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 REPLY 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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page**

Statutes and Rules

Other Authorities

INTRODUCTION

In our opening brief, we showed that the district court erred in suppressing evidence derived from the NIT Warrant. That warrant was authorized by Fed. R. Crim. P. 41(b)(4) and, in any event, the good-faith exception to the exclusionary rule applied. Two subsequent developments bolster these arguments. First, nine more district courts have denied suppression.[1] Thirty-three district courts thus now agree with the government's no-suppression position. Second, an amendment to Rule 41 went into effect on December 1, 2016, that places the validity of warrants like the NIT Warrant beyond reproach. Rule 41(b)(6) now provides magistrate judges with the authority to issue warrants when the location of electronic media or information "has been concealed through technological means." This provision confirms application of the good-faith exception here because there is minimal—if any—deterrence benefit to be found in sanctioning law enforcement conduct that the Federal

[1] *See United States v. Dzwonczyk*, 2016 WL 7428390 (D. Neb. Dec. 23, 2016); *United States v. Vortman*, 2016 WL 7324987 (N.D. Cal. Dec. 16, 2016); *United States v. Hammond*, 2016 WL 7157762 (N.D. Cal. Dec. 8, 2016); *United States v. Duncan*, 2016 WL 7131475 (D. Or. Dec. 6, 2016); *United States v. Owens*, 2016 WL 7053195 (E.D. Wisc. Dec. 5, 2016); *United States v. Tippens*, No. 16-CR-5110 (W.D. Wa. Nov. 30, 2016); *United States v. McLamb*, No. 16-CR-92 (E.D. Va. Nov. 28, 2016); *United States v. Lough*, 2016 WL 6834003 (N.D. W. Va. Nov. 18, 2016); *United States v. Kienast*, 2016 WL 6683481 (E.D. Wisc. Nov. 14, 2016).

Rules' drafters, Congress, and the Supreme Court have concluded is appropriate.

I. THE GOOD-FAITH EXCEPTION APPLIES BECAUSE THE FBI REASONABLY RELIED ON THE NIT WARRANT

As *Leon* teaches, this Court may forgo assessing the validity of the NIT Warrant and "turn[] immediately to a consideration of the officers' good faith." *United States v Leon*, 468 U.S. 897, 925 (1984). Though Magistrate Judge Buchanan certainly had authority to issue the NIT Warrant pursuant to Rule 41(b)(4), *see* Part III.A *infra*, we believe it makes sense to assess "good faith" in this case because the Rule 41(b)(6) amendment plainly demonstrates that the FBI's reliance on the NIT Warrant was objectively reasonable and that there is no deterrence benefit to suppression.

In April 2016, the Supreme Court approved Rule 41(b)(6), which provides magistrate judges "in any district where activities related to a crime may have occurred" with the authority to issue warrants "to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district" if the district "where the media or information is located has been concealed through technological means." This Rule 41 provision was intended, in part, to address the fact that "child abusers sharing child pornography may use proxy services designed to hide their true IP

addresses,"[2] which is what Croghan and Horton did when they used Tor to mask the locations of their illegal activities. Congress approved Rule 41(b)(6)'s grant of authority by not acting on the amendment, and it went into effect on December 1, 2016.

This "amendment is evidence that the drafters of the Federal Rules do not believe that there is anything unreasonable about a magistrate issuing this type of warrant; the Rules had simply failed to keep up with technological changes." *United States v. Darby*, 2016 WL 3189703, at *13 (E.D. Va. June 3, 2016). "That is, there is nothing unreasonable about the scope of the [NIT] warrant itself," *id.*, and the FBI agents acted with the objectively reasonable belief that the NIT Warrant comported with the Fourth Amendment. Moreover, suppression is a remedy of last resort, to be used for the "sole" purpose of deterring "future" violations by law-enforcement authorities. *Davis v. United States*, 564 U.S. 229, 236-37 (2011). Thus, even if Rule 41(b)(4) did not authorize Magistrate Judge Buchanan to issue the NIT Warrant, future law-enforcement officers clearly may apply for and obtain such a warrant pursuant to Rule 41(b)(6). Accordingly, a Rule 41(b) violation is unlikely to recur and suppression here will have no

