and located in the place indicated.

United States v. Norris, 640 F.3d 295, 300 (7th Cir. 2011) (quoting *United States v. Spry*, 190 F.3d 829, 835 (7th Cir. 1999)). Instead of focusing on technical aspects of probable cause, the reviewing court should consider all facts presented to the magistrate. *United States v. Lloyd*, 71 F.3d 1256, 1262 (7th Cir. 1995). And "[w]here the police have acted pursuant to a warrant, the independent determination of probable cause by a magistrate gives rise to a presumption that the arrest or search was legal." *Id.* Probable cause affidavits supporting applications for warrants are to be "read as a whole in a realistic and common sense manner," and "doubtful cases should be resolved in favor of upholding the warrant." *United States v. Quintanilla*, 218 F.3d 674, 677 (7th Cir. 2000) (citation omitted). A judge determines probable cause exists to search when the "known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband

or evidence of a crime will be found." *Ornelas v. U.S.*, 517 U.S. 690, 696 (1996) (citations omitted). "When a search is authorized by a warrant, deference is owed to the issuing judge's conclusion that there is probable cause." *U.S. v. Sutton*, 742 F.3d 770, 773 (7th Cir. 2014).

III. DISCUSSION

Grisanti does not challenge the accuracy of the information articulated by law enforcement in any of the warrants and there are no disputed factual issues. Neither party requested a hearing on the motion to suppress and the Court is able to rule on the motion without a hearing. "District courts are required to conduct evidentiary hearings only when a substantial claim is presented and there are disputed issues of material fact that will affect the outcome of the motion." *United States v. Curlin*, 638 F.3d 562, 564 (7th Cir. 2011).

Grisanti moves to suppress all evidence seized from his office computer at Our Place, asserting that issuance of the NIT warrant violated Section 636(a) of the Federal Magistrate Act and Federal Rule of Criminal Procedure 41(b). Specifically, he asserts that the magistrate judge exceeded her authority when she authorized the deployment of the NIT which reached computers outside of her geographic jurisdiction. He also asserts that the deployment of the NIT lacked probable cause and violated the Fourth Amendment.

As an initial matter, the Court notes that the validity of this particular NIT warrant has been the subject of numerous defense challenges and dozens of decisions throughout the country. See *United States v. Brooks*, No. 16-CR-6028L, 2017 WL 3835884 at *9 (W.D. NY August 31, 2017) (citations omitted). "More than 40 district courts have held hearings regarding suppression of evidence generated from the NIT." *United States v. Horton*, 863 F.3d 1041, 1045-46 (8th Cir. 2017) (citations omitted). Most district courts that have heard these suppression motions have denied them, and of the few that have granted suppression some of those were later reversed at the

appellate level. *See id*. (citations omitted). *United States v. Workman*, 863 F.3d 1313, 1314 (10th Cir. 2017). This Court will first determine whether probable cause existed and then examine the magistrate judge's authority.

A. The Network Investigative Technique (NIT) Warrant

Grisanti argues there was a lack of probable cause to support the Playpen search warrants and the affidavits in support of the search warrants violated the particularity requirements of the Fourth Amendment. In particular, he asserts that because the TOR network masked his identity, the FBI could not have had probable cause that he was allegedly conducting criminal activities prior to the issuance of the NIT warrant which was necessary to first identify Playpen users, therefore probable cause was lacking as it relates specifically to him. (Filing No. 27 at 8.) The Government responds that the NIT affiant, a 19-year FBI veteran who regularly investigates federal child pornography violations, affirmatively articulated that due to the numerous affirmative steps required for a user to find and access Playpen, there was probable cause to believe that "any user who successfully accesse[d] the website had, at a minimum, 'knowingly accessed with intent to view child pornography or attempted to do so.'" (Filing No. 35 at 23.)

