San Antonio Divison United States v. Torres

United States District Court for the Western District of Texas

September 09, 2016, Filed

No. 5:16-CR-285-DAE

Reporter
2016 U.S. Dist. LEXIS 122086

SAN ANTONIO DIVISON UNITED STATES OF AMERICA, Plaintiff, vs. JEFFREY JERRY TORRES, Defendant.

Notice: Decision text below is the first available text from the court; it has not been editorially reviewed by LexisNexis. Publisher's editorial review, including Headnotes, Case Summary, Shepard's analysis or any amendments will be added in accordance with LexisNexis editorial guidelines.

Opinion

[*1] ORDER DENYING MOTION TO SUPPRESS

This matter comes before the Court on Defendant Jeffrey Jerry Torres' Motion to Suppress Evidence (Dkt. # 23). The Court has considered Mr. Torres' briefing, the Government's response (Dkt. # 28), and the allocution of Ronald Ortman, Esq., on behalf of Mr. Torres, and Tracy Thompson, Esq., on behalf of the government at a hearing held on September 8, 2016. For the reasons stated below, Mr. Torres' Motion to Suppress is **DENIED** (Dkt. # 23).

I. Background Facts

Mr. Jeffrey Jerry Torres, a resident of San Antonio, Texas, is charged with receiving and possessing child pornography, in violation of 18 U.S.C.

§§ 2252A(a)(2) and (a)(5)(B). (Dkt. # 4 at 1-2.) The charges against Mr. Torres

1

stem from his alleged activity on "Website A,"1 which contained prohibited images of child pornography and child erotica. (Dkt. # 23 at 2.)

According to the warrant applications submitted as evidence in the case, "Website A" was a website accessible on an anonymity internet network known as "The Onion Router" or "Tor" network. ("Bletsis Aff.," Dkt. # 23, Ex. 5-2 ¶ 14). Only internet users who have installed free and publicly available Tor software are able to access the Tor network. (Id.) The Tor software **[*2]** bounces a user's internet communications through a network of computers scattered across the world. (Id. ¶ 15.) As a result, when a user on the Tor network accesses a website, the IP address of the Tor "exit node"-the last computer through which the user's communications were routed-appears in the website's IP log, and the user's actual IP address is not recorded. (Id. ¶ 15.)

The Tor network permits users to set up websites as "hidden services." (Bletsis Aff. ¶ 16.) The IP address for a hidden service site is replaced with a series of algorithm-generated characters which are not searchable through traditional means, and can only be located via communication with other users or from internet postings describing the content available and the method for locating

1The search warrants and pleadings before the Court obscured the name of the site, commonly known as "Playpen," to prevent users from fleeing, destroying evidence, or notifying other users of the investigation. (Dkt. # 28, Ex. 1, at 2 n.1.)

2

such information. (Id. ¶¶ 16-17.) Accordingly, accessing hidden service sites requires a number of affirmative steps by the user.

On February 20, 2015, Agent Douglas Macfarlane of the Federal Bureau of Investigations filed **[*3]** an affidavit in support of a search warrant in the Eastern District of Virginia. (Macfarlane Aff., Dkt. # 23, Ex. 6.) Agent Macfarlane described "Website A," a hidden service site on the Tor network; "Website A" was a message board website whose primary purpose was the advertisement and distribution of child pornography. (Id. ¶ 11.) Accordingly to Agent Macfarlane, "Website A" conservatively hosted 95,148 posts, 9,333 topics, and 158,094 members, and had been operating since August 2014.2 (Id.) Agent Macfarlane stated that the homepage of Website A depicted two partially clothed prepubescent females with their legs spread apart, as well as certain user instructions. (Id. ¶ 12.) The "register an account" hyperlink on the homepage encouraged prospective users to register with a fake email address, and warned against posting any information that could be used to identify the user. (Id. ¶ 13.) Once registered, a user had access to such forums as "Preteen-Boy," "Preteen- Girl," "Jailbait Videos," "Family-Incest," "Kinky Fetish," and "Toddlers." (Id.