[2] Honorable Reena Raggi, Report of the Advisory Committee on Criminal Rules 8 (May 6, 2015), *available at* http://www.uscourts.gov/sites/default/files/2015-05-criminal_rules_report_0.pdf.

deterrent effect. *See United States v. Broy*, 2016 WL 5172853, at *9 (C.D. Ill. Sept. 21, 2016) (the "only benefit to suppression in this case would be ensuring magistrate judges are more careful about issuing NIT warrants in the future," but that "benefit would not last for long" because of Rule 41(b)(6)'s December 1 effective date and, at any rate, the "exclusionary rule is designed to control the conduct of *law enforcement*, not the conduct of federal judges").

A. The NIT Warrant Was Not Void *Ab Initio*

In arguing the good-faith exception to the exclusionary rule is inapplicable, Croghan ignores Rule 41(b)(6).[3] Instead, relying on Judge Gorsuch's concurrence in *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), Croghan asserts (at 25-26, 28-30) that the NIT Warrant was "no warrant

[3] For his part, Horton acknowledges the amendment but asserts (at 17-18) that it shows the government "was clearly aware that the NIT Warrant was not authorized when it made its application in February, 2015," thus confirming law enforcement acted in bad faith. But Horton points to nothing indicating that the FBI agents were actually aware of the proposed amendment. In any event, even assuming the executing agents were cognizant of it, "an awareness that Rule 41 was subject to amendment merely demonstrates 'recognized ambiguities in the Rule, not that [the government] acted with deliberate disregard for the rule." *Vortman*, 2016 WL 7324987, at *12 (quoting *United States v. Henderson*, 2016 WL 4549108, at *6 (N.D. Cal. Sept. 1, 2016)); *see also Hammond*, 2016 WL 7157762, at *5 ("That an amendment to Rule 41 (clarifying the propriety of warrants like the NIT Warrant, *i.e.*, warrants authorized by magistrate judges to remotely search computers whose locations are not known) was pending when the NIT warrant was issued also falls far below the bar of evidence that establishes deliberate disregard.").

at all" because the magistrate judge lacked "territorial authority" to issue it. And, Croghan contends, the good-faith exception does not apply to warrants void *ab initio*. This argument fails for several reasons.

First, Croghan nowhere addresses the point made in our opening brief (at 31) that Magistrate Judge Buchanan "plainly had authority—and thus jurisdiction—to issue the NIT Warrant for searches of activating computers *within* her district." Thus, as numerous courts have concluded, the suggestion that the NIT Warrant was *wholly* void and *entirely* lacking judicial approval is untenable. *See Duncan*, 2016 WL 7131475, at *3 ("warrant itself was not wholly without statutory authority, so it was not void when it was issued"); *Tippens*, No. 16-CR-5110, at p.18 (same); *United States v. Anzalone*, 2016 WL 5339723, at *11 (D. Mass. Sept. 22, 2016) (same); *United States v. Knowles*, 15-CR-875, p.22 (D.S.C. Sept. 14, 2016) (same).[4]

Second, the Supreme Court has repeatedly invoked the good-faith exception in similar situations where, for example, law-enforcement officers acted in objectively reasonable reliance on: a subsequently invalidated arrest warrant, *Herring v. United States*, 555 U.S. 135 (2009); a later-overruled legal

[4] Horton recognizes this point (at 10), but asserts that the government provided "[n]o authority" for its not-wholly-void "position." As the cases cited in the text demonstrate, however, there is abundant authority supporting this argument.

