NOS. 16-3976 (L) & -3982

IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

UNITED STATES OF AMERICA,
APPELLANT

v.

STEVEN SHANE HORTON & BEAU BRANDON CROGHAN,
DEFENDANTS-APPELLEES

ON APPEAL FROM AN ORDER
ENTERED IN THE UNITED STATES
DISTRICT COURT FOR THE SOUTHERN DISTRICT OF IOWA

GOVERNMENT'S OPENING BRIEF

KEVIN E. VANDERSCHEL
United States Attorney
Southern District of Iowa

KATHERINE MCNAMARA
Assistant United States Attorney
Southern District of Iowa

LESLIE R. CALDWELL
Assistant Attorney General

SUNG-HEE SUH
Deputy Assistant Attorney General

DAVID B. GOODHAND
Appellate Section, Criminal Division
United States Department of Justice
950 Pennsylvania Ave. NW, Rm. 1714
Washington, DC 20530
202-353-4468
david.goodhand@usdoj.gov

CASE SUMMARY AND STATEMENT ON ORAL ARGUMENT

This is a consolidated appeal from an order of the district court suppressing evidence that was derived from the government's use of a Network Investigative Technique Warrant issued by a magistrate judge in the Eastern District of Virginia pursuant to Fed. R. Crim. P. 41(b). Oral argument should be heard in this consolidated appeal because the issues presented are novel and complex. The government seeks 15 minutes of oral argument time.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes, Rules, and Constitutional Provisions

STATEMENT OF JURISDICTION

The district court had subject matter jurisdiction over these cases because the indictments charged defendants, Steven Horton and Beau Croghan, with offenses against the United States. 18 U.S.C. § 3231. On September 19, 2016, the district court entered an Order suppressing evidence to be used in the trials against Horton and Croghan. (DCD1 39.)[1] On October 11, 2016, the United States filed timely notices of appeal and certifications from the order granting suppression. (DCD1 40; DCD2 57.) This Court consolidated these appeals on October 21, 2016. This Court has jurisdiction over the government's appeals pursuant to 18 U.S.C. § 3731.

[1] "DCD1" refers to the docket in Croghan's criminal case (15-CR-48 (S.D. Iowa)), while "DCD2" refers to the docket in Horton's case (15-CR-51 (S.D. Iowa)).

STATEMENT OF ISSUES

1. The district court erred in holding that the magistrate judge lacked authority under Federal Rule of Criminal Procedure 41(b) to issue the Network Investigative Technique (NIT) Warrant.

United States v. New York Tel. Co., 434 U.S. 159 (1977)

United States v. Falls, 34 F.3d 674 (8th Cir. 1994)

Fed. R. Crim. P. 41(b)

2. The district court erred in holding that the purported Rule 41(b) violation required suppression.

United States v. Freeman, 897 F.2d 346 (8th Cir. 1990)

United States v. Faulkner, 826 F.3d 1139 (8th Cir. 2016)

U.S. Const. amend. IV

3. The district court erred when it suppressed evidence of child pornography obtained by federal agents acting in objectively reasonable, good-faith reliance on the NIT Warrant.

Davis v. United States, 564 U.S. 229 (2011)

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

United States v. Leon, 468 U.S. 897 (1984)

United States v. Houston, 665 F.3d 991 (8th Cir. 2012)

U.S. Const. amend. IV

STATEMENT OF THE CASE

A. Statement of facts

In November 2015, Steven Horton and Beau Croghan were separately charged with accessing or attempting to access child pornography. (DCD1 3; DCD2 3.) The Federal Bureau of Investigation had identified Horton and Croghan as targets during its investigation into Playpen,[2] a global online forum through which registered users—including Horton and Croghan—advertised, viewed, and distributed illegal child pornography. (NIT Aff. ¶6.)[3] The scale of child exploitation on Playpen was massive: between August 2014 and February 2015, the website had more than 150,000 members and contained over 95,000 posts and over 9,000 topics related to child pornography. (NIT Aff. ¶11.) Images and videos shared through the site were categorized according to victim age, and gender, and type of sexual activity depicted. (NIT Aff. ¶14.) The site also featured forums where users discussed issues related to child sexual abuse, including tips for grooming child victims and evading law enforcement. (NIT Aff. ¶6.)

---

[2] To protect the security of the investigation, the name of this website was not initially disclosed in search warrant documents, but was alternately referenced as the "TARGET WEBSITE" or "Website A." (NIT Aff. ¶2 n.1.)

[3] Horton attached the FBI's NIT Warrant Affidavit to his Motion to Withdraw Guilty Plea (DCD2 39) as Exhibit 3. For this Court's convenience, it is cited as "NIT Aff."

Playpen operated on the anonymous internet network Tor (short for "The Onion Router"),[4] which allows users to access websites without revealing their actual internet protocol ("IP") address, geographic location, or other identifying information. (NIT Aff. ¶¶7-9.) To access the Tor network, a user must first download and install the Tor software client. *See* www.torproject.org. The Tor software protects users' privacy online by routing their communications through a series of relay computers (called "nodes") run by volunteers around the world. (NIT Aff. ¶8.) When a Tor user visits a website, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address, which could otherwise be used to identify a user. (NIT Aff. ¶8.) There is no practical way to trace the user's actual IP address back through the Tor exit node. (NIT Aff. ¶8.)

Within the Tor network, certain websites, like Playpen, operate as "hidden services." (NIT Aff. ¶9.) Like open Internet websites, hidden services are hosted on computer servers that communicate through IP addresses; unlike open websites, the IP address for a computer hosting a hidden service is replaced with a Tor-based web address, which is a series of 16 algorithm-generated characters followed by the suffix ".onion." (NIT Aff. ¶9.) It is not possible to

[4] The United States Naval Research Laboratory created Tor as a means of protecting government communications and it is now available to the public. (NIT Aff. ¶7.)

find a hidden service's IP address using public lookups; and because Tor hidden services are not indexed like open websites, it is not possible to find a hidden service using a Google-type search. (NIT Aff. ¶¶9-10.)

A user accessing Playpen thus had to take several affirmative steps: downloading and installing the Tor software; acquiring the unique .onion address for Playpen from another user or targeted online postings; finding Playpen on the Tor network; and, once there, gaining access to the site's content by entering a username and password. (NIT Aff. ¶¶7, 9-10, 12.) Playpen visitors were instructed not to enter a real name or post information that could be used to identify them, and were assured that Playpen could not see their actual IP addresses and would protect their privacy. (NIT Aff. ¶¶12-13.) It was thus extremely unlikely that any user could find Playpen inadvertently and access the site without knowledge of its child pornography content. (NIT Aff. ¶¶10, 12-14.)

In February 2015, the FBI seized control of the Playpen website and operated it for approximately two weeks from a government-controlled facility in the Eastern District of Virginia. (NIT Aff. ¶30.) To identify and apprehend the anonymous users of Playpen, the FBI first obtained a Title III order in the Eastern District of Virginia to monitor and intercept user communications on the Playpen site. (DCD2 39-2, pp.1-6.) Second, the FBI obtained a warrant in the Eastern District of Virginia to deploy a Network Investigative Technique

("NIT") to locate and identify individuals who had accessed Playpen to view and share child pornography (the "NIT Warrant"). (DCD2 39-3, pp.2-39.) The NIT was a set of computer instructions designed to transmit computer-related identifying information, including the actual IP address, from the computers of registered Playpen users to a government-controlled computer. (NIT Aff. ¶¶31-35.) Third, after identifying and locating residences associated with the IP addresses of users who had accessed Playpen, FBI agents obtained warrants in districts across the country to search those residences for evidence of child pornography. This case related to the NIT Warrant.

FBI Special Agent Douglas Macfarlane submitted an affidavit in support of the NIT Warrant. The affidavit stated that Playpen was a website dedicated to the advertisement and distribution of child pornography (NIT Aff. ¶6); detailed its architecture and content (NIT Aff. ¶¶14-27); explained that the site operated as a hidden service on the Tor network, thereby masking users' actual IP addresses, their location, and identities (NIT Aff. ¶¶7-9); and described the numerous steps a user must take to locate Playpen and access its content (NIT Aff. ¶¶10, 12-13). The affidavit asserted that, given Playpen's patently illegal content and the affirmative steps required to access it, there was probable cause to believe that any user who accessed the site by entering a username and password did so with the intent to advertise, distribute, and/or view child

pornography. (NIT Aff. ¶¶6, 10.) The affidavit further asserted that use of the NIT was necessary to identify and locate the users and administrators of Playpen, and that other investigative procedures usually employed in criminal investigations of this type had either failed or would likely fail if tried. (NIT Aff. ¶31.)