2On March 4, 2015, when the FBI ceased to host "Website A" and it was removed from the internet, the site contained a total of 117,773 posts, 10,622 topics, and 214,898 **[*4]** members. ("Allovio Aff.," Dkt. # 23, Ex. B, ¶ 11.)

3

¶ 14.) Agent Macfarlane stated that many of the images on the site depicted sexual abuse of children. (Id. ¶ 27.)

On February 19, 2015, the FBI executed a search warrant at the residence of the suspected administrator of "Website A," and commenced to operate "Website A" from a government server in Newington, Virginia.

(Macfarlane Aff. ¶ 30.) Agent Macfarlane sought a warrant in the Eastern District of Virginia to employ a network investigative technique ("NIT") whereby those users who accessed the target website-hosted in the Eastern District of Virginia-by logging in with a username and password, would be issued certain instructions, causing the "activating" computer to send certain information to a computer run by the Government. (Id. ¶ 33.) This information included the IP address of the "activating" computer, a unique identifier generated by the NIT to distinguish "activating" users from one another, and the operating system of the "activating" computer. (Id. ¶ 34.) The purpose of the NIT was to obtain information to assist the FBI in identifying the "activating computers" and their users. (Id. ¶ 35.) The warrant was issued on February 20, 2016, by United States **[*5]** Magistrate Judge Buchanan in the Eastern District of Virginia, and authorized deployment of the NIT between February 20, 2015, and March 6, 2015. (Dkt. # 23, Ex. 6 at 38.)

On October 6, 2015, Special Agent Jeffrey Allovio, of the Federal Bureau of Investigations, filed an affidavit in the Western District of Texas in

4

support of a residential search warrant. ("Allovio Aff.," Dkt. # 23, Ex. B, ¶ 26.) Agent Allovio testified that on February 21, 2015, the NIT was deployed after the user "Bigman 123" registered an account on "Website A," and was actively logged onto the account for 5 hours and 13 minutes. ("Allovio Aff.," Dkt. # 23, Ex. B,

¶ 26.) During this time, monitoring revealed that the user "Bigman 123" accessed materials including the "Young Sounds Collection," "Beauty latina preteen girl and dad 3/3/5," and at least one other image depicting an exposed prepubescent female. (Id. ¶¶ 26-32.) FBI Agents were able to determine that the IP Address was operated by Time Warner

Cable. (Id. ¶ 31.) The FBI served an administrative subpoena on Time Warner Cable, which connected Mr. Torres to the IP address. (Id.)

Based upon this information and other data contained in the affidavit in support of the search warrant, **[*6]** Magistrate Judge Pamela Mathy issued a search warrant on October 6, 2015, authorizing a search of the premises where Mr. Torres was known to reside. (Dkt. # 23, Ex. B. at 33.) The warrant authorized the FBI to seize such materials as computers and electronic storage devices. (Id. at 35-38.) Agents executed the search on October 7, 2015, and seized various phones, a computer, cameras, storage devices such as USB drives and SIM cards, and a tablet. (Dkt. # 23, Ex. B at 46-48.) Torres agreed to be interviewed, and admitted that he had been accessing and downloading child pornography through a variety

5

of file exchange programs for approximately 1.5 years. ("FBI Interview. 10.7.15," Dkt. # 23, Ex. B at 56-63.) A subsequent forensic search of Mr. Torres' computer revealed that he possessed at least 141 image files and 84 video files depicting child pornography; these files included toddlers, graphic degradation of female children, and at least one video of a male infant being abused by an adult female. (Dkt. # 23, Ex. B at 77-81.)

The NIT warrant signed on February 20, 2015, uncovered information that resulted in the issuance of a multitude of subsequent search warrants around the country; defendants **[*7]** nationwide challenged the validity of the NIT warrant, and courts have reached various conclusions as to the warrant's validity. See e.g., *United States v. Epich, No. 15-cr-163-PP, 2016 WL 953269 (E.D. Wis. March 14, 2016)*; United States v. Werdene, No. 14-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016).