precedent, *Davis*, 564 U.S. at 241; or a statute ultimately deemed unconstitutional, *Illinois v. Krull*, 480 U.S. 340 (1987). Croghan tries to distinguish these cases (at 29-30), claiming those officers had at least relied on an "authority"—the warrant, legal precedent, or statute—that was valid at one point, as opposed to the NIT Warrant that was "void *ab initio*." Croghan's focus on *when* the warrant or statute was invalidated misses the point of *Herring* and *Davis*, which instruct that the exclusionary rule should only be applied when law enforcement are so culpable that exclusion can achieve meaningful deterrence that is worth the price paid by the justice system in suppressing evidence. The legal status of a warrant under the Fourth Amendment—whether void at the outset or "recalled five months" before it was executed, as in *Herring*, 555 U.S. at 137-38—is not what determines application of the good-faith exception. Indeed, adherence to a rule that depends solely on whether the magistrate judge had Rule 41(b) authority to issue the NIT Warrant at the outset would lead to absurd results: "evidence obtained through a warrant that was supported by probable cause, but that ran afoul of a jurisdictional statute, must be suppressed, but . . . evidence seized pursuant to a warrant later found not to be supported by probable cause, an issue of constitutional dimension, can be preserved by a finding of good faith." *United States v. Allain*, 2016 WL 5660452, at *11 n.8 (D. Mass. Sept. 29, 2016); *see also Lough*, 2016 WL 6834003, at *10 n.12 ("justifying

exclusion when a warrant is void *ab initio*, but inclusion when a warrant is non-existent, as in *Herring*, would require some semantic gymnastics").

Third, even Croghan's lone authority—*Krueger*—ultimately "ha[d] no occasion" to consider whether the good-faith exception could have applied because the government had waived that argument. 809 F.3d at 1113 n.5. And, in fact, the majority's analysis indicated the question of good faith is normally an important consideration when evaluating the appropriate remedy for a Rule 41(b) violation. The majority noted that the warrant in that case "clearly violate[d] Rule 41(b)(1)," *id.* at 1117, but then cited *Herring* with approval and contrasted the circumstances present in *Krueger* with those in the Sixth Circuit's decision in *United States v. Master*, 614 F.3d 236 (2010), where "'officers mistakenly, but inadvertently, presented the warrant to an incorrect magistrate.'" *Krueger*, 809 F.3d at 1117 & n.10 (quoting *Master*, 614 F.3d at 242-43). *Master* declined to exclude the evidence, finding "at first blush" that "'the benefits of deterrence'" did not "'outweigh the costs.'" 614 F.3d at 243 (quoting *Herring*, 555 U.S. at 141). *Krueger* also cited Tenth Circuit precedent that "explain[ed] that the exclusionary rule is appropriate only if the law enforcement activity at issue was not objectively reasonable." 809 F.3d at 1117. If anything, then, the majority's analysis in *Krueger* suggests that the good-faith exception remains available in a factual setting such as this case. Moreover, in Judge

Gorsuch's *Krueger* concurrence—the sole support for Croghan's void-*ab-initio* argument—Judge Gorsuch himself recognized that the good-faith exception could apply to warrants deemed void *ab initio*, declaring that whether "we lack a valid warrant . . . doesn't quite finish the story" because the "Fourth Amendment, after all, doesn't prohibit unwarranted searches but unreasonable ones." *Id.* at 1125 (Gorsuch, J., concurring). And, "[e]ven when an unreasonable search does exist," the court "must be persuaded that 'appreciable deterrence' of police misconduct can be had before choosing suppression as the right remedy." *Id.* (quoting *Herring*, 555 U.S. at 141).

B. The FBI's Investigation Was Lawful, Reasonable, and Necessary

Without apparent irony, Croghan also asserts (31-33) that the good-faith exception is inapplicable because the FBI's conduct "is worth deterring," claiming the agents: facilitated the dissemination of child pornography (by keeping Playpen up and running for two weeks); acted unlawfully (by failing to maintain "custody" of child-pornography images); and misled the magistrate judge (by telling her the places to be searched were within her district). Croghan did not proffer these contentions below and the district court did not rely on them.[5]

[5] In declining to invoke the good-faith exception, the district court opined only that the FBI agents should have understood "adequate case law" cast doubt

