United States v. Workman

United States District Court for the District of Colorado

September 6, 2016, Decided

Criminal Case No. 15-cv-00397-RBJ-1

Reporter
2016 U.S. Dist. LEXIS 133782

UNITED STATES OF AMERICA, Plaintiff, v. ANDREW JOSEPH WORKMAN, 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.

Core Terms

magistrate judge, users, suppression, seized, good-faith, activating, child pornography, computers, authority to issue, tracking, website, void, reasons, exigent circumstances, warrantless search, searched, longrod, network, server, rule violation, authorize, search warrant, good faith, Investigative, Attachment, expectation of privacy, evidence obtained, government claim, district court, instructions

Opinion

[*1] ORDER

This matter is before the Court on defendant's motion to suppress [ECF No. 33]. For the reasons discussed in this Order, defendant's motion is granted.

I. FACTS

This case arises out of an investigation into a child pornography website. ECF No. 36 at 1. In September 2014, the Federal Bureau of Investigation began investigating a website named Playpen, suspecting it of hosting users for the purpose of advertising, distributing, and accessing child pornography. *Id.* Playpen had more than 150,000 registered users and contained tens of thousands of posts related to child pornography. *Id.*; ECF No. 36-1 at ¶ 10-13.

Playpen was not accessible through traditional search engines or browsers. ECF No. 36 at 1-3. It operated on "The Onion Router" or "Tor." *Id.* Tor conceals a user's location and activity by encrypting data and sending it through a series of random relay nodes. *Id.* Users have to download specific Tor software or utilize a Tor "gateway" to get onto the Tor network and then navigate to a site like Playpen. *Id.*

1

Additionally, Playpen encouraged users to register anonymously using a false email

address. ECF No. 33-1 at ¶ 38. After registering, users could access different sections of **[*2]** the

website, including forums relating to sexual exploitation of children. *Id.* at ¶ 42. For example,

Playpen had forums and sub-forums for "jailbait," "preteen," and "toddlers." ECF No. 36-1 at ¶

14. Playpen also encouraged users to upload child pornography and contained discussion boards

relating to sexual abuse of children. ECF No. 33-1 at ¶ 40.

The Network Investigative Technique Warrant

In February 2015, the FBI apprehended the administrator of Playpen and took control of

the website. ECF No. 36 at 1-3. Rather than shut down Playpen, however, the FBI operated the

website from a government facility in the Eastern District of Virginia for close to two weeks in

an effort to identify website users. To do so the FBI sought and obtained two forms of court

authorization from the United States District Court for the Eastern District of Virginia which

enabled it to obtain information about users visiting the site. *Id.* First, the FBI obtained a Title

III application to monitor Playpen's chat function. ECF No. 33-2. Second, the FBI obtained a

warrant (the NIT Warrant) to deploy a Network Investigative Technique (NIT). ECF No. 33-3.

The NIT Warrant was issued by Magistrate Judge Theresa Carroll Buchanan in the

Eastern **[*3]** District of Virginia. *Id.* The warrant stated,

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia. (Identify the person or describe the property to be searched and give its location): See Attachment A. The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): See Attachment B.

Id.

Thus, attachment A described the place to be searched. *Id.* at 2. It stated that the NIT

Warrant "authorize[d] the use of [an NIT] to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described

2

below." *Id.* It explained that the computer server, which was located at a government facility in the Eastern District of Virginia, was operating a Tor network child pornography website. *Id.*

Further, it stated that the activating computers were those of any user or administrator who logged into the child pornography website. *Id.*

Attachment B identified the property to be seized. *Id.* It listed seven pieces of information to be seized "[f]rom **[*4]** any 'activating' computer": (1) the IP address, and the date and time the NIT determined the IP address; (2) a unique identifier generated by the NIT; (3) the type of operating system running on the computer; (4) information about whether the NIT had already been delivered to the activating computer; (5) the activating computer's Host Name; (6) the activating computer's active operating system username; and (7) the activating computer's media access control address. *Id.* at 3.