The affidavit also provided details about how the NIT operated and what information it would obtain from the computer of any user or administrator who logged into Playpen by entering a username and password (the "activating" computer). (NIT Aff. ¶¶33-34.) The computer code comprising the NIT would be added to the digital content on the Playpen website, residing on the government-controlled server in Newington, Virginia. (NIT Aff. ¶33.) After a user entered a username and password to access Playpen, the website would send, and that user's computer would download, the content of the website to display web pages on the user's computer. (NIT Aff. ¶33.) That content would be augmented by the NIT instructions, which would accompany the website content back to the user's "activating" computer, and once downloaded with that content, would cause the activating computer to send specific location-identifying information back to the government. (NIT Aff. ¶¶33-34.) The NIT would thus be deployed in the Eastern District of Virginia from the government-controlled server, and the NIT would thereafter move outside the district when

the Playpen website residing on that government-controlled server sent content to a user's computer outside the district. (NIT ¶¶32-33.) The affidavit therefore asked that the court issue a search warrant authorizing the use of the NIT to "cause an activating computer—wherever located—to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer, as described above and in Attachment B." (NIT Aff. ¶46.)

A federal magistrate judge in the Eastern District of Virginia issued the NIT Warrant on February 20, 2015. (DCD2 39-3, p.38.) In describing the property to be searched, the warrant referred to Attachment A, which stated that the FBI was authorized to deploy the NIT on the government-controlled server hosting the Playpen website (located in the Eastern District of Virginia), and to use the NIT to obtain the information listed in Attachment B from "activating computers," which were defined as the computers "of any user or administrator who logs into [Playpen] by entering a username and password." (*Id.* at p.36.) The property to be seized was described by reference to Attachment B, which listed seven pieces of information, including the actual IP address, to be retrieved from the activating computers. (*Id.* at p.37.)

The FBI used the NIT to identify the IP addresses of hundreds of Playpen users. In Horton's case, the NIT was used to identify an IP address associated with a Playpen user called "boybuttlover123." (DCD2 39, p.3.) On February 26, 2015, "buttboylover123" accessed a Playpen forum titled "CHIBILICIOUS (413 pics) (Updated January 22, 2015)," which contained a link to an image that depicted an adult male inserting his penis into the mouth of a prepubescent girl. (DCD2 39-1, p.20.) Also on February 26, 2015, "buttboylover123" accessed a Playpen post titled "Giselita," which contained an image that depicted the exposed vagina of a prepubescent girl. (*Id.* at p.20.) Using publicly available websites, the FBI determined that the IP address associated with "buttboylover123" was operated by Mediacom; the FBI served Mediacom an administrative subpoena and, based on information provided by Mediacom and a database search of public records, determined that the IP address was assigned to a subscriber, Horton, who lived in Glenwood, Iowa. (*Id.* at pp.20-21.)

Similarly, the NIT was used to identify an IP address associated with a Playpen user called "beau2358," who had accessed a Playpen forum with child-pornography links on three occasions in February and March 2015; the FBI determined that the IP address associated with "beau2358" was assigned to a

subscriber, Croghan, who lived in Council Bluffs, Iowa. (DCD1 3, pp.4-5; DCD1 39, p.4.)[5]

A federal grand jury sitting in the Southern District of Iowa thereafter charged Horton and Croghan with accessing or attempting to access child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). (DCD1 3; DCD2 3.)

B. Suppression proceedings

Horton and Croghan argued the NIT Warrant was issued in violation of Fed. R. Crim. P. 41,[6] and the evidence obtained by use of the NIT Warrant must

---

[5] The FBI used the information obtained from the NIT Warrant to obtain search warrants from a federal magistrate judge in the Southern District of Iowa, but the subsequent searches of Horton and Croghan's homes and computers did not reveal additional child pornography.

[6] As relevant here, Rule 41(b) authorizes a magistrate judge to issue a warrant: for "a person or property located within the district," (b)(1); for "a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed," (b)(2); and "to install within the district a tracking device," which may be used "to track the movement of a person or property located within the district, outside the district, or both," (b)(4). Absent congressional intervention, Rule 41 will be amended on December 1, 2016, to add subsection (b)(6), which provides:

> [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 (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been

be suppressed. (DCD2 45; DCD1 33.) They also argued the government had not acted in good faith.[7] The government responded that the magistrate judge had authority to issue the NIT Warrant pursuant to Rule 41(b)(4). (DCD1 36, pp.4-7.) In any event, suppression is not an appropriate remedy for a Rule 41 violation absent a showing of prejudice, which Horton and Croghan could not make. (*Id.* at pp.7-13.) Finally, even if the NIT Warrant was found defective, the evidence was admissible pursuant to the good-faith exception to the exclusionary rule. (*Id.* at pp.14-15.)

Because the facts leading to Horton and Croghan's arrests were "fundamentally the same" and "undisputed," the district court (Pratt, J.) concluded an evidentiary hearing was unnecessary. (DCD1 39, p.1.) On September 19, 2016, the court granted Horton and Croghan's motions to suppress. The district court first held Rule 41(b)(4) inapplicable because the NIT

---

damaged without authorization and are located in five or more districts.

[7] Neither Croghan nor Horton challenged the existence of probable cause for the NIT search, and the district court did not comment on the existence of probable cause for the NIT Warrant. But every federal court to have addressed the issue has held that the NIT Warrant satisfied both the Fourth Amendment's particularity and probable cause requirements. *See, e.g., United States v. Anzalone*, 2016 WL 5339723, at *7 (D. Mass. Sept. 22, 2016); *United States v. Epich*, 2016 WL 953269, at *2 (E.D. Wisc. Mar. 14, 2016); *United States v. Michaud*, 2016 WL 337263, at **4-5 (W.D. Wash. Jan. 28, 2016).

was not a "tracking device": the NIT "clearly did not 'track' the 'movement of a person or object.' Indeed, it did not 'track' the 'movement' of anything; rather, it caused computer code . . . to relay specific information to the government-controlled computers in Virginia." (*Id.* at p.10.)[8] The district court thus concluded that the Eastern District of Virginia magistrate judge "lacked authority to issue the NIT Warrant." (*Id.* at p.11.)

The court next held that the Rule 41(b) violation required suppression. A "warrant issued without jurisdiction is void *ab initio*" and "any search conducted pursuant to such warrant is the equivalent of a warrantless search," for which suppression is "an appropriate remedy." (DCD1 39, p.14.) In the alternative, the court held, suppression was required because Horton and Croghan were prejudiced. (*Id.* at pp.15-19.) Citing this Court's prejudice test, which requires defendants to show "the search might not have occurred or would not have been so abrasive if the Rule had been followed," the district court reasoned that, "[h]ad Rule 41 been complied with," law enforcement would not have obtained Horton and Croghan's IP addresses and would not have been able to link those IP addresses to Horton and Croghan through subsequent investigation and

[8] The court also reasoned that (b)(1) and (b)(2) were inapplicable because Horton and Croghan's computers—the "property" searched—were never "located" in the Eastern District of Virginia. (DCD1 39, pp.7-8.)

administrative subpoenas. (*Id.* at pp.15, 18 (quoting *United States v. Freeman*, 897 F.2d 346, 349-50 (8th Cir. 1990)).) "It is clear in this case" that the search pursuant to the NIT Warrant would not "have occurred without the violation of Rule 41(b)." (*Id.* at p.18.)

The court further held the good-faith exception to the exclusionary rule inapplicable, reasoning the exception does not apply to "evidence seized pursuant to a warrant that was void at its inception" but "only to evidence seized under a once-valid warrant that was subsequently invalidated." (DCD1 39, p.15 (internal quotation marks omitted).) And even if the good-faith exception could apply to a void warrant, the court declared, it was "inapplicable" because "law enforcement was sufficiently experienced" and there "existed adequate case law casting doubt on magisterial authority to issue precisely this type of NIT Warrant." (*Id.* at p.18.) Further, any "societal costs" attributable to suppression were "outweighed by the fact that suppression will deter police from obtaining warrants from judges who lack jurisdiction to issue them.'" (*Id.* at 14 n.7 (internal quotation marks and brackets omitted).)