Even assuming the accuracy of Croghan's allegations about the FBI's Playpen investigation, they have little bearing on the lawfulness of the agents' actions in securing and executing the NIT Warrant, the only focus of *Leon*'s good-faith inquiry. If these allegations have any relevance, they are mainly relevant to a motion to dismiss on outrageous-government-conduct grounds, a litigation tactic pursued by other Playpen defendants but not Croghan or Horton. Appellees' inaction is understandable because the courts have uniformly denied the dismissal motions of these other Playpen defendants. *See*,

---

on the magistrate judge's authority to issue the NIT Warrant, a point the government refuted in its opening brief (at 32-33, 47). Horton resuscitates this claim (at 15-16), asserting three decisions showed that, in February 2015, "the government was on notice that courts disapproved of the government violating the jurisdictional limitations of Rule 41." But *Krueger* and *United States v. Glover*, 736 F.3d 509 (D.C. Cir. 2013), could not have put law-enforcement agents on "notice" of anything pertinent to the NIT Warrant, because neither court considered a Rule 41(b)(4) tracking-device warrant. And, though *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013), did involve a NIT, it was a different, more invasive, one, *id.* at 755. Moreover, unlike this case, where the NIT code was installed on the website operating on a Virginia-based server, *see* note 10 *infra*, in *In re Warrant*, "there [wa]s no showing that the installation of the 'tracking device' (i.e. the software) would take place within" the authorizing magistrate judge's district. *Id.* at 758. In contrast to these dissimilar legal authorities, as we noted in our opening brief (at 43-44), when agents sought approval for the NIT Warrant in this case, the FBI had already received authority to use four similar NITs. And, three additional NIT warrants recently have been unsealed. These were authorized in the District of Maryland before the FBI applied for the present NIT Warrant. *See* 13-MJ-1744, -1745, & -1746. Thus, at the time of this NIT Warrant application, seven similar warrants had already been approved.

e.g., *Vortman*, 2016 WL 7324987, at **3-6; *Hammond*, 2016 WL 7157762, at **5-6; *Allain*, 2016 WL 5660452, at **12-13.

These courts have correctly rebuffed these attacks on the FBI's conduct because the FBI acted reasonably in seizing the Playpen website and temporarily operating it for two weeks in an effort to identify the thousands of anonymous users accessing child pornography through Tor. As Agent Macfarlane explained in his NIT affidavit, because of the "unique nature of the Tor network and the method by which the network protects the anonymity of its users," other investigative procedures usually employed in these types of criminal investigations had failed or reasonably appeared "unlikely to succeed." NIT Aff. ¶ 31. Accordingly, once the government assumed administrative control of the Playpen website, it was "necessary" to temporarily operate the website "to locate and apprehend" those subjects who were "engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation." NIT Aff. ¶ 30. And, just as Agent Macfarlane predicted, because of the FBI's investigative actions, there are now more than 200 active prosecutions, including prosecutions of at least 48 alleged hands-on abusers. The FBI's actions have also led to the

identification or rescue of at least 49 American children who were subject to sexual abuse.[6]

Moreover, contrary to Croghan's claim, the Playpen investigation was entirely lawful. The "government did not create Playpen. Nor did it add content to the website, or even engage with Playpen users. The government merely attached itself to an illicit website that was already 'established and ongoing,' as illustrated by the fact that Playpen had already been operating for approximately six or seven months prior to government seizure." *Vortman*, 2016 WL 7324987, at *5 (citation omitted). The government thus "did not distribute any child pornography," *id.*, as Croghan asserts (at 31).

And, though Croghan contends for the first time (at 31) that the FBI agents "violated federal law" by failing to maintain child-pornography images in their custody or control, this is not accurate. Section 3509(m) of Title 18 forbids the "reproduction of child pornography . . . [i]n any criminal proceeding" and mandates that any "property or material that constitutes child pornography" shall "remain in the care, custody, and control of either the Government or the court." Section 3509(m) also commands that, "[n]otwithstanding Rule 16 of the Federal Rules of Criminal Procedure," a court in such a criminal proceeding

[6] *See* http://www.justice.gov/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation.

must deny a defendant's request to copy child-pornography materials "so long as the Government makes the property . . . reasonably available to the defendant." As § 3509(m)'s language makes plain, it is a criminal-discovery provision that places no substantive restrictions on the investigative activities of law-enforcement agencies.