In March 2015 the FBI received information, through its use of the NIT, about Playpen user "longrod." ECF No. 36 at 8. "Longrod" had been a Playpen member since December 31, 2014. *Id.* Additionally, "longrod" had logged into the website for a total of 11 hours and 45 minutes through March 1, 2015. *Id.* The NIT indicated that "longrod" used an IP address operated by the Internet Service Provider Comcast. *Id.* The FBI subsequently served Comcast with an administrative subpoena. *Id.* Comcast responded that the IP address associated with "longrod" was registered to a customer named D. Gurule living in Lone Tree, Colorado. *Id.*

The Residential Warrant

The FBI then sought and obtained a search warrant (the Residential Warrant) for **[*5]** Mr. Gurule's address from Magistrate Judge Nina Y. Wang of

this district. ECF No. 33-1. On September 18, 2015 FBI agents executed the warrant. ECF No. 36 at 8. Upon arrival, they discovered that defendant Andrew Workman subleased a bedroom from Mr. Gurule. *Id.* The

3

Agents found Mr. Workman in his bedroom actively downloading child pornography from the Internet. *Id.* Mr. Workman agreed to a non-custodial interview with the FBI agents. *Id.* at 9. He admitted that he was the user "longrod" on Playpen. *Id.* Additionally, he admitted to using a Tor network and a virtual private network (VPN) to hide his true location. *Id.*

Agents seized Mr. Workman's computer. *Id.* A forensic review later revealed a hidden folder under the user "Andrew" that contained approximately 1,248 images and 171 videos of child pornography. *Id.*

On October 7, 2015 the Grand Jury returned an indictment against Mr. Workman for one count of Receipt of Child Pornography and one count of Possession of Child Pornography in violation of *18 U.S.C. §§ 2252A(a)(2)* and *(a)(5)(B)*. ECF No. 36-1. Mr. Workman now moves to suppress all evidence obtained or derived from the NIT Warrant. ECF No. 33.

II. ANALYSIS

Mr. Workman moves to suppress the evidence obtained or derived from the **[*6]** NIT Warrant, arguing that the government's search of Mr. Workman's computer violated both *Federal Rule of Criminal Procedure 41* and *28 U.S.C. § 636(a)*.1 ECF No. 33. The government opposes the motion, arguing that the magistrate judge had authority to issue the NIT Warrant under *Rule 41(b)(2)* and *(b)(4)* and thus had authority to issue the search under *28 U.S.C. § 636(a)(1)*. ECF No. 36 at 9-10. Alternatively, the government asserts that even if the NIT Warrant was defective, the evidence should not be suppressed because (1) the alleged violation did not prejudice Mr. Workman, nor is there evidence of intentional and deliberate disregard of *Rule 41*;

1 28 U.S.C. § 636(a)(1) states,

(a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law . . . 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[.]

4

(2) the officers acted in good faith; and (3) a warrantless search was justified due to exigent

circumstances. *Id.* at 10-11. The Court will address each argument in turn.2

Rule 41(b)

Mr. Workman asserts that the NIT Warrant violated Federal **[*7]** Rule of Criminal Procedure

41(b) because Magistrate Judge Buchanan did not have authority to authorize a search of Mr. Workman's computer, which was located outside of the Eastern District of Virginia. I agree with Mr. Workman.

First, the Court finds that *Rule 41(b)(1)* did not authorize the issuance of the NIT Warrant. Under *Rule 41(b)(1)*, "[a]t the request of a federal law enforcement officer or an attorney for the government . . . a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district[.]" "Property" includes both "tangible objects" and "information." *Fed. R. Crim. P. 41(a)(2)(A)*.