In the instant Motion to Suppress, Mr. Torres seeks to suppress "all evidence seized . . . including but not limited to his statements to law enforcement plus the computers, cellphones, SIM cards, cameras, flash drives and digital images and information seized from his residence." (Dkt. # 23 at 1-2.) Mr. Torres argues that the residential search warrant was based upon information obtained in an unlawful search of his "activating" computer. (Id. at 2.)

6

II. Whether Locating Mr. Torres' IP Address Constituted a Search

The *Fourth Amendment to the United States Constitution* 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, 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. Am. IV. When analyzing a motion to suppress evidence allegedly

obtained in violation of the *Fourth Amendment*, the Court must first determine

"whether or not a *Fourth amendment* 'search' has occurred." Kyllo v. United

States, *533 U.S. 27, 31 (2001)*.

In determining **[*8]** whether a search occurred, the court must consider

whether "a person ha[s] exhibited an actual (subjective) expectation of privacy and

. . . that the expectation is one that society is prepared to recognize as

'reasonable.'" *Katz v. United States, 389 U.S. 347, 361 (1967)*). The Supreme

Court has found that individuals have a reasonable

expectation of privacy in their

cell phones, due to the extensive amount of personal information contained therein.

Riley v. California, 134 S. Ct. 2473 (2014). Likewise, it is reasonable to find that

persons also have a reasonable expectation of privacy in their personal computers,

due to the vast amount of personal information they contain. See United States v.

7

Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004); *Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001)*; *Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001)*.

Conversely, courts-both those to address the issue in the context of the NIT warrant and those addressing the issue in the context of IP addresses more generally, have consistently found that there is no reasonable expectation of privacy in an IP address itself, even when using a Tor browser. See United

States v. Darby, No. 2:16-cr-36, 2016 WL 3189703, at *5 (E.D. Va. June 3, 2016) (finding subject of NIT search at issue here had no reasonable expectation of privacy in his IP address); Werdene, 2016 WL 3002376 at *14-*20 (same); *In re U.S. for Historical Cell Site Data, 724 F.3d 600, 612 n.12 (5th Cir. 2013)* (citing the lack of expectation of privacy in IP addresses, e-mail addresses, phone numbers, and addressing information on the envelopes to support the conclusion that **[*9]** there is no reasonable expectation of privacy in cell site data); *United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010)* ("Federal courts have uniformly held that subscriber information provided to an internet provider is not protected by the *Fourth Amendment's* privacy expectation because it is voluntarily conveyed to third parties" (internal quotations omitted)); *United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010)*; *United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007)* (likening IP addresses to phone numbers dialed, and finding no reasonable expectation of privacy in an IP address).

8

Here, the NIT placed code on Mr. Torres' computer without his permission, causing it to transmit his IP address and other identifying data to the government. That Mr. Torres did not have a reasonable expectation of privacy in his IP address is of no import. This was unquestionably a "search" for *Fourth Amendment* purposes. Accordingly, analysis of the Motion to Suppress is appropriate.

III. Whether the Search Violated *Federal Rule of Criminal Procedure 41* and *Section 636 of the Federal Magistrates Act*

Mr. Torres urges the Court to suppress all evidence found as a result of the residential search warrant executed on October 7, 2015. (Dkt. # 23.) He argues that the original NIT warrant was unlawful, because the issuing magistrate judge had no authority to issue a warrant to search any activating computer located outside of her judicial district. (Dkt. # 23 at 8.) He argues **[*10]** that, absent the original, unlawful search, the government would never have obtained the information underlying the residential warrant application, and agents never would have entered his home. (Id.)