Finally, the FBI did not "mislead[]" the magistrate judge by suggesting that the "places to be searched (the computers that accessed Playpen)" were only located in the Eastern District of Virginia, as Croghan repeatedly asserts (at 15-16, 32-33). The NIT warrant application declared that the "property" identified in Attachment A was located in the Eastern District of Virginia. Attachment A, in turn, identified the "[p]lace to be [s]earched" by reference to: (a) the NIT "to be deployed on" the computer server "operating the Tor network child pornography website," which was then located "at a government facility in the Eastern District of Virginia"; and (b) the "activating computers," *i.e.*, the computers "of any user or administrator who logs into" Playpen, which was then operating on the Virginia-based server. NIT App. (Attach. A). In his affidavit, Agent Macfarlane elaborated on the NIT's function by explaining that the search warrant would authorize 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." NIT Aff. ¶ 46. Thus, as every federal court to have considered this issue has concluded, the FBI "did not mislead the magistrate but was instead up front about the NIT's method and scope." *United States v. Werdene*, 2016 WL 3002376, at **11, 14 (E.D. Pa. May 18, 2016); *see also United States v. Libbey-Tipton*, No. 16-CR-236, p. 11 (N.D. Ohio Oct. 19, 2016); *United States v. Rivera*, No. 15-CR-266, pp. 9-10 (E.D. La. July 20, 2016); *United States v. Matish*, 2016 WL 3545776, at *24 (E.D. Va. June 23, 2016).

In sum, to pierce the anonymous veil provided by Tor, the government lawfully took advantage of the Playpen seizure to identify those child-pornography collectors accessing that website. As a result of this operation, the FBI successfully identified hundreds of Playpen users located across the country, including numerous hands-on abusers. These FBI actions should be commended, not deterred.

II. THE NIT WARRANT WAS SUFFICIENTLY PARTICULAR

As the government noted in its opening brief (at 29), below neither Croghan nor Horton "suggested the NIT Warrant was insufficiently particular." Nonetheless, Croghan now makes this claim (at 14-18), asserting the NIT

Warrant failed to describe the places to be searched with sufficient particularity.[7] He is mistaken.

A warrant meets the Fourth Amendment's particularity requirement if "the items to be seized and the places to be searched [are] described with sufficient particularity as to enable the searcher to locate and identify the places and items with reasonable effort and to avoid mistakenly searching the wrong places or seizing the wrong items." *United States v. Gleich*, 397 F.3d 608, 611 (8th Cir. 2005). The NIT Warrant specifically described the things to be seized—seven pieces of information obtained from the activating computers. NIT App. (Attach. B). Further, it described the place to be searched as the "activating computers . . . of any user or administrator who logs into [Playpen] by entering a username and password." NIT App. (Attach. A). The warrant thus "only permitted the government to collect a specific, limited set of data from 'activating computers,' which [we]re defined as computers of any individual who logs into Playpen with a username and password." *Vortman*, 2016 WL 7324987, at *9.

[7] Though Croghan did not make this claim below, we recognize that this Court may affirm on any grounds supported by the record whether or not raised, argued, decided, or relied upon by the district court. *United States v. Carter*, 884 F.2d 368, 374 (8th Cir. 1989).

"Every court to consider this question has found" the NIT Warrant was "sufficiently particular." *Anzalone*, 2016 WL 5339723, at *7.[8] The NIT Warrant's descriptions were constitutionally sufficient because they "limited which computers could be searched and what information could be obtained as a result of that search." *Allain*, 2016 WL 5660452, at *9; *cf. United States v. Karo*, 468 U.S. 705, 718 (1984) (explaining that a warrant to install a beeper need not specifically "describe the 'place' to be searched" as long as it "describe[s] the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested").