Here, under *Rule 41(b)(1)*, Magistrate Judge Buchanan had authority to issue a warrant to search for and seize property located within the Eastern

District of Virginia. However, under Attachment A labeled "Place to be Searched," the NIT Warrant clearly states that it authorized the NIT to "obtain information . . . from the activating computers." ECF No. 33-3 at 2. It is undisputed that the activating computer at issue here-Mr. Workman's computer-was located in the District of Colorado. Therefore, *Rule 41(b)(1)* did not authorize the search of Mr. Workman's computer because the place **[*8]** to be searched and information to be seized were located outside of the Eastern District of Virginia. *See Levin*, 2016 WL 2596010, at *5 (finding that the

2 It is worth noting that several other courts have considered motions to suppress evidence obtained and derived from the NIT Warrant. At least two courts have denied the motions to suppress before them while others have granted them for a multitude of reasons. *See e.g.*, *United States v. Matish*, No. 4:16CR16, 2016 WL 3545776 (E.D. Va. June 23, 2016) (suppression not appropriate); *United States v. Darby*, No. 2:16CR36, 2016 WL 3189703, at *14 (E.D. Va. June 3, 2016) (same); *United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010, at *15 (D. Mass. May 5, 2016) (suppression appropriate). This Court discusses several of those decisions throughout this Order.

5

NIT Warrant was not authorized by *Rule 41(b)(1)* where the defendant's computer was located in Massachusetts); *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016) (holding that the NIT Warrant was not authorized by 41(b)(1) "because the object of the search and seizure was [the defendant's] computer, not located in the Eastern District of Virginia").

However, the government contends that even if Magistrate Judge Buchanan lacked authority to issue the NIT Warrant under *Rule 41(b)(1)*, she had authority to issue the warrant under *Rule 41(b)(2)* and *(4)*. For the following reasons, I disagree.

Rule 41(b)(2) states that "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 **[*9]** is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed[.]" The government argues that by signing into the Playpen site, information-such as the user's IP address-traveled from the user's computer to the Playpen site, which was located in the Eastern District of Virginia. ECF No. 36 at 13. Further, the government contends that the NIT, which was installed onto Playpen's server in the Eastern District of Virginia, would cause instructions to be attached to Playpen's data, and that once the user logged on to Playpen, the user would pull the data and instructions back through the relay nodes to his computer. *Id.* Finally, the government asserts that once the data arrive at the user's computer, the instructions cause a search to be executed and the user's computer to respond with the requested information, such as the IP address. *Id.* Thus, the government claims that "in accordance with *Rule 41(b)(2)*, the warrant permits a search in another district since the property (i.e., the information) was located within the Eastern District of Virginia initially and moved,

6

upon the voluntar[y] activity of the user, to that other district **[*10]** before the warrant was executed."

Id.

I am not persuaded by the government's argument. *Rule 41(b)(2)* applies to property located in the same district as the magistrate judge at the time the warrant is issued. As stated above, the NIT was designed to search "activating computers," and, in this case, Mr. Workman's computer was located in the District of Colorado when the warrant was issued. Further, there is no evidence that the property (information) to be seized, such as Mr. Workman's IP address, was located in the Eastern District of Virginia at the time the warrant was

issued either. Therefore, *Rule 41(b)(2)* does not apply. *See Levin*, 2016 WL 2596010, at *6 (finding that *Rule 41(b)(2)* did not apply because "the actual property to be searched was not the NIT nor the server on which it was located, but rather the users' computers"); *Darby*, 2016 WL 3189703, at *12 (*Rule 41(b)(2)* did not allow the magistrate judge to issue the same warrant because "[a]t the time the warrant was issued, Defendant's computer was outside the district and not accessing the website.").

Rule 41(b)(4) states that "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 **[*11]** located within the district, outside the district, or both[.]" A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." *Fed. R. Crim. P. 41(a)(2)(E)*. The government claims that the NIT acted as a tracking device because it attached instructions to the data as it traveled outside of the district to the user's computer. ECF No. 36 at 13.

Again, I am not persuaded by the government's argument. While it is tempting to view the NIT as a tracking device, the reality of the technology at issue here is that the NIT did not

7

"track the movement of . . . property" as *Rule 41(b)(4)* contemplates. The government did not obtain Mr. Workman's IP address by tracking the data as it moved through various relay nodes back to Mr. Workman's computer. Rather, the government, through the NIT, searched Mr.

Workman's computer and seized his IP address along with various other pieces of information. As such, *Rule 41(b)(4)* is inapplicable. *See also United States v. Ryan Anthony Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016) ("the NIT does not track; it searches").