Federal Rule of Criminal Procedure 41(b) and *Section 636 of the Federal Magistrates Act* concern the scope of a magistrate's authority. *Section 636 of the Federal Magistrates Act* states that:

Each United States Magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that

9

appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law-all powers and duties conferred or imposed upon United States commissioners by

law or by the Rules of Criminal Procedure for the United States District Courts.

28 U.S.C. § 636(a). This rule, regarding the magistrate judge's jurisdiction,

incorporates by reference *Federal Rule of Criminal Procedure 41(b)*. *Rule 41(b)*

gives the magistrate authority to issue a warrant at "the request of a federal law

enforcement officer or an attorney for the government" in the following

circumstances:

(1) a magistrate judge with authority in the district . . . has the 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 the person **[*11]** 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;

(3) a magistrate judge-in an investigation of domestic terrorism or international terrorism-with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(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 use of the device to track the movement of a person or property located within the district, outside the district, or both . . .

10

Fed. R. Crim. P. 41(b)(1)-(4).3

The district courts that have already analyzed whether the NIT Warrant violated *Rule 41(b)* have reached various conclusions. See e.g., United

States v. Michaud, 3:15-cr-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan.

28, 2016) (finding that "the NIT Warrant technically violates the letter, but not the

spirit, of *Rule 41(b)*); United States v. Levin, No. 15-10271-WGY, 2016 WL

2596010, at *7 (D. Mass. May 5, 2016) (finding the NIT Warrant substantively

violated *Rule 41(b)*); United States v. Werdene, No. 14-434, 2016 WL 3002376, at

* 7 (E.D. Pa. May 18, 2016) (finding the NIT Warrant procedurally violated Rule

41(b)). **[*12]**

A. Whether the Magistrate Had Jurisdiction Under *Rules 41(b)(1)-(3)*

In this case, the Court finds that the magistrate judge did not have the

authority to issue the NIT warrant under *Rules 41(b)(1)-(3)*. Mr. Torres and the

government agree that the 'activating computer' was located in San Antonio,

Texas, at all relevant times. Accordingly, at the time the warrant was issued, Mr.

Torres' computer was not located in the Eastern District of Virginia, as it must be

for the magistrate judge to have the authority to issue the warrant under Rule

3Federal Rule of Criminal Procedure 41(b)(5) authorizes the issuance of warrants where activity related to a crime took place in the magistrate's district, but property related to the crime is located in such places as a U.S. "territory, possession, or commonwealth," or a U.S. "diplomatic or consular mission in a foreign state." This is inapplicable

here, where the activating computer was not located in a territory, but in San Antonio, and the Court will not address the provision.

11

41(b)(1) or 41(b)(2). *Fed. R. Civ. P. 41(b)(1)-(2)*. Further, child pornography is not currently considered to be an act of domestic or international terrorism, as it must for the magistrate judge to have authority under Rule 41(b)(3). Fed. R. Civ.

P. 41(b)(3). **[*13]**

B. Whether the Magistrate Had Jurisdiction Under Rule 41(b)(4)

The Government urges the Court to find that the magistrate judge in the Eastern District of Virginia had jurisdiction under Rule 41(b)(4), which permits a magistrate judge to issue a warrant to install a tracking device "within the district." (Dkt. # 28 at 23-24.) Such a tracking device may continue to operate even when the tracked object moves outside the district. *Fed. R. Civ. P. 41(b)(4)*. (Dkt. # 28 at 23-24.)

Of the district courts to address the NIT warrant, two have determined that the magistrate judge had jurisdiction under Rule 41(b)(4). The court in United States v. Darby made this determination after finding that activating users of "Website A" "digitally touched down in the Eastern District of Virginia when they logged into the site." No. 2:16-cr-36, 2016 WL 3189703, at *12 (E.D. Va. June 3, 2016). According to the Darby court, this "digital touch down" on the server in the Eastern District of Virginia was sufficient to convey the magistrate judge authority to issue the NIT warrant. (Id.) The court in United States v. Matish determined the magistrate judge had authority under Rule 41(b)(4) after concluding that any