"Several courts have found that the NIT warrant was supported by probable cause. The affidavit supporting the NIT warrant described the Playpen site, the TOR network, the NIT program, the offenses under investigation and definitions of technical terms." *United States v. Dorosheff*, Case No. 16-30049, 2017 WL 1532267 at *4 (C.D. Ill. April 27, 2017) (citations omitted). "The main site page accordingly made it obvious that this was a website dealing with prepubescent minors, large files or sets of files, images that were not allowed to be posted elsewhere, and that it required both previews and encryption." (Filing No. 35 at 26.) "The affidavit described Playpen as a global online forum through which registered users distributed and accessed

child pornography. The affidavit describes the site's contents including details about its forum structure, which was organized by sexual interest, gender, and age." *Dorosheff*, 2017 WL 1532267 at *4. Although, the FBI did not have specific information identifying Playpen's users before NIT's deployment, at a minimum, the NIT warrant affidavit supported probable cause that Playpen's users intentionally concealed their identities in order to engage in illicit activity and NIT allowed law enforcement to identify those users. The magistrate's inference that registered Playpen users accessed the site with an intent to view child pornography supported a probable cause determination to authorize the use of the NIT to collect information that would identify Playpen users.

Along the same line of reasoning Grisanti poses regarding his lack of probable cause argument, he also argues that the warrant lacked particularity because the NIT would have gathered information on people who are "innocent"[1] whenever it captured users accessing the Playpen website who were not viewing child pornography (Filing No. 27 at 10). The Government responds that the site's use of the anonymous TOR network makes it highly unlikely that an innocent user would accidently reach the site and register an account to see its contents. (Filing No. 35 at 28.) Further, the landing page of Playpen depicted two images of partially clothed prepubescent females with their legs spread apart making it immediately apparent the illicit nature of the site to any user who was able to find the site (before actually registering an account). *Id.* at 13.

The Government cites *U.S. v. Froman*, where the Fifth Circuit affirmed a district court's holding of probable cause when a defendant subscribed to a readily apparent child pornography website. 355 F.3d 882, 889 (5th Cir. 2004) ("It was also common sense that a person who is a member of a group involved in the collection of child pornography would have child pornography

[1] Grisanti does not explicitly state how innocent users' information might be captured, but it can be assumed that the innocent users are the interconnected computers that the TOR network uses to mask users' identities.

from a number of sites. There was probable cause for the issuance of the search warrant.") (citation omitted). By the Fifth Circuit's same reasoning, the NIT warrant was sufficiently particular because it sent computer code to gather IP and MAC addresses of registered users of Playpen who accessed the site during the two-week period that the Government controlled the site.

> Attachments A and B of the NIT warrant, entitled "Place to be Searched," and "Information to be Seized," described with precise language exactly what would be searched and seized—the warrant authorized the NIT to be employed on the computer server hosting Playpen, in order to obtain specific information from computers of 'any user or administrator who logs into [Playpen] by entering a username and password.'

(Filing No. 35 at 32) (citation omitted). It would strain common sense to conclude that if an innocent user somehow reached Playpen's hidden website that the same user would then register an account when Playpen's landing page made it readily apparent that the site was a forum for accessing, viewing, and downloading child pornography. Unlike the District Court for the Southern District of Texas case that Grisanti cites, the NIT warrant specifically described how the NIT search technique would contact target computers/users because rather than searching interconnected computers through the TOR network, the NIT's deployment would ensure that only Playpen's registered users who accessed the site during the search would have code installed on their computers to identify its users. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 754, 758-59 (S.D. Texas 2013). The NIT also generated a unique identifier (MAC address) to distinguish data from that of other computers that might also be in the same general area as the Playpen users' computers (Filing No. 35 at 32). Further, as it relates specifically to the search warrant of Grisanti's office computer, the Government received confirmation that he was the only employee that used that computer; therefore, innocent users with similar IP addresses would not have been included in the NIT's search. The MAC address linked the Playpen user to a specific computer at Our Place. Because Playpen operated on a hidden

website and required users to register before entering a site contextually identifying itself as a forum for child pornography, the NIT search warrant was sufficiently particular to capture the IP and MAC addresses of those using Playpen for illegal activities. Accordingly, probable cause existed and suppression is not warranted for this reason.