Further evidence in support of this Court's conclusion that *Rule 41(b)* did not authorize the issuance of the NIT Warrant can be found in the Supreme Court's recent authorization of an amendment to the Rule. Effective **[*12]** December 1, 2016 magistrate judges will have authority to issue warrants like the NIT Warrant so long as their district has a connection with the criminal activity being investigated. *Darby*, 2016 WL 3189703, at *11. The amendment states,

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 . . .

Id. (quoting *Fed. R. Crim. P. 41(b)(6)* (proposed amendment)). At least in this Courts view, a plain reading of the current *Rule 41(b)* and proposed Section (6) indicates that Section (6) is an entirely new grant of magistrate judge authority, rather than a clarification of the scope of Rule(b)(2) or (4).

For the above reasons, the Court finds that Magistrate Judge Buchanan lacked authority under *Rule 41(b)* to issue the NIT Warrant, and therefore, the NIT Warrant violated *28 U.S.C. § 636(a)* for the same reasons. As such, the Court must determine whether suppression is appropriate. For the following reasons, I find that it is.

8

The Tenth Circuit's opinion **[*13]** in *United States v. Pennington, 635 F.2d 1387* (10th Cir.

1980) sets forth the analytical framework for determining whether a *Rule 41* violation justifies

suppression. *United States v. Krueger, 809 F.3d 1109, 1113-14 (10th Cir. 2015)*. The Court

must first determine "whether that specific *Rule 41*

violation rises to the level of a Fourth

Amendment violation." *Id.* If so, suppression is appropriate. *See id.* However,

[i]f [the Court determines] that the *Rule 41* violation is *not* of constitutional import, [the Court] then consider[s] whether the defendant can establish that, as a result of the Rule violation, (1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.

Id. at 1114 (quoting *Pennington, 635 F.2d at 1390*) (internal quotations omitted). If the

defendant can establish prejudice or intentional disregard of *Rule 41*, suppression is warranted.

Id. However, if the defendant cannot, "a non-constitutional violation of *Rule 41* will not, by

itself, justify suppression." *Id.*

The Court need not determine whether this *Rule 41* violation is of constitutional import

or whether there is evidence of intentional and deliberate disregard of the Rule because it would

not alter the Court's outcome. Following the prejudice **[*14]** standard set forth in *Krueger*, the Court

finds that Mr. Workman was prejudiced by the violation, and therefore suppression is warranted.

In *Krueger*, the government argued that the prejudice inquiry asks whether a magistrate judge *in*

the appropriate district could have issued the warrant. *Id. at 1116*. The Tenth Circuit rejected

this argument. *Id.* The *Krueger* court stated, "[w]hen it comes to something as basic as who can issue a warrant, we simply cannot accept such a speculative approach." *Id.* Rather, the Tenth

Circuit held that the appropriate prejudice inquiry asks whether "*the issuing federal magistrate*

judge could have complied with the Rule." *Id.* (emphasis added).

9

The Court finds that Mr. Workman has established prejudice because the search of his computer would not have occurred had *Rule 41(b)(1)* been followed. In my view, had Magistrate Judge Buchanan understood that the NIT technology would search computers in other districts-rather than track information as it traveled from her district to others-she probably would not have issued the NIT Warrant given the limitations of the Rule. And had the NIT Warrant not been issued, the search of Mr. Workman's computer would not have occurred as it did.3 *See Krueger, 809 F.3d at 1117* (citing *United States v. Glover, 736 F.3d 509, 514-15 (D.C.Cir.2013)* for the proposition **[*15]** that a *Rule 41* violation cannot be excused as a mere "technical defect").