12

person who accessed "Website A" made "'a virtual trip' via the Internet to Virginia." Matish, 4:16-cr-16-HCM-RJK, ECF No. 90, at 39 (E.D. Va. June 23, 2016). The Matish court likened **[*14]** the situation to that in *Kyllo v. United States. 533 U.S. at 40*. In Kyllo, the Supreme Court found that investigators' use of thermal imaging was a "search" for *Fourth Amendment* purposes, and that such a search is "presumptively unreasonable" without a warrant. Id. The Matish court characterized the thermal imaging at issue in Kyllo as an electronic entry into Kyllo's home; extending this logic, the Matish court found that "activating users" electronically entered the Eastern District of Virginia when they accessed "Website A," permitting the court to exercise jurisdiction under Rule 41(b)(4). Matish, at 39.

This Court disagrees with the reasoning in Darby and Matish, and instead finds persuasive the reasoning in Michaud, a case from the Western District of Washington, addressing the NIT Warrant. 2016 WL 337263. The court in Michaud reasoned that the installation of the NIT "occurred on the government-controlled computer, located in the Eastern District of Virginia," because the activating computer in Michaud, like the "activating computer" at issue in the instant case, never physically entered the Eastern District of Virginia. Id. at *6. The Michaud court concluded that "even applying flexibility to *Rule 41(b)* . . . the NIT Warrant technically violates the letter, but not the spirit, of *Rule 41(b)*." Id. at

13

*6. Likewise, this Court **[*15]** finds that the "activating computer" was never physically

present within the Eastern District of Virginia, and that any digital presence of the

"activating computer" was insufficient to convey jurisdiction under Rule 41(b)(4).

Bolstering this argument, on April 28, 2016, the Supreme Court

submitted the following proposed amendment to *Rule 41(b)* to the Congress:

(b) at the request of a federal law enforcement officer or an attorney for the government . . .

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or . . .

Letter from Justice John G. Roberts to the Honorable Paul D. Ryan and the

Honorable Joseph R. Biden, Jr. (Apr. 28, 2016),

www.uscourts.gov/file/19848/download. This proposed amendment, if adopted,

will directly address the issue before the Court today. Until that time, the existence

of the proposed amendment indicates at a minimum that there is currently

ambiguity **[*16]** as to the state of the law.

Clearly, *Rule 41(b)*, as it applies to electronic searches, is currently an

ambiguous area of the law where reasonable minds may differ. Nevertheless, this

Court finds that the plain language of Rule 41(b)(4) did not grant the magistrate

14

judge in the Eastern District of Virginia the jurisdiction to issue the NIT Warrant at issue here. It is inappropriate for this Court to engage in a process of finesse justifying an ethereal presence of the defendant's computer in Virginia, where the plain language of the rule as now written does not provide jurisdiction under these circumstances. As no provision of *Rule 41(b)* gave the magistrate judge authority to issue the NIT warrant, the warrant technically violates *Rule 41*.

IV. Whether the Violation of *Rule 41* Warrants Suppression

The exclusionary rule requires that evidence obtained pursuant to a search violating the *Fourth Amendment* be suppressed. However, "[e]ach time the exclusionary rule is applied it exacts a substantial social cost for the vindication of *Fourth Amendment* rights." *Rakas v. Illinois, 439 U.S. 128, 137 (1978)*; see

also *United States v. Payner, 447 U.S. 727, 734 (1980)*. Accordingly, "the application of the rule has been restricted to those areas where its remedial objectives are thought most efficaciously served." *United States v. Calandra, 414 U.S. 338, 348 (1974)*. The Supreme Court clearly articulated this principle in **[*17]** United States v. Leon, explaining that where a warrant is executed in good faith, even if the warrant itself is found to be procedurally defective, evidence obtained in good-faith reliance need not be suppressed. *United States v. Leon, 468 U.S. 897, 922 (1984)*. This is the "good faith" exception to the exclusionary rule. The rationale behind this decision is simple:

15

The deterrent purpose of the exclusionary rule necessarily assumes that police have engaged in willful, or at the very least negligent, conduct which has deprived the defendant of some right. By refusing to admit evidence gained as a result of such conduct, the courts hope to instill in those particular investigating officers, or in their future counterparts, a greater degree of care toward the rights of the accused.