C. NIT Warrant decisions

The FBI's execution of the NIT Warrant led to the identification of hundreds of Playpen users located across the country. Many of those individuals have moved to suppress evidence obtained by the NIT Warrant. To date, 28 of

those motions have been resolved: in 24 cases, courts have denied suppression; in only 4 cases, including this one, have courts granted suppression.[9]

In the 24 cases denying suppression, including three in this Circuit, courts have reached different conclusions regarding whether Rule 41(b) was violated, but *all* have held the evidence admissible pursuant to the good-faith exception to the exclusionary rule. Several courts have concluded that the NIT Warrant was authorized by Rule 41(b)(4) but, in any event, the evidence would have been admissible pursuant to the good-faith exception.[10] Other courts have held that the NIT Warrant was not authorized by Rule 41(b), but concluded the non-constitutional violation did not mandate suppression and, in any event, the evidence was admissible pursuant to the good-faith exception.[11] Finally, three

---

[9] For this Court's convenience, contemporaneous with this brief, the government has filed an appendix containing those district court decisions not otherwise available in a computerized legal database.

[10] *See United States v. Johnson*, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016); *United States v. Dzwonczyk*, No. 15-CR-3134 (D. Neb. Oct. 5, 2016) (magistrate judge's report and recommendation); *United States v. Smith*, No. 15-CR-467 (S.D. Tex. Sept. 28, 2016); *United States v. Jean*, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); *United States v. Eure*, 2016 WL 4059663 (E.D. Va. July 28, 2016); *United States v. Matish*, 2016 WL 3545776 (E.D. Va. June 23, 2016); *United States v. Darby*, 2016 WL 3189703 (E.D. Va. June 3, 2016).

[11] *See United States v. Stepus*, No. 15-CR-30028 (D. Mass. Oct. 28, 2016); *United States v. Libbey-Tipton*, No. 16-CR-236 (N.D. Ohio Oct. 19, 2016); *United States v. Allain*, 2016 WL 5660452 (D. Mass. Sept. 29, 2016); *United States v. Anzalone*, 2016 WL 5339723 (D. Mass. Sept. 22, 2016); *United States v. Knowles*, No. 15-CR-875 (D.S.C. Sept. 14, 2016); *United States v. Torres*, 2016 WL 4821223

courts have found the NIT Warrant void *ab initio*, but concluded the evidence was admissible pursuant to the good-faith exception.[12] In addition to the court below, only three district courts have held the NIT Warrant void *ab initio* and refused to apply the good-faith exception. *See United States v. Workman*, 2016 WL 5791209 (D. Colo. Sept. 6, 2016); *United States v. Arterbury*, No. 15-CR-182 (N.D. Okla. May 12, 2016); *United States v. Levin*, 2016 WL 2596010 (D. Mass. May 5, 2016).[13]

SUMMARY OF ARGUMENT

The district court suppressed the NIT-derived evidence after finding that, although the FBI had a warrant to use the NIT to track down Playpen users cloaked in anonymity by the Tor network, the warrant was issued by a magistrate judge in the wrong district and violated Rule 41(b). Twenty-four

---

(W.D. Tex. Sept. 9, 2016); *United States v. Henderson*, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *United States v. Adams*, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016); *United States v. Acevedo-Lemus*, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Rivera*, No. 15-CR-266 (E.D. La. July 20, 2016); *United States v. Werdene*, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *United States v. Epich*, 2016 WL 953269 (E.D. Wisc. March 14, 2016); *United States v. Stamper*, No. 15-CR-109 (S.D. Ohio, Feb. 19, 2016); *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

[12] *See United States v. Scarbrough*, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016); *United States v. Broy*, 2016 WL 5172853 (C.D. Ill. Sept. 21, 2016); *United States v. Ammons*, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016).

[13] The government has filed notices of appeal from the suppression orders in *Workman* and *Levin*.

lower federal courts have upheld the NIT Warrant, finding it authorized under Rule 41 or executed in good faith. The district court erred in finding otherwise.

First, the court erroneously concluded that Rule 41(b) did not authorize the NIT Warrant. Interpreted flexibly, as the Supreme Court has instructed, Rule 41(b)(4) empowered the magistrate judge to issue the warrant authorizing the use of the NIT as a tracking device. Although not a physical tracking device, like a beeper affixed to a car, the NIT operated similarly in the internet context: it augmented Playpen's child pornography content residing on the website server in the Eastern District of Virginia and, after a user made a virtual trip to that district to download Playpen content, the NIT followed that content back to the user's computer, where it caused the computer to send identifying information back to the government.

Second, the court misconstrued the nature of the alleged Rule 41(b) error in ordering suppression. Suppression is not an appropriate remedy for non-constitutional, non-prejudicial, and non-intentional violations of Rule 41, such as the violation alleged here. The magistrate judge's alleged mistaken interpretation of Rule 41(b)'s venue provisions did not implicate, let alone violate, the Fourth Amendment and therefore the alleged mistake was not of constitutional dimension. Non-constitutional violations of Rule 41 rarely, if ever, require suppression of evidence obtained from warrants, like the NIT

Warrant, that comply with the Fourth Amendment's probable cause, particularity, and judicial-approval requirements.

Finally, the court erred by refusing to apply the good-faith exception to the exclusionary rule. The court reasoned that good faith could never apply to a warrant issued in violation of Rule 41(b), but that reasoning is illogical and contrary to Supreme Court precedent. If good faith applies to violations of the Fourth Amendment, as established by *United States v. Leon*, 468 U.S. 897 (1984), it defies reason to say that good faith does not apply to mere violations of the Federal Rules of Criminal Procedure. The exclusionary rule is a remedy of last resort, applied only where it results in appreciable deterrence of flagrant, culpable law enforcement misconduct. Here, the error, if it was one, was made by the magistrate judge, not the FBI, making suppression an especially inapt and ineffective remedy. Moreover, the FBI acted reasonably in devising the NIT to track down and apprehend anonymous Playpen users. The FBI detailed its Playpen investigation and the utility of the NIT in an affidavit; presented it to a magistrate judge in the district where the website was located and the NIT would be deployed; obtained judicial authorization for the search; and executed the NIT according to the warrant's terms. That the NIT Warrant was later deemed invalid because the magistrate judge allegedly misapprehended her territorial authority does not vitiate the agents' objectively reasonable reliance on it.

Allowing Horton and Croghan to escape prosecution for a heinous crime that society has a significant interest in preventing simply because a judge made a non-constitutional, rule-based mistake offends basic concepts of justice.

ARGUMENT

I. THE DISTRICT COURT ERRED IN HOLDING THAT THE MAGISTRATE JUDGE LACKED AUTHORITY UNDER RULE 41(b)(4) TO ISSUE THE NIT WARRANT

The district court erroneously concluded that the magistrate judge did not have authority to issue the NIT Warrant pursuant to Rule 41(b)(4).

A. Standard of review

This Court "may reverse a suppression order not only if it rests on clearly erroneous findings of fact, but also 'if the ruling reflects an erroneous view of the applicable law.'" *United States v. Berry*, 113 F.3d 121, 122 (8th Cir. 1997).

B. Rule 41(b)(4) authorized the magistrate judge to issue the NIT Warrant

Rule 41(b)(4) authorized the magistrate judge in the Eastern District of Virginia to issue a warrant to install the NIT on the government-controlled Playpen server located within the district, and that warrant properly authorized use of the NIT to track the movement of information—the digital child pornography content requested by users who logged into Playpen's website—as it traveled from the server in the Eastern District of Virginia through the encrypted Tor network to its final destination: the users' activating computers,

wherever located. At that point, the NIT caused the activating computers to transmit specified network information back to the government over the open Internet, thus enabling the government to locate and identify the user. As numerous courts have determined, the NIT Warrant was thus validly issued pursuant to Rule 41(b)(4). *See Johnson*, 2016 WL 6136586, at **3-7; *Dzwonczyk*, No. 15-CR-3134, at 12-13; *Smith*, No. 15-CR-467, at 14-15; *Jean*, 2016 WL 4771096, at **15-17; *Eure*, 2016 WL 4059663, at *8; *Darby*, 2016 WL 3189703, at **11-12; *Matish*, 2016 WL 3545776, at **17-18.