B. The Magistrate Judge's Jurisdiction

Grisanti also argues the evidence must be suppressed because the magistrate judge exceeded her jurisdictional authority when she approved the initial search warrant. Congress established jurisdictional geographic limitations on the judicial authority of magistrate judges, which may be modified elsewhere as authorized by law. 28 U.S.C. § 636(a)(1). Fed. R. of Crim. P. 41(b) outlines in detail the requirements and powers of a magistrate judge when issuing a warrant at the request of a federal law enforcement officer or an attorney for the government. Rule 41(b)(1) gives federal magistrate judges authority "to search for or seize a person or property located *within*" their district. *Id*. (Emphasis added). Rule 41(b)(2) allows for the search or seizure of property that is located within the district, but might be moved prior to execution of the warrant. *Id*. Rule 41(b)(4) allows a magistrate judge to issue a warrant to install within the district a tracking device, which may track inside and outside of the district. *Id*. And, Rule 41(b)(6)(A)[2] provides that a magistrate judge has the authority, in any district where activities related to a crime may have occurred, "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 the district where the media or information is located has been concealed through technological means." *Id*.

[2] A 2016 Amendment now explicitly authorizes a magistrate judge with authority in any district where activities may have occurred to issue a warrant to use remote access to search electronic storage media located within or outside that district if the district where the media or information is located has been concealed through technological means. Fed. R. Crim. P. 41(b)(6)(A). However, this amendment occurred a year after Grisanti was indicted.

Grisanti argues that the magistrate judge's issuance of a warrant to search property outside of the Eastern District of Virginia violated the territorial restrictions provided in the Federal Magistrate Act. He relies, in part, on a holding from the Eighth Circuit in *United States v. Horton*, 863 F.3d 1041(8th Cir. 2017).

> When the NIT warrant was issued in this case, Federal Rule of Criminal Procedure 41 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). The rule 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 expressly allow a magistrate judge in one jurisdiction to authorize the search of a computer in a different jurisdiction.

Horton, 868 F. 3d at 1047.

The Government argues that the tracking device exception in Rule 41(b)(4) and property movement exception in Rule 41(b)(2) should apply here because Grisanti reached into the Eastern District of Virginia through a "virtual trip," where the Playpen site was being hosted, when he logged into Playpen and that the NIT tracking device was also installed in this district through the website (Filing No. 35 at 39). Grisanti contends that the NIT does not meet the definition of a tracking device which is defined under 18 U.S.C. § 3117(b) as "an electronic device which permits tracking of the movement of a person or object." He also argues that Rule 41(b)(2) does not apply because the property at issue, the computer at Our Place, was at all times located in Indiana and was never in the Eastern District of Virginia (Filing No. 27 at 5). In response, the government argues that the Playpen website was located in Virginia when the warrant authorizing the NIT was issued.

The Eighth Circuit rejected the tracking device exception based on how the NIT actually worked—it installed codes on user's computers located in districts outside of Eastern District of Virginia—which exceeded the magistrate judge's jurisdiction. *Horton*, 863 F. 3d at 1047-48

(agreeing with the majority of courts that have concluded that the plain language of Rule 41 and statutory definition of 'tracking device' do not support so broad a reading to encompass the mechanism of the NIT deployment used in this case). Similarly, this Court finds that even if Rule 41(b)(4) supported a broad reading of 'tracking device' it would not authorize an exception to the magistrate judge's jurisdictional limitations because the NIT in this instance was installed on users computers (property) outside of the Eastern District of Virginia.

This Court's sister court, the Central District of Illinois, held that Rule 41(b)(2) did not apply because the property to be searched through the deployment of the NIT, users' computers, were never located in the Eastern District of Virginia at any time including when the warrant was issued, thereby rejecting the government's argument that the relevant property was the Playpen website. *Dorosheff*, 2017 WL 1532267 at *6 (C.D. Ill. April 27, 2017) ("Rule 41(b)(2) granted the magistrate authority to issue a warrant to search the computers only of Playpen users whose *computers* were located in the Eastern District of Virginia" at the time of the warrant's issuance and later moved outside that district) (emphasis added). Similarly, Grisanti's computer was not located in Virginia at the time the magistrate judge authorized the warrant to search users' computers through the deployment of the NIT because it was located in Indiana at all times, and therefore the magistrate judge exceeded her authority.