Id. at 919 (quoting *United States v. Peltier, 422 U.S. 531, 539 (1975)*).

Accordingly, evidence obtained pursuant to an invalid warrant should only be

suppressed "in those unusual cases in which exclusion will further the purposes of

the exclusionary rule." *Leon, 468 U.S. at 918*.

The Fifth Circuit has interpreted this "good faith" exception to apply

where exclusion of illegally-obtained evidence will not deter official illegality or

preserve judicial integrity, and where the "violation is neither of constitutional

dimensions nor intentional." *United States v. Comstock, 805 F.2d 1194, 1210* (5th

Cir. 1986); **[*18]** see also *United States v. Richardson, 943 F.2d 547, 550 (5th Cir. 1991)*

(explaining that after Leon, suppression is warranted only in limited

circumstances). As such, non-willful violations of *Rule 41*, where a search is

executed pursuant to a warrant, properly supported by an affidavit showing

probable cause, and issued by a competent and neutral magistrate judge, do not

require suppression. *Comstock, 805 F.2d at 1200*. Accordingly, "[t]he

exclusionary rule should only be applied when its benefits outweigh its costs."

Herring v. United States, 555 U.S. 135, 141 (2009).

16

Here, the violation of Rule 41(b)(4) did not have a Constitutional dimension; the FBI sought and obtained a series of warrants based upon probable cause. That Rule 41(b)(4) is ambiguous when applied to the instant situation, where the location of a target server is known but the locations of those computers accessing the server are not, does not render any violation of the rule unconstitutional. This ambiguity is evidenced by the variety of conclusions courts have reached regarding the permissibility of the NIT warrant under Rule 41(b)(4).

Further, there is no evidence that either the FBI agents seeking the warrant or the magistrate judge in the Eastern District of Virginia willfully violated Rule 41(b)(4) or otherwise acted in bad faith when they respectively sought and issued the NIT warrant. The evidence before the **[*19]** Court demonstrates that the FBI conducted an extensive investigation of "Website A" over a period of time, sought and obtained a search warrant well-supported by probable cause to deploy a NIT to identify the IP addresses of those computers accessing the site, and used these IP addresses to obtain residential search warrants, such as the one used to apprehend Mr. Torres. Mr. Torres agrees with the Government that both the NIT warrant and the residential search warrant were supported by probable cause. (Dkt. # 28 at 2.)

At the hearing, Defense counsel urged the Court to abstain from considering whether the agents in the case acted in good faith. This argument is inapposite, where the Supreme Court has explicitly created a good-faith exception

17

to the exclusionary rule. See *Leon, 468 U.S. at 922*; *Richardson, 943 F.2d at 550*; *Comstock, 805 F.2d at 1210*.

Applying the exclusionary rule here would "exact a substantial social cost for the vindication of *Fourth Amendment* rights," and could result in the suppression of a significant quantity of evidence currently being used to prosecute individuals who allegedly downloaded child pornography from "Website A" during a two-week period in 2015. See *Rakas, 439 U.S. at 137*. There is no evidence that the violation of *Rule 41(b)* was willful, that it was acquired in bad **[*20]** faith, or that suppression of the evidence at issue here will deter future illegality. Rather, the instant NIT warrant has brought to light the need for Congressional clarification regarding a magistrate's authority to

issue a warrant in the internet age, where the location of criminal activity is obscured through the use of sophisticated systems of servers designed to mask a user's identity. Suppression is not warranted here, and Mr. Torres' Motion to Suppress is **DENIED** (Dkt. # 23).

IT IS SO ORDERED.

DATED: San Antonio, Texas, September 9, 2012.

18

End of Document