The government contends that the correct prejudice standard asks whether the evidence could have been obtained by other lawful means. ECF No. 36 at 16. Under that standard, the government argues that Mr. Workman did not suffer prejudice because the "core information obtained by the NIT Warrant," Mr. Workman's IP address, "is public information in which the defendant has no reasonable expectation of privacy and [which the government may obtain] by other lawful means."4 ECF No. 36 at 16. The government cites *Michaud* to support its argument. 2016 WL 337263, at *7 (the defendant did not suffer prejudice because he "has no

3 The government argues that "the search authorized by the Residential Warrant . . . satisfied *Rule 41(b)(1)* because that warrant was signed by Magistrate Judge Wang for a residence in Colorado." ECF No. 36 at 21. The government

focuses too narrowly on the Residential Warrant and ignores the direct connection between the two warrants. This Court's prejudice analysis focuses on the NIT Warrant and all evidence obtained as a result. The evidence obtained from the NIT Warrant-Mr. Workman's IP address-led to the issuance of the Residential Warrant. **[*16]**

4The government claims that "[e]ven though it was difficult to tie the anonymized IP address to Defendant Workman's true IP address, that true data still was public information, like an unlisted telephone number, and eventually could have been discovered." ECF No. 36 at 16. This point is contradicted by Special Agent Douglas Macfarlane's affidavit in support of the NIT Warrant, indicating that the FBI could not obtain Playpen users' IP addresses through other means. ECF No. 36-1 at ¶ 31. He stated, "[d]ue to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or 'nodes,' . . .

other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried." *Id.*

10

reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, [his] assigned IP address, which ultimately led to [his] geographic location"). I disagree with the government, and I do not find *Michaud* persuasive in light of Tenth Circuit precedent.

The government's **[*17]** prejudice standard focuses on whether the *evidence* could have been obtained by other lawful means, while *Krueger* asks whether this particular *search* would have occurred if the Rule had been followed.

Additionally, the government's reference to "other lawful means" is unclear. To the extent the government is suggesting that a defendant is not prejudiced where the government could have conducted the search at issue without a warrant, the government's standard could comport with *Krueger*.5 In that case, if, hypothetically, the government did not need a warrant to deploy the NIT, and Magistrate Buchanan had followed *Rule 41(b)* and refused to sign the NIT Warrant, the particular search of Mr. Workman's computer could have occurred anyway. However, that is not the case here. While the Court recognizes that Mr. Workman does not have a reasonable expectation of privacy in his IP address, the problem with the government's argument is that it ignores Mr. Workman's expectation of privacy in the place searched-his personal computer that he was using for private purposes in his home. *See United States v. Andrus, 483 F.3d 711, 718 (10th Cir.), decision clarified on denial of reh'g, 499 F.3d 1162 (10th Cir. 2007)* ("A personal computer is often a repository for private information the computer's **[*18]** owner does not intend to share with others."). The government is not permitted to conduct a warrantless search of a place in which a defendant has a reasonable expectation of privacy simply because it intends to seize property for which the defendant does not have a reasonable

5 However, imagining ways in which the government could have obtained Mr. Workman's IP address- for example, by asking a magistrate judge in the District of Colorado to sign the warrant -is the type of speculation foreclosed in *Krueger. 809 F.3d at 1116* ("instead of focusing on what the Government *could have* done to comply with *Rule 41(b)(1)*, we conclude that prejudice in this context should be anchored tothe facts as they actually occurred").

11

expectation of privacy. For example, if Mr. Workman had written his IP address written down on a piece of paper and placed it on his desk in his home, the government would not be permitted to conduct a warrantless search of his home to obtain that IP address. The same is true here. The

government could not have performed the search of Mr. Workman's computer absent a warrant, and, as described above, Magistrate Judge Buchanan would not have issued this warrant had *Rule 41(b)* been followed.

In sum, under the standards set **[*19]** forth in *Krueger* and *Pennington*, suppression is appropriate.

Good Faith

The government also claims that suppression is not appropriate because the officers

executing the NIT Warrant acted in good faith. ECF No. 36 at 22. For the reasons discussed below, I disagree.