The court below, however, found subdivision (b)(4) inapplicable, declaring the NIT was not a tracking device. The district court's narrow interpretation of Rule 41(b)(4) conflicts with decisions from the Supreme Court and this Court, which have urged a "flexible" interpretation of Rule 41 to include within its scope electronic intrusions authorized upon a finding of probable cause. *United States v. New York Tel. Co.*, 434 U.S. 159, 169 & n.16 (1977) (upholding a 20-day search warrant for a pen register to collect dialed telephone number information, despite the fact that Rule 41's definition of "property" did not, at that time, include such information and required that a search be conducted within 10 days); *United States v. Falls*, 34 F.3d 674, 678 (8th Cir. 1994) (upholding warrant authorizing silent video surveillance, despite the

fact that the list of items then subject to seizure under Rule 41 included only tangible objects, contraband, and persons).

The Supreme Court's flexible reading of Rule 41 was "reinforce[d]" by Rule 57(b), which provides, "[i]f no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute." *New York Tel. Co.*, 434 U.S. at 170 (internal quotation marks omitted). Stated another way, when presented with a constitutionally valid, and not statutorily prohibited, request for a search warrant, courts are empowered to read the language of Rule 41 broadly in determining whether the requested search falls within its scope. *Id.*; *see also Falls*, 34 F.3d at 678 (Rule 41(b) "must not be interpreted too narrowly"); *United States v. Villegas*, 899 F.2d 1324, 1334 (2d Cir. 1990); *United States v. Torres*, 751 F.2d 875, 878 (7th Cir. 1984). This flexible approach to Rule 41 vindicates Fourth Amendment interests by encouraging law enforcement to seek a warrant rather than resorting to warrantless searches justified by claims of exigency, and by allowing magistrate judges to issue warrants for searches that meet the requirements of the Fourth Amendment but may not fit neatly within Rule 41's parameters due to advances in technology. *See Falls*, 34 F.3d at 679 ("Rule 41(b) is flexible enough to encompass silent video surveillance" and "such surveillance is regulated by the requirements of the Fourth Amendment").

Rule 41(b)(4) allows a magistrate judge "to issue a warrant to install within the district a tracking device," which may be used "to track the movement of a person or property located within the district, outside the district, or both." The Rule defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b); *see* Fed. R. Crim. P. 41(a)(2)(E) (incorporating this definition). The Rule further defines "property" to include not only "tangible objects," but also "information." Fed. R. Crim. P. 41(a)(2)(A). Although the term "device" is not more specifically defined in the Rule, it is a word commonly used to describe "[a] thing made or adapted for a particular purpose." Oxford English Dictionary, https://en.oxforddictionaries.com/definition/device (last visited: November 11, 2016).

Applying these definitions, the NIT qualifies as a "tracking device" within the meaning of Rule 41(b)(4). As applied to older technologies, the Rule contemplates that a tracking device may be a mechanical tool used to track the movement of a tangible object—*e.g.*, a transmitter affixed to a container of chloroform placed in a vehicle traveling over public roadways, like the beeper in *United States v. Knotts*, 460 U.S. 276 (1983). As applied to newer technologies, the Rule envisions that a tracking device may be an electronic device used to track the movement of information—*e.g.*, computer instructions embedded in

digital content traveling on data highways, like the NIT in this case. The NIT comprised a set of "computer instructions" "designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government." (NIT Aff. ¶33.) The NIT would "augment" the digital content requested by Playpen users and, once a user's computer downloaded the requested content and the NIT, the NIT would "reveal to the government environmental variables and certain registry-type information that may assist in identifying the user's computer, its location, and the user of the computer." (NIT Aff. ¶¶33-34.)

Essentially, the NIT was designed to follow illegal child pornography content requested by a user who accessed Playpen in the Eastern District of Virginia, through the anonymous Tor network nodes, and back to the user's activating computer; at that point, the NIT caused the transmission of the location-identifying information back to the government over the open Internet, thus circumventing Tor's encryption and allowing the government to identify and locate the user. Similar to a transmitter affixed to an automobile that is programmed to send location-enabling signals (like GPS coordinates) back to a government-controlled receiver at pre-determined intervals, the NIT augmenting the digital content requested by a Playpen user was designed to send location-enabling information (like an actual IP address) back to a government-

controlled computer when the illegal child pornography content reached its ultimate destination—the user's activating computer. Thus, although not a physical beeper affixed to a tangible object, the NIT operated as a digital tracking device of intangible information within the meaning of Rule 41(b)(4).

The NIT also was installed in the Eastern District of Virginia, as required by Rule 41(b)(4), which authorizes a magistrate judge to issue a warrant "to install within the district a tracking device." After being installed in the Eastern District of Virginia, the NIT only moved outside the district after a Playpen user entered the district to retrieve the illegal website content it augmented. Agents deployed the NIT alongside Playpen's digital content on the government-controlled server in the Eastern District of Virginia. (NIT Aff. ¶32.) This deployment constituted installation of a tracking device under Rule 41, as users then retrieved the NIT from the Playpen server by logging on and downloading information from that server. Any person seeking to access Playpen's child pornography content thus had to make, "in computer language, 'a virtual trip' via the Internet to Virginia," where the server was located. *Matish*, 2016 WL 3545776, at *18; *Dzwonczyk*, No. 15-CR-3134, at 13 (same); *Smith*, No. 15-CR-467, at 14-15 (same); *Darby*, 2016 WL 3189703, at *12 (same). When an individual entered his username and password on the Playpen website, it triggered installation of the NIT; both of these actions occurred in the Eastern

District of Virginia. (NIT Aff. ¶33.) Thus, for purposes of Rule 41's tracking-device provision, the NIT was installed at the location where it was obtained by a Playpen user (the Playpen server in the Eastern District of Virginia), not where the NIT ultimately disclosed the location-identifying information (the user's computer). And like a tangible tracking device, it followed the digital information or "property" obtained from Playpen in Virginia to its destination, namely each defendant's computer in Iowa, and reported that location back to government agents.

Rather than read Rule 41(b) "flexibl[y]," *Falls*, 34 F.3d at 679, the district court interpreted its venue provisions rigidly. Focusing exclusively on Rule 41(a)(2)(E)'s "person or object" language, the court reasoned that the NIT "did not 'track' the 'movement of a person or object,'" but "caused computer code to be installed on the activating user's computer." (DCD1 39, p.10.) And, the court concluded, Rule 41's "plain language" does not "support so broad a reading as to encompass the mechanism of the NIT." (*Id.*) But Rule 41(b) is "broad enough" to "include" the NIT "within its scope." *Falls*, 34 F.3d at 678-79. Just as *Falls* held that Rule 41(b) was "flexible enough" to encompass "silent video surveillance" though the Rule spoke only of tangible items, *id.*, Rule 41's tracking-device language is flexible enough to encompass the NIT, which tracks the movement of computer instructions embedded on digital content. The

court's finding is contrary to the spirit of Rule 41(b) generally and reflects an overly technical interpretation of Rule 41(b)(4)'s "tracking device" provision specifically.

The district court also erred by finding the NIT was not a tracking device because Playpen users "never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district." (DCD1 39, p.11 (internal quotation marks omitted).) The court's analysis misses the point. A Playpen user logged into the Playpen server and sent commands directing the server to return information to him, and the server complied with those commands. That the user did not have administrator-level control over the computer server hosting the Playpen website does not mean that the user did not control his access to Playpen or its illegal content. Unless and until a user affirmatively logged onto the Playpen website in the Eastern District of Virginia, where the NIT had already been embedded, the NIT could not be deployed. *See Jean*, 2016 WL 4771096, at *17 ("undisputed that *but for* [the defendant] electronically travelling in search of child pornography to the [Playpen server] in Virginia, the NIT could not have been deployed"); *Smith*, No. 15-CR-467, at 14-15 (defendant caused NIT's deployment by entering district via Internet to avail himself of Playpen's child pornography content).

II. THE DISTRICT COURT ERRED IN HOLDING THAT THE PURPORTED RULE 41(b) VIOLATION REQUIRED SUPPRESSION

Even if Rule 41(b)(4) did not authorize the NIT Warrant, the district court erred in ordering suppression because the alleged Rule 41 violation was not of constitutional dimension, did not prejudice Horton or Croghan, and was not intentional.