Despite the NIT warrant exceeding the magistrate judge's jurisdictional limitations, suppression of the resulting evidence from the execution of the warrant is not warranted because the evidence is appropriately admissible under the good faith exception to the exclusionary rule established in *United States v. Leon*, 468 U.S. 897, 926 (1984). "[V]iolations 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." *U.S. v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008) (holding

that the violation of Rule 41 did not require suppression and that allowing the defendants "to go free [due to a procedural flaw] would be a remedy wildly out of proportion to the wrong."). "Nevertheless, the officer's reliance on the magistrate's probable-cause determination and on the technical sufficiency of the warrant he issues must be objectively reasonable." *Leon*, 468 U.S. 897 at 922-23.

Grisanti attempts to factually distinguish *Cazares-Olivas* by arguing that the law enforcement agents in that case had probable cause and the federal magistrate judge had jurisdiction over the district in which the search was executed despite not securing the physical warrant. The Court is not persuaded. *Cazares-Olivas* involved a violation of Rule 41's authorization of telephonic warrants that described a particular procedural process to be followed. Both the district court and the Seventh Circuit found that because the proper procedure for issuing a telephonic warrant was not followed, no warrant issued and the search was conducted in the absence of a warrant. *Id.* at 728. Although that case involved a violation of a different section of Rule 41, the Seventh Circuit casted a broad brush when it held violations of federal rules do not justify the exclusion of evidence seized on probable cause and generally characterized Rule 41 without regard for the specific section violated. *Id.* at 730. The same rationale articulated in *Cazares-Olivas* also applies to this case. Because there was probable cause for the NIT warrant, the good faith exception applies and the public interest in having juries receive all probative evidence of a crime outweighs the procedural error that occurred. The NIT warrant necessarily operated in a manner that implicated advanced technology and complicated procedural issues regarding magistrate's geographic jurisdictional limitations including exceptions; therefore, law enforcement agents would not have reasonable grounds to believe that the warrant was improperly issued and they acted in good faith.

In addition to the good faith exception, the Court agrees with the Government that the Seventh Circuit recognizes that federal courts have inherent power to issue search warrants consistent with the Fourth Amendment, in cases where the benefits of public safety are great and the costs to personal privacy are modest. See *United States v. Torres*, 751 F.2d 875 (7th Cir. 1984). In Torres, the court found "[t]here is no right to be let alone while assembling bombs in safe houses." *Id* at 883. Likewise, there is no right to be let alone while advertising, distributing, receiving and accessing illegal child pornography on TOR's hidden service.

Accordingly, suppression is not warranted despite any violation of Rule 41(b).

C. Suppression based on destroyed evidence

Finally, Grisanti argues the evidence should be suppressed because his expert could not examine the hard drive that was taken from the computer and destroyed between the time of the initial search on August 18, 2015 and the second search on August 19, 2015. Grisanti offers a computer forensics expert, Tami Loehrs ("Loehrs"), who signed an affidavit stating that his alleged accessing of Playpen cannot be corroborated because the hard drive does not exist. (Filing No. 27 at 3.) The Government responds that the hard drive does not exist because Grisanti criminally obstructed the investigation by destroying the evidence and that he is charged with that crime. (Filing No. 35 at 46.) Loehrs also opines that the NIT used software to exploit vulnerabilities in the TOR browser and that a computer exploited is a fundamental alteration that could be responsible for the activity that Grisanti is accused of committing. (Filing No. 27 at 3.) The Government has produced evidence that Grisanti was a registered user of Playpen before the NIT was deployed and that common child pornography images were recovered from his home computer in Kentucky establishing evidentiary links to Grisanti's Playpen activities on his work computer in Indiana. Grisanti is entitled to present his defense expert's testimony at trial, but it

does not provide a basis for suppression, particularly when it is alleged that he is the reason the evidence is unavailable. (Filing No. 35-1 at 20; Filing No. 35 at 47.)

IV. CONCLUSION

For the reasons set forth above, the Court **DENIES** Grisanti's Motion to Suppress (Filing No. 27).

SO ORDERED.

Date: 10/17/2017

TANYA WALTON PRATT, JUDGE
United States District Court
Southern District of Indiana

DISTRIBUTION:

Armand I. Judah
LYNCH, COX, GILMAN & GOODMAN, P.S.C.
ajudah@lynchcox.com

Bradley P. Shepard
UNITED STATES ATTORNEY'S OFFICE
brad.shepard@usdoj.gov