In *United States v. Leon, 468 U.S. 897 (1984)*, the Supreme Court recognized a good-faith exception to the exclusionary rule. *United States v. Clarkson, 551 F.3d 1196, 1203 (10th Cir. 2009)*. Because the exclusionary rule is designed to deter police misconduct, the *Leon* Court determined that "even if an officer in a given case obtained evidence in violation of the *Fourth Amendment*, it made no sense to exclude that evidence if the officer was nevertheless acting in an objectively reasonable manner when he seized the evidence." *United States v. Herrera, 444 F.3d 1238, 1249 (10th Cir. 2006)* (citing *Leon, 468 U.S. at 918-20*). Therefore, the *Leon* Court adopted the good-faith exception to the exclusionary rule and "applied that exception where an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope, even though the search warrant was later deemed to be invalid." *Id.*

(internal quotation marks omitted).

12

Whether the good-faith exception applies where the issuing judge lacked authority to issue the warrant-where the warrant is essentially void at the outset-is an unresolved issue **[*20]** in the Tenth Circuit. *See United States v. Baker, 894 F.2d 1144 (10th Cir. 1990)*. In *Baker*, the Tenth Circuit determined that a Colorado state court judge did not have jurisdiction pursuant to *18 U.S.C. §§ 1151-1153* to issue a warrant to seize property within the boundaries of tribal land.

Id. at 1147. In its discussion of the good-faith exception, the *Baker* court stated,

[a]lthough it is true . . . that *Leon* and *Sheppard* have been held inapplicable to most warrantless searches . . . the case at bar, involving a warrant but one that was essentially void *ab initio*, appears to fall somewhere between the two poles occupied by the defective-warrant and absent- warrant cases. Neither party has cited any authority on point either for or against application of *Leon* and *Sheppard* to this situation, and we have found little.

Id. at 1147-48 (internal citations and footnote omitted). Although the *Baker* court recognized the issue, it did not purport to resolve the issue, as it held that the government could not establish good faith in any event. *Id. at 1148*.

The district court in *Krueger* also considered this issue, specifically with respect to a violation of *Rule 41(b)(1)*, and it determined that the agents' good faith could not "cure a fatally defective warrant." *998 F. Supp. 2d 1032, 1036 (D. Kan. 2014)*. However, the government did not raise the issue on appeal, and therefore **[*21]** the Tenth Circuit had "no occasion to consider whether the district court correctly concluded that . . . the good-faith exception to the warrant requirement was inapplicable given the obviousness of the *Rule 41* defect[.]" *809 F.3d at 1113 n.5*.

At least one district court within the Tenth Circuit has analyzed the good-faith exception as it relates to the NIT Warrant. *United States v. Arterbury*, No. 15-cr-182, slip op. (N.D. Okla. Apr. 25, 2016 (adopting the report and recommendation of the magistrate judge, ECF No. 42).

The *Arterbury* court recognized that the Playpen

case presents a scenario in which there are two

13

warrants and the "second warrant is secured in the appropriate jurisdiction, but probable cause for the second warrant was secured by means of an earlier, invalid warrant." *Id.* at 24. The court asked, "Should the good-faith exception permit officers to rely on the second, valid warrant? Or is the second warrant fatally flawed because of the invalidity of the first warrant?" *Id.*

The *Arterbury* court ultimately concluded that the good-faith exception did not apply to the NIT Warrant for two reasons. First, it rejected the notion that the NIT warrant constituted a mere "technical violation" of *Rule 41(b)*. *Id.* at 25. I agree with the court's reasoning on this point. As discussed **[*22]** in *Krueger*, "[o]ver the years, [the Tenth Circuit has] addressed many other provisions of *Rule 41*" and "never conclud[ed] that the alleged *Rule 41* violation(s) at issue justified suppression." *809 F.3d at 1116 n.7*. However, those cases generally involved violations of the procedural or technical requirements set forth in *Rule 41(a)*, *(c)*, *(d)*, or *(e)*.6 *Id.*;

Arterbury, No. 15-cr-182, slip op. at 25. As a result, those cases offer limited guidance with respect to *Rule 41(b)(1)*, "which is unique from other provisions of *Rule 41* because it implicates 'substantive judicial authority.'" *Krueger, 809 F.3d at 1116 n.7* (quoting *United States v. Berkos, 543 F.3d 392, 397 (7th Cir. 2008)*); *see also Levin*, 2016 WL 2596010, at *7 (finding that the good-faith exception did not apply to the NIT Warrant in part because "*Rule 41* . . . has both procedural and substantive provisions - and the difference matters" and concluding that a violation of *Rule 41(b)* is a substantive violation).