A. Standard of review

This Court reviews de novo "'whether the Fourth Amendment was violated.'" *United States v. Welch*, 811 F.3d 275, 279 (8th Cir. 2016) (quoting *United States v. Bell*, 480 F.3d 860, 863 (8th Cir. 2007)). Similarly, the district court's legal findings concerning the nature of, and appropriate remedy for, the alleged Rule 41 violation are reviewed de novo. *See Falls*, 34 F.3d at 678; *United States v. Gatewood*, 786 F.2d 821, 824-25 (8th Cir. 1986).

B. Suppression may not be used to remedy a non-constitutional Rule 41(b) violation unless a defendant shows prejudice or bad faith, and neither Horton nor Croghan have made such a showing

This Court has repeatedly affirmed that, "[a]bsent a constitutional infirmity," the exclusionary rule is only applied "to violations of Federal Rule 41 that prejudice a defendant or show reckless disregard of proper procedure." *United States v. Hyten*, 5 F.3d 1154, 1157 (8th Cir. 1993); *see also United States v. Turner*, 781 F.3d 374, 387 (8th Cir.), *cert. denied*, 136 S. Ct. 208 (2015); *United*

States v. Bieri, 21 F.3d 811, 816 (8th Cir. 1994); *United States v. Freeman*, 897 F.2d 346, 350 (8th Cir. 1990). Thus, "unless" the Rule 41 "defect permitted an unconstitutional warrantless search," the prejudicial-error rule applies. *Gatewood*, 786 F.2d at 824.[14]

In this case, the district court committed two errors in analyzing the nature of, and remedy for, the alleged Rule 41(b) violation. First, the court mistakenly found the alleged error, which was essentially one of venue, to be of constitutional magnitude and erroneously concluded that suppression was required without regard to prejudice or good faith. Second, the court erred in finding that Horton and Croghan were prejudiced.

1. The alleged Rule 41(b) violation was not of constitutional dimension

The threshold question in determining whether a Rule 41 violation may justify the harsh sanction of suppression is whether the error rises to the level of

[14] Numerous other federal courts of appeals have adopted essentially the same standard. *See United States v. Burgos-Montes*, 786 F.3d 92, 109 (1st Cir.), *cert. denied*, 136 S. Ct. 599 (2015); *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000); *United States v. Chaar*, 137 F.3d 359, 362 (6th Cir. 1998); *United States v. Gerber*, 994 F.2d 1556, 1560 (11th Cir. 1993); *United States v. Luk*, 859 F.2d 667, 671 (9th Cir. 1988); *United States v. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988); *United States v. Anderson*, 851 F.2d 384, 390 (D.C. Cir. 1988); *United States v. Comstock*, 805 F.2d 1194, 1207 (5th Cir. 1986); *United States v. Stefanson*, 648 F.2d 1231, 1235 (9th Cir. 1981); *United States v. Pennington*, 635 F.2d 1387, 1390 (10th Cir. 1980); *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975).

a Fourth Amendment violation. *Hyten*, 5 F.3d at 1157; *see Burke*, 517 F.2d at 386 ("[C]ourts should be wary in extending the exclusionary rule in search and seizure cases to violations which are not of constitutional magnitude."). The alleged error in this case, which involved Rule 41(b)'s venue provisions, did not implicate, let alone violate, the Fourth Amendment's warrant requirements.

The Fourth Amendment requires that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized." U.S. Const. amend. IV. To give proper effect to the Warrant Clause, all warrants must be issued by a "neutral and detached magistrate," meaning a person who is disengaged from the activities of law enforcement and capable of determining whether probable cause existed for the requested search or seizure. *Shadwick v. City of Tampa*, 407 U.S. 345, 350 (1972) (internal quotation marks omitted). A warrant is therefore valid for purposes of the Fourth Amendment if it is (1) supported by probable cause, (2) sufficiently particular, and (3) issued by a neutral and detached magistrate. *See Dalia v. United States*, 441 U.S. 238, 255 (1979); *United States v. Faulkner*, 826 F.3d 1139, 1145-46 (8th Cir. 2016).

The NIT Warrant met these constitutional requirements. Horton and Croghan have never disputed that the NIT Warrant established probable cause to search the computers of users who logged into Playpen with the intent to

view, download, and disseminate child pornography. Similarly, they have never suggested the NIT Warrant was insufficiently particular, and every court to have decided the issue has held the NIT Warrant sufficiently particularized. *See* note 7 *supra*. Moreover, Horton and Croghan have never claimed that the magistrate judge to whom the warrant was presented was not neutral and detached. These undisputed facts demonstrate the error in the district court's suppression ruling because there is "no authority for applying the exclusionary rule to procedural violations which do not implicate the constitutional values of probable cause or description of particularity of the place to be searched and the items to be seized." *Freeman,* 897 F.2d at 348; *see also Torres*, 2016 WL 4821223, at *7 ("[N]on-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.") (citing *Comstock*, 805 F.2d at 200).

Notwithstanding the manifest constitutionality of the NIT Warrant, the district court deemed it void *ab initio*, reasoning that, because Rule 41(b) did not grant the magistrate judge authority to issue the NIT Warrant, she was without jurisdiction to do so and thus "there simply was no judicial approval." (DCD1 39, p.13 (internal quotation marks omitted).) The court's reasoning is flawed because it equates Rule 41(b)'s venue provisions with the Fourth Amendment's

warrant requirements. But the requirements of Rule 41 and the Fourth Amendment are not "coextensive." *United States v. Schoenheit*, 856 F.2d 74, 77 (8th Cir. 1988) (internal quotation marks omitted). While Rule 41(b) places limits on the territorial authority of magistrate judges to issue certain types of search warrants, the Fourth Amendment says nothing about where the magistrate's authority may be exercised. With respect to the issuing magistrate's authority, all the Constitution requires is that the warrant be issued by a neutral and detached magistrate who is divorced from law enforcement activities and capable of determining probable cause.[15] Here, the NIT Warrant was judicially approved for Fourth Amendment purposes because it was issued by a neutral and detached magistrate judge who determined that the warrant was supported by probable cause and particularly described the place to be searched and things to be seized. *See Faulkner*, 826 F.3d at 1145-46 (though "technical deficiency that the warrant specified a certain county for placement of the GPS device when it was actually placed in a neighboring county might be a violation of state law," it was "not a Fourth Amendment violation" because warrant supported by

[15] Proposed Rule 41(b)(6) changes the title of Rule 41(b) from "Authority to Issue a Warrant" to "Venue for a Warrant Application," a change that is "not substantive," but "makes clear that Rule 41(b) identifies the courts that may consider an application for a warrant, *not the constitutional requirements* for the issuance of a warrant, which must still be met." Advisory Committee Notes (emphasis added).

probable cause "as determined by a neutral magistrate"); *Freeman*, 897 F.2d at 350 (no Fourth Amendment violation for technical error in execution of warrant because it did not implicate probable cause or particularity).

Moreover, the magistrate judge plainly had authority—and thus jurisdiction—to issue the NIT Warrant for searches of activating computers *within* her district, *see* Rule 41(b)(1), and therefore the court's finding that the warrant was wholly void, entirely lacking judicial approval, is untenable. *Anzalone*, 2016 WL 5339723, at *11 (warrant not void at its issuance because magistrate judge had authority to issue warrant for search within her district); *Adams*, 2016 WL 4212079, at *6 (similar).

In sum, this alleged Rule 41(b) violation was not of constitutional magnitude. The soundness of this conclusion is reinforced by numerous decisions involving analogous Rule 41 provisions, in which courts held the violations non-constitutional and denied suppression. For example, courts have refused to suppress evidence where the warrant was issued by an unauthorized individual,[16] and where the warrant was requested or executed by an

[16] *See, e.g., United States v. Britt*, 959 F.2d 232 (4th Cir. 1992) (unpublished) (per curiam) (assuming issuance of warrant by unauthorized state judge violated Rule 41, "a technical breach of Rule 41, without more, does not mandate suppression of evidence" and since defendant "has not shown that the search violated fourth amendment principles . . . the exclusion of evidence would be inappropriate"); *Martinez-Zayas*, 857 F.2d at 136-37 (no plain error where federal

unauthorized individual.[17] Courts also have held, or stated in dicta, that suppression was not required where, as is alleged here, the warrant authorized a search that exceeded Rule 41's territorial limitations.[18]

These authorities establish that the alleged Rule 41(b) error in this case was not of constitutional dimension, and suppression was not justified. The authorities relied upon by the district court to conclude otherwise (DCD1 39, at pp.12-14) are not to the contrary. In *Krueger*, the Tenth Circuit bypassed the question "whether the Fourth Amendment contains a within-district limitation on magistrate judges' warrant-issuing authority," because the court held that the

---

warrant was issued by unauthorized individual in violation of Rule 41 because defendant's "Rule 41 claim is not of constitutional magnitude"); *Comstock*, 805 F.2d at 1207 (similar).