Second, the *Arterbury* court determined that where the warrant is void *ab initio* under *Rule 41(b)* the good-faith exception does not apply. No. 15-cr-182, slip op. at 26. (citing *Levin*, 2016 WL 2596010, at *12). Again, I agree. In addressing the same issue, the *Levin* court

6 For example, in *United States v. Pulliam*, the Tenth Circuit held that the police's failure to provide the defendant with a copy of the search warrant contemporaneous with the search in violation of *Fed. R. Crim. P. 41(f)(1)* did not justify suppression. *748 F.3d 967, 973 (10th Cir. 2014)*.

14

reasoned that "[b]ecause a warrant that was void at the outset **[*23]** is akin to no warrant at all, cases

involving the application of the good-faith exception to evidence seized pursuant to a warrantless

search are especially instructive." 2016 WL 2596010, at *12; *see also Krueger*, 809 F.3d at

1123-24 (Gorsuch, J., concurring) (a warrant issued beyond the territorial jurisdiction of a

magistrate's powers "was no warrant at all"). And, as is true in the Tenth Circuit, the *Levin* court

noted that the good-faith exception does not apply to warrantless searches. *Id.*; *Baker*, 894 F.2d

at 1147. The *Levin* court continued,

> [t]o hold that the good-faith exception is applicable here would collapse the distinction between a voidable and a void warrant. But this distinction is meaningful: the former involves "judicial error," such as misjudging the sufficiency of the evidence or the warrant application's fulfillment of the statutory requirements[,] while the latter involves "judicial authority," i.e., a judge act[ing] outside of the law, outside of the authority granted to judges in the first place.

2016 WL 2596010, at *12 (internal citations and quotations omitted).

In sum, a violation of *Rule 41(b)(1)* is substantive, not technical. Thus, a warrant issued

in violation of *Rule 41(b)(1)* is void.7 As such,

where the issuing judge acts outside of **[*24]** her

authority the good-faith exception should not apply. As the Court determined above, Magistrate

Judge Buchanan lacked authority under *Rule 41(b)* and *28 U.S.C. § 636(a)* to issue the NIT

Warrant for the search of Mr. Workman's computer. Therefore, the NIT Warrant is void as to

Mr. Workman and the Court will not apply the good-faith exception.

7 The government asserts that the NIT Warrant was not "essentially void at the outset" because it 41(b)(1) authorized its issuance in at least one place-the Eastern District of Virginia. ECF No. 36 at 10. I am not convinced that if a magistrate judge issues a warrant that exceeds her authority in almost every respect, the warrant is not void as long as it also covers a search for which the magistrate judge had authority to issue a warrant-particularly where the search the government claims is "valid" is not at issue in this case. Rather, looking to the particular facts of this case, I find that the NIT Warrant was void as to Mr. Workman.

15

Exigent Circumstances

Finally, the government contends that suppression is not warranted because exigent

circumstances justified the search even without a valid warrant. ECF No. 36 at 23. I am not persuaded.

The "exigent circumstances" exception **[*25]** permits a warrantless search "when the circumstances posed a significant risk to the safety of a police officer or a third party." *United States v. Najar, 451 F.3d 710, 717 (10th Cir. 2006)*. Where, as here, the alleged concern is personal danger, the test is "whether (1) the officers have an objectively reasonable basis to believe there is an immediate need to protect the lives or safety of themselves or others, and (2) the manner and scope of the search is reasonable[.]" *Id. at 718*. The burden is on the government to establish the existence of exigent circumstances. *Arden v. McIntosh, 622 F. App'x 707, 709 (10th Cir. 2015)*.