[17] *See, e.g., Freeman*, 897 F.2d at 348-50 (warrant requested by individual who was not "a federal law enforcement officer" violated Rule 41, but suppression not required because violation was non-fundamental and non-prejudicial) (internal quotation marks omitted); *Luk*, 859 F.2d at 673-74 (similar); *Pennington*, 635 F.2d at 1390 (similar); *Burke*, 517 F.2d at 386-87 (similar).

[18] *See, e.g., United States v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008) (stating, in dicta, that a violation of Rule 41(b) caused by the issuance of a warrant that authorized a search in another judicial district would not require suppression); *United States v. $64,000 in U.S. Currency*, 722 F.2d 239, 246 (5th Cir. 1984) (any Rule 41 violation that occurred when Louisiana judge issued warrant to search envelope seized in Utah and then brought to Louisiana did not warrant suppression); *United States v. Goff*, 681 F.2d 1238, 1240 & n.1 (9th Cir. 1982) (even if search warrant for items that were not yet in the district violated Rule 41, no suppression required).

defendant had established actual prejudice from the Rule 41(b) violation. *United States v. Krueger*, 809 F.3d 1109, 1115 (10th Cir. 2015). In *Glover*, which involved a challenge to the territorial provision of Title III, 18 U.S.C. § 2518(3), the D.C. Circuit relied on Rule 41(b)(2) to inform its interpretation of § 2518(3), but the court held only that a violation of § 2518(3) required suppression pursuant to Title III's statutory suppression provision; the court did not decide whether a violation of Rule 41(b)(2) required suppression under the Fourth Amendment. *United States v. Glover*, 736 F.3d 509, 514-16 (D.C. Cir. 2013). And in *Berkos*, the Seventh Circuit merely held Rule 41(b), which it said "deals with substantive judicial authority," inapplicable to 18 U.S.C. § 2703(a), because it found that § 2703(a) incorporated only the procedural provisions of Rule 41. *Berkos*, 543 F.3d at 398.

Berkos, in fact, undermines the district court's conclusion that suppression was required here because of the purportedly "substantive" nature of a Rule 41(b) violation (DCD1 39, p.13). Although the Seventh Circuit characterized Rule 41(b) as "a substantive provision," it emphasized that "violations 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." 543 F.3d at 396-97. The court explained that "allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant would be wildly

out of proportion to the wrong," and stated that, had the government made that argument, the court would have affirmed the denial of the defendant's motion to suppress on that basis alone. *Id*. at 396 (internal quotation marks omitted). In this case, the government made that argument (DCD1 36, p.15), and the district court erred in rejecting it. *See United States v. Hornick*, 815 F.2d 1156, 1157-58 (7th Cir. 1987) ("In light of *Leon,* it is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the fourth amendment, that would call for suppression."). *Cf. Sanchez-Llamas v. Oregon*, 548 U.S. 331, 348 (2006) (violation of treaty provision that did not "implicate[] important Fourth and Fifth Amendment interests" did not trigger exclusionary rule, which applies "primarily to deter constitutional violations"); *United States v. Caceres*, 440 U.S. 741, 755-57 (1979) (violation of statutory requirements that go beyond the Constitution's demands does not justify suppression unless the statute itself specifies this remedy).

2. Horton and Croghan were not prejudiced by the alleged Rule 41(b) error

The district court also erred in finding that, if a showing of prejudice was required, Horton and Croghan were actually prejudiced. "To determine prejudice," this Court "ask[s] whether the search would have occurred had the rule been followed." *Welch*, 811 F.3d at 281 (internal quotation marks omitted); *see Hyten*, 5 F.3d at 1157. Given the evident constitutionality of the NIT

Warrant, the searches would have occurred had the NIT Warrant been presented to a federal magistrate judge in the Southern District of Iowa. *See* Rule 41(b)(1) ("a magistrate judge with authority in the district . . . has authority to issue a warrant to search for . . . property located within the district"). Such a magistrate judge surely would have authorized the very same searches of Horton and Croghan's computers that occurred. *See Darby*, 2016 WL 3189703, at *12 (finding no prejudice because Rule 41(b)(1) authorized search of defendant's computer, located in Eastern District of Virginia). *Cf. Martinez-Zayas*, 857 F.2d at 136 ("this warrant could have been obtained from a federal magistrate"); *United States v. Ritter*, 752 F.2d 435, 441 (9th Cir. 1985) (declining to suppress evidence because there was "no indication that a federal magistrate would have handled the search differently than did the state judge").[19]

[19] Suppression for a Rule 41 violation is also authorized if "reckless disregard of proper procedure is evident." *Bieri*, 21 F.3d at 816. As demonstrated *infra*, the FBI acted in good faith when it executed the NIT Warrant. That, in turn, "precludes any finding of reckless disregard of proper procedure on their part." *Hyten*, 5 F.3d at 1157; *see Bieri*, 21 F.3d at 816 ("because no evidence exists that the officers acted in bad faith, it follows that there was no reckless disregard of proper procedure by the state officers").

III. THE DISTRICT COURT ERRED WHEN IT SUPPRESSED EVIDENCE OF CHILD PORNOGRAPHY OBTAINED BY FEDERAL AGENTS ACTING IN OBJECTIVELY REASONABLE RELIANCE ON THE NIT WARRANT

As we have shown, the NIT Warrant was authorized by Rule 41. However, because evidence seized pursuant to a search warrant issued by a magistrate judge that is later determined to be invalid "will not be suppressed if the executing officer's reliance upon the warrant was objectively reasonable," *United States v. Proell*, 485 F.3d 427, 430-32 (8th Cir. 2007), this Court may choose to bypass the Rule 41 question and simply assess good faith. As we demonstrate *infra,* the district court's determination that the good-faith exception to the exclusionary rule never applies to search warrants later deemed "void" is contrary to Supreme Court precedent, and its conclusion that the agents did not act in good faith reliance on the NIT Warrant is unsupported by the record.

A. Standard of review

This Court reviews the district court's "application of the *Leon* exception de novo." *United States v. Houston*, 665 F.3d 991, 994 (8th Cir. 2012) (internal quotation marks omitted); *Berry*, 113 F.3d at 124 ("[w]e review de novo" district court's conclusion that "good-faith exception did not apply").

B. The district court erred in holding the good-faith exception to the exclusionary rule categorically inapplicable to warrants later deemed "void"

Suppression is a remedy of last resort, to be used for the sole purpose of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression outweigh its heavy costs. *Davis v. United States*, 564 U.S. 229, 236-37 (2011); *Herring v. United States*, 555 U.S. 135, 140-41 (2009). "The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring*, 555 U.S. at 141 (citing *Illinois v. Gates*, 462 U.S. 213, 223 (1983)). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144.

These principles are reflected in the good-faith exception to the exclusionary rule articulated in *Leon*: when police act in "objectively reasonable reliance on a subsequently invalidated search warrant" obtained from a neutral and detached magistrate, "the marginal or nonexistent benefits produced by suppressing evidence . . . cannot justify the substantial costs of exclusion." 468 U.S. at 922. The good-faith exception thus recognizes that, "when an officer acting with objective good faith has obtained a search warrant from a judge or

magistrate and acted within its scope . . . there is no police illegality and thus nothing to deter." *Id.* at 920-21.

The district court refused to apply the good-faith exception—"*Leon* is inapplicable"—because, in its view, it does not apply when law-enforcement agents rely on a warrant deemed "void." (DCD1 39, pp.13-15.) Specifically, the court opined, because Rule 41(b) did not authorize the issuance of the NIT Warrant, the warrant was "void from the outset" and "akin to no warrant at all." (*Id.* at p.13 (internal quotation marks omitted).)