Here, the government contends that the ongoing abuse of children by Playpen users created the exigency. ECF No. 36 at 24. Its argument rests on its contention that Playpen encouraged its users to upload new or fresh images of child sexual abuse, which in essence encouraged its users to actively abuse children and take pictures or videos of the act. *Id.* at 25. While this Court recognizes that the active abuse of children certainly constitutes an exigency, the facts here don't suggest that, at the time the search of Mr. Workman's computer, the officers executing the NIT had "an objectively reasonable basis to believe there is an *immediate need* to protect the lives or safety of themselves or others." **[*26]** *Najar, 451 F.3d at 718* (emphasis added). The government's claim that there was an immediate need to protect children from ongoing sexual abuse is belied by the undisputed fact that the after seizing the Playpen server the FBI

16

kept Playpen up and running for almost two weeks. Further, several months elapsed between the time that the FBI deployed the NIT (the search of Mr. Workman's computer) and the search of Mr. Gurule's home-the point in time when the FBI arguably could have rescued a child from ongoing sexual abuse. The government's willingness to keep Playpen operating and the several months that it took to finally search Mr. Gurule's home does not suggest to the Court that its officers believed that they needed to act immediately.

The government also argues that the FBI was permitted to conduct a warrantless search of Mr. Workman's computer because "the destruction of IP login evidence was imminent." *Id.*

The Tenth Circuit has recognized that "[w]hen officers have reason to believe that criminal evidence may be destroyed or removed *before a*

warrant can be obtained, the circumstances are considered sufficiently critical to permit a warrantless entry." *United States v. Scroger, 98 F.3d 1256, 1260 (10th Cir. 1996)* (internal citation and quotations omitted). Here, however, **[*27]** the government had time to obtain a warrant, and, in fact, they did obtain one. They simply did it incorrectly and in violation of *Rule 41(b)*. It does not follow that there was no time or "no way for the government to have obtained the NIT Warrant." *Levin*, 2016 WL 2596010, at *14. Instead of going to a magistrate judge, the government could have gone to a district court judge, to which *Rule 41(b)* does not apply. *Levin*, 2016 WL 2596010, at *14 ("The magistrate judge who issued this warrant sits primarily in Alexandria, Virginia . . . Four district judges and three senior judges sit routinely in that courthouse.").

Furthermore, where the imminent destruction of evidence is at issue, the test is whether

(1) there is clear evidence of probable cause; (2) the crime is serious and the circumstances such that the destruction of the evidence is likely; (3) the entry is limited in scope to the minimum intrusion necessary to prevent the destruction of evidence; and (4) the exigency is supported by

17

clearly defined indicators that are not subject to police manipulation or abuse. *United States v. Aquino, 836 F.2d 1268, 1272 (10th Cir. 1988)*. The government has not carried it burden of establishing the fourth element. The government has not convinced me that its deployment of the NIT is not subject to police manipulation, particularly **[*28]** where the government manipulated the exigent circumstances by seizing the Playpen server and then running Playpen from an FBI facility for nearly two weeks. FBI did not seize the Playpen server, discover "longrod" uploading or downloading child pornography, and "rush in" to seize longrod's IP address. Rather, it kept the Playpen server running while it waited for "exigent circumstances" to develop.

In sum, because the government has failed to carry its burden to establish personal danger or the imminent destruction of evidence, the exigent circumstances exception does not apply here.

Conclusion

For the above reasons, the motion to suppress must be granted. And it is not without

concern that the Court reaches this decision. One of the long-recognized and ill-favored consequences of the exclusionary rule is that "some guilty defendants may go free or receive reduced sentences as a result of favorable plea bargains[.]" *Leon, 468 U.S. at 907*. This is particularly difficult to stomach where the crime at issue is something as reprehensible as the possession of child pornography. On the other hand, this ruling might serve as a reminder to respect the substantive and jurisdictional limitations on magistrate judges' **[*29]** authority and to be attentive to "something as basic as who can issue a warrant." *Krueger, 809 F.3d at 1116*.

18

III. ORDER

Therefore, defendant's motion to suppress [ECF No. 33] is GRANTED.

DATED this 6th day of September, 2016.

BY THE COURT:

_____

R. Brooke Jackson

United States District Judge

19

End of Document