The district court's reasoning ignores controlling Supreme Court precedent, and should be rejected. *Herring*, for example, invoked the good-faith exception in a case involving the arrest of an individual pursuant to an arrest warrant that had been "recalled five months earlier"; at the time of the officer's arrest of the individual, the warrant was thus non-existent. 555 U.S. at 137-38. The Supreme Court nonetheless held that suppression was inappropriate where "an officer reasonably believes there is an outstanding arrest warrant, but that belief turns out to be wrong," even though the error was due to police negligence. *Id.* at 137. Similarly, in *Arizona v. Evans*, 514 U.S. 1, 15-16 (1995), another case involving the arrest of an individual pursuant to a quashed, and therefore non-existent, warrant, the Court held that the arresting officer had acted "objectively reasonably when he relied upon the police computer record," which contained

an error made by a court clerk, and that "the *Leon* framework supports a categorical exception to the exclusionary rule for clerical errors of court employees." In *Davis*, the Court invoked the good-faith exception in a case involving the warrantless search of a car's driver incident to his arrest pursuant to binding legal precedent later overruled, 564 U.S. at 241. And, in *Illinois v. Krull*, 480 U.S. 340, 354-57 (1987), the Court invoked the good-faith exception in a case involving the warrantless search of a junkyard pursuant to a state statute later declared unconstitutional. In all of those cases, the Supreme Court found that the warrantless search or arrest at issue violated the Fourth Amendment, and yet the Court found suppression inappropriate because law enforcement had acted in objectively reasonable reliance on the subsequently invalidated warrant, statute, or legal precedent that would have authorized the search or arrest, and exclusion therefore would not deter future police misconduct.

The facts of this case fall comfortably within this body of law and mandate the same result. Assuming that the NIT Warrant was void because the magistrate judge lacked territorial authority to issue it, and further assuming that the FBI's use of the NIT thereby amounted to an unconstitutional warrantless search or was somehow prejudicial, suppression is not warranted because the agents acted in objectively reasonable reliance on the subsequently invalidated warrant and were not culpable for the magistrate judge's purported error. *See*

Davis, 564 U.S. at 240 ("in 27 years of practice under *Leon*'s good-faith exception, we have never applied the exclusionary rule to suppress evidence obtained as a result of nonculpable, innocent police conduct") (internal quotations and citation omitted).

In deeming the good-faith exception inapplicable, the district court "adopt[ed]" the reasoning of *United States v. Levin*, No. 15-12071 (D. Mass. 2016). (DCD1 39, p.14.) *Levin* purported to distinguish the above precedents, noting none involved a warrant that was void *ab initio*. But such a distinction—between warrants that are "voidable" due to judicial error and warrants that are "void" due to the absence of judicial authority—is unavailing. As *Leon* and its progeny make clear, the legal status of a warrant under the Fourth Amendment does not, as a categorical matter, limit the reach of the good-faith exception. Rather, application of the good-faith exception requires a "rigorous weighing of [the exclusionary rule's] costs and deterrence benefits," and "[t]he basic insight of the *Leon* line of cases is that the deterrence benefits of exclusion 'var[y] with the culpability of the law enforcement conduct' at issue." *Davis*, 564 U.S. at 238 (quoting *Herring,* 555 U.S. at 143). Accordingly, a court's focus in conducting that cost-benefit analysis is on "the flagrancy of the police misconduct at issue." *Id.* (internal quotation marks omitted). Here, the district court erroneously focused only on the reasons why the NIT Warrant was supposedly "no warrant

at all" (DCD1 39, at p.13 (internal quotation marks omitted)), which may explain why the court found the NIT search unconstitutional but says nothing about the agents' conduct, and therefore does not answer the critical question of whether suppression is an appropriate remedy. *Hudson v. Michigan*, 547 U.S. 586, 592 (2006) ("[B]ut-for causality is only a necessary, not a sufficient, condition for suppression."); *Gates*, 462 U.S. at 223 ("The question whether the exclusionary rule's remedy is appropriate in a particular context has long been regarded as an issue separate from the question whether the Fourth Amendment rights of the party seeking to invoke the rule were violated by police conduct.").

In this case, the purported error rendering the NIT Warrant "void"—the absence of territorial authority to issue the warrant—was made by the magistrate judge, not law enforcement. The Supreme Court has consistently expressed a "strong preference for warrants" and mandated "great deference" to a magistrate's determination that a warrant is constitutionally sufficient. *Leon*, 468 U.S. at 914 (internal quotation marks omitted); *see Messerschmidt v. Millender*, 132 S. Ct. 1235, 1245 (2012). Nonetheless, *Levin*—the authority embraced by the court below—also reasoned that, though the police may defer to a magistrate's probable-cause determination, such deference is inappropriate when a magistrate judge determines its own jurisdiction. But it is just as much a question for the magistrate judge whether Rule 41(b) provides territorial authority to issue

a warrant as it is whether the affidavit establishes probable cause. Accordingly, if an officer may defer to a magistrate's determination that a warrant complies with the Fourth Amendment, he may surely defer to a magistrate's determination that a warrant complies with the Federal Rules of Criminal Procedure. In both situations, the error, if any, is attributable to the judge, not the officer, leaving "no police illegality and thus nothing to deter." *Leon*, 468 U.S. at 921. Moreover, if "[p]enalizing the officer for the magistrate's error" in assessing compliance with the Fourth Amendment's probable cause requirement "cannot logically contribute to the deterrence of Fourth Amendment violations," *id.*, then penalizing the FBI for the magistrate's error in assessing compliance with Rule 41(b)'s venue provisions, which are not constitutionally required, likewise cannot deter future Fourth Amendment violations. *See Eure*, 2016 WL 4059663, at **8-9.

In concluding that suppression was the only remedy for the allegedly "void" NIT Warrant, the district court ignored the Supreme Court's admonition that "suppression is not an automatic consequence of a Fourth Amendment violation." *Herring*, 555 U.S. at 137, 141. The decision to exclude evidence is divorced from whether a Fourth Amendment violation occurred. Suppression thus depends not on the nature of the constitutional violation, as the district court erroneously concluded, but on the culpability and severity of police (not

judicial) misconduct and whether exclusion will deter future Fourth Amendment violations. *Id*. at 144.

C. The district court erred in alternatively concluding that the agents did not act in objectively reasonable, good-faith reliance on the NIT Warrant

"The 'good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the [issuing judge's] authorization.'" *Houston*, 665 F.3d at 995 (quoting *Proell*, 485 F.3d at 430). The district court alternatively concluded that, even if it were to hold that the good-faith exception could apply to circumstances involving a search pursuant to a warrant issued without jurisdiction, the exception was inapplicable here because "law enforcement was sufficiently experienced" and there "existed adequate case law casting doubt on magisterial authority to issue precisely this type of NIT Warrant." (DCD1, 39 pp.18-19.) It was not reasonable for the district court to conclude that a well trained officer should have understood that the NIT warrant was illegal despite the authorization of the Eastern District of Virginia magistrate judge.

First, as detailed above, the agent could have reasonably believed that the warrant was constitutional and complied with Rule 41, specifically, subsection (b)(4), as numerous district courts have held, *see* p.19 *supra*. Indeed, when the FBI sought judicial approval for this NIT Warrant, it had received judicial

approval to use NITs in other cases. *See*, *e.g., United States v. Laurita*, 2016 WL 4179365 (D. Neb. Aug. 5, 2016) (re-affirming use of similar NIT pursuant to warrant issued in 2012); *see also* Docket #63, *United States v. Levin*, No. 1:15-CR-10271 (D. Mass.) (reproduced at App. 165-66) (identifying three unsealed, judicially-authorized NIT warrants); *but cf. In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (denying warrant for use of far more invasive NIT).

Second, though no federal appellate court has thus far addressed the validity of an NIT warrant under Rule 41(b) since this NIT Warrant was issued, lower courts have differed on the question.[20] The court below conceded this, noting "numerous district courts" have "reached varying conclusions on the legal issues at play." (DCD1 39, p.5.) The "varying" legal conclusions of these "numerous" federal courts proves that the "mandate of Rule 41(b)" is not "plain," as the district court simultaneously—and incongruously—suggested. (*Id.* at p.19 (internal quotation marks omitted)). It was therefore not unreasonable for the FBI agents to have deferred to, and relied on, the magistrate judge's determination of her territorial authority to issue the NIT Warrant. *See*

[20] *See, e.g.*, *Allain*, 2016 WL 5660452, at *12 n.10 (recognizing courts' differing views of the magistrate's authority to issue the NIT Warrant). *Compare Jean*, 2016 WL 4771096, at **16-17 (no violation of Rule 41(b)) *with Michaud*, 2016 WL 337263, at *6 (technical violation of Rule 41(b)).

Leon, 468 U.S. at 914 (mandating deference to magistrate's decision where "[r]easonable minds" have differed on legal sufficiency of warrant); *United States v. Barraza-Maldonado*, 732 F.3d 865, 869 (8th Cir. 2013) ("Officers should not be faulted for adhering to existing precedent until that precedent is authoritatively overruled."); *see also Heien v. North Carolina*, 135 S. Ct. 530, 540 (2014) (finding officer's interpretation of ambiguous "stop lamp" law, which had not previously been construed by state appellate courts, objectively reasonable).

Third, though recognizing numerous federal *judges* have reached varying conclusions about the NIT Warrant's validity, the district court erroneously determined that the law-enforcement *agents* should have known the NIT Warrant was invalid. Thus, the court opined, suppression was necessary to "deter law enforcement from seeking warrants from judges lacking jurisdiction to issue them." (DCD1 39, p.18.) But that is precisely the omniscient state of mind eschewed by *Leon* and this Court. In *Houston*, for example, a state agent seized the defendant's computers in South Dakota and transported them to Wisconsin, where the defendant was being investigated for a six-year-old act of sexual molestation and possession of child pornography. 665 F.3d at 993-94. A detective then applied for a warrant to search these computers, and a state magistrate authorized a search for evidence relating to violations of certain Wisconsin criminal statutes. *Id.* at 994. In arguing the good-faith exception did

not apply, the defendant contended no reasonable officer could believe that computers seized in South Dakota might contain evidence of a six-year-old violation of a Wisconsin statute. *Id.* at 996. *Houston* rejected this claim, declining to "impose" on an officer the "duty" of ascertaining the "legal and jurisdictional limits of a judge's power to issue interstate search warrants as well as statutory limitation periods for prosecutors." *Id.* (footnote omitted). It is "the magistrate's responsibility to determine whether the officer's allegations constitute probable cause and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment." *Id.* (internal quotation marks omitted); *see also Leon*, 468 U.S. at 921 ("In the ordinary case, an officer cannot be expected to question the magistrate's . . . judgment that the form of the warrant is technically sufficient."); *Berry*, 113 F.3d at 124 ("The municipal judge signed both the affidavit and the warrant and, as the final reviewing authority, he must shoulder the ultimate responsibility for the clerical error in the warrant."); *Bieri*, 21 F.3d at 816 ("We believe Deputy Ringler could easily have assumed the warrant, issued by a judge with many years of experience, was lawful."); *Libbey-Tipton*, No. 16-CR-236, at 12 ("The FBI agents can hardly be faulted for failing to understand the intricacies of the jurisdiction of federal magistrates.") (alterations and internal quotation marks omitted).

Fourth, in finding that the FBI agents could not have reasonably believed the NIT Warrant was properly issued in the face of "case law casting doubt" on the magistrate's authority, the district court cited only three authorities: *Glover*, *Krueger*, and *In re Warrant to Search a Target Computer*. (DCD1 39, pp.18-19.) But none of these decisions cast doubt on the Eastern District of Virginia magistrate judge's Rule 41 authority. *Glover* and *Krueger*, we have explained, are inapt; neither assessed the lawfulness of a tracking-device warrant like the NIT. As for *In re Warrant,* that decision addressed the installation of a different, more invasive NIT to a computer in an unknown location to discover the identity of criminal suspects. That court found it "plausible" that the NIT was a "tracking device," but decided it did not satisfy Rule 41(b)(4)'s installation requirement because there was "no showing that the installation of the 'tracking device' (*i.e.* the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet." 958 F. Supp. 2d at 758.

Finally, though the district court vaguely intimated—via a parenthetical quotation from *Levin*—that the agent's conduct reflected "'systemic error or reckless disregard of constitutional requirements'" (DCD1 39, p.18), the court pointed to nothing in the record to support such a conclusion. This omission is understandable because the record establishes that the FBI committed no error

at all and acted with scrupulous regard for the requirements of Rule 41 and the Constitution. Faced with the daunting task of apprehending possibly thousands of individuals engaged in repugnant child pornography crimes, but cloaked in anonymity by their use of Tor, the FBI developed a sophisticated NIT to unmask and locate suspected criminals; it presented a detailed warrant affidavit, explaining the NIT and its operation, establishing probable cause, and describing the places to be searched and things to be seized with particularity, to a neutral and detached magistrate judge in the district with the strongest known connection to the criminal activity under investigation; it obtained and relied upon a facially valid warrant authorizing its use of the NIT; and it executed the search according to the terms of the warrant. That the warrant was later found defective because of the magistrate judge's mistaken interpretation of her territorial authority pursuant to Rule 41(b) does not render the agents' reliance on the warrant objectively unreasonable, just like it is not objectively unreasonable for a police officer to rely on a magistrate judge's mistaken assessment of probable cause. *See Utah v. Strieff*, 136 S. Ct. 2056, 2064 (2016) (holding seizure without probable cause not flagrant Fourth Amendment violation); *see also Allain*, 2016 WL 5660452, at *12 ("The FBI's investigation into Playpen involved sophisticated and novel technology—used both by the operators and users of Playpen as well as the federal investigators—and the FBI

made a reasonable attempt to structure a search warrant that complied with rules that have not evolved as quickly as the technology."); *Darby*, 2016 WL 3189703, at *13 (FBI "did the right thing" and "should be applauded for its actions in this case").

As we have described, the FBI agents' conduct was neither deliberate nor culpable. Moreover, the Rule 41(b) violation, if it was one, was committed by the magistrate judge and "punishing the errors of judges is not the office of the exclusionary rule." *Davis*, 564 U.S. at 238-39 (internal quotation marks omitted).[21] The costs of suppression, on the other hand, are substantial. The court's suppression order, if affirmed, would exclude "reliable, trustworthy evidence bearing on [Horton and Croghan's] guilt or innocence" of an abhorrent crime that society has a significant interest in deterring. *Id.* at 237. "Considering the unspeakable harm caused by child pornography, and the creative and limited conduct of the FBI that was undertaken to mitigate that harm, . . . suppression is entirely unwarranted here." *Acevedo-Lemus*, 2016 WL 4208436, at *8. Any "error in procedure was inadvertent and the harsh application of the therapeutic

[21] The absence of any deterrence benefit is underscored by the proposed amendment to Rule 41(b), which, if enacted, will expressly permit magistrate judges to authorize warrants for remote electronic searches such as the one in this case. *See* note 6 *supra*.

exclusionary rule in the circumstances" was "entirely inappropriate." *United States v. Burgard*, 551 F.2d 190, 193 (8th Cir. 1977).

CONCLUSION

For these reasons, the government respectfully requests that the Court reverse the district court's order suppressing evidence.

Respectfully submitted,

KEVIN E. VANDERSCHEL
United States Attorney
Southern District of Iowa

KATHERINE MCNAMARA
Assistant United States Attorney
Southern District of Iowa

LESLIE R. CALDWELL
Assistant Attorney General

SUNG-HEE SUH
Deputy Assistant Attorney General

/s/ David B. Goodhand
DAVID B. GOODHAND
Appellate Section, Criminal Division
United States Department of Justice
950 Pennsylvania Ave. NW, Rm. 1714
Washington, DC 20530
202-353-4468
david.goodhand@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on November 22, 2016, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Eighth Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ David B. Goodhand
DAVID B. GOODHAND
Appellate Section, Criminal Division
United States Department of Justice
950 Pennsylvania Ave. NW, Rm. 1714
Washington, DC 20530
202-353-4468
david.goodhand@usdoj.gov

CERTIFICATE OF COMPLIANCE

I hereby certify that the brief has been scanned for viruses and that to the best of my knowledge the brief is virus free.

I further certify that Word software was used to prepare this brief.

I further certify that this brief complies with the type-volume limitations as set forth in Fed. R. App. P. 32(a)(7)(c). There are 50 pages containing 11,655 words, using Calisto MT 14 point, in the brief.

/s/ David B. Goodhand
DAVID B. GOODHAND
Appellate Section, Criminal Division
United States Department of Justice
950 Pennsylvania Ave. NW, Rm. 1714
Washington, DC 20530
202-353-4468
david.goodhand@usdoj.gov