[8] *Vortman*, 2016 WL 7324987, at *9; *Hammond*, 2016 WL 7157762, at *3; *Duncan*, 2016 WL 7131475, at *3; *Lough*, 2016 WL 6834003, at *6; *Kienast*, 2016 WL 6683481, at *4; *Tippens*, No. 16-CR-5110, at pp. 11, 14; *United States v. Allain*, 2016 WL 5660452, at *9 (D. Mass. Sept. 29, 2016); *United States v. Smith*, No. 15-CR-467, pp. 7-8 (S.D. Tex. Sept. 28, 2016); *United States v. Anzalone*, 2016 WL 5339723, at *7 (D. Mass. Sept. 22, 2016); *United States v. Knowles*, No. 15-CR-875, pp. 23-24 (D.S.C. Sept. 14, 2016);*United States v. Jean*, 2016 WL 4771096, at **11-12 (W.D. Ark. Sept. 13, 2016); *Henderson*, 2016 WL 4549108, at *4; *United States v. Acevedo-Lemus*, 2016 WL 4208436, at *7 n.4 (C.D. Cal. Aug. 8, 2016); *United States v. Rivera*, No. 15-CR-266, pp. 11-13 (E.D. La. July 20, 2016); *United States v. Matish*, 2016 WL 3545776, at **13-14 (E.D. Va. June 23, 2016); *United States v. Darby*, 2016 WL 3189703, at *8 (E.D. Va. June 3, 2016); *United States v. Epich*, 2016 WL 953269, at *2 (E.D. Wisc. March 14, 2016); *United States v. Michaud*, 2016 WL 337263, at **4-5 (W.D. Wash. Jan. 28, 2016).

Croghan maintains (at 15-18) that particularity was lacking because thousands of users accessed Playpen and the government "made no effort to tailor its warrant request to particular users or even a particular group of users." But there is no requirement that the government "only target administrators or users which used the site regularly and aggressively." *Vortman*, 2016 WL 7324987, at *9 (internal quotation marks omitted). In any event, as the warrant affidavit carefully explained, the many affirmative steps required to access Playpen ensured that the warrant only applied to those persons actively trying to access child pornography, each of whom was attempting to commit a crime. NIT Aff. ¶¶ 7, 9-14. Thus, the "fact that the warrant authorized the FBI to search tens of thousands of potential targets 'does not negate particularity because it would be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor network.'" *Matish*, 2016 WL 3545776, at *14; *see also Henderson*, 2016 WL 4549108, at *4 (warrant was "sufficiently particular as it specifie[d] that the NIT search applies only to computers of users accessing the website, a group that is necessarily actively attempting to access child pornography").

III. RULE 41(b)(4) AUTHORIZED MAGISTRATE JUDGE BUCHANAN TO ISSUE THE NIT WARRANT

As we have suggested, this Court need not address the propriety of the NIT Warrant because the FBI's "reliance upon the warrant was objectively

reasonable," *United States v. Proell*, 485 F.3d 427, 430 (8th Cir. 2007). But if this Court considers that question, it should conclude that the NIT Warrant was authorized by Rule 41(b)(4).

A. The NIT Warrant Satisfied Rule 41(b)(4)'s Requirements

Rule 41(b)(4) gives magistrate judges the authority to issue warrants for tracking devices to be installed in their districts. Once installed, such a tracking device may continue to operate even if the object being tracked moves outside the district. As numerous district courts have correctly concluded, this is "exactly analogous to what the NIT Warrant authorized." *Darby*, 2016 WL 3189703, at *12.[9]

The NIT tracked the flow of intangible property—that is, the information contained on the Playpen website. Specifically, the NIT augmented the digital content requested by Playpen users from the government-controlled server operating in Virginia and, once the user's computer downloaded the requested content and the NIT, the NIT revealed to the government "registry-type information"—most importantly, an IP address, which allowed the government to determine the location of that computer. NIT Aff. ¶¶ 33-34. Moreover,

[9] *See also McLamb*, No. 16-CR-92, at pp. 17-18; *Lough*, 2016 WL 6834003, at **4-6; *United States v. Johnson*, 2016 WL 6136586, at **4-7 (W.D. Mo. Oct. 20, 2016); *Smith*, No. 15-CR-467, at pp. 14-15; *Jean*, 2016 WL 4771096, at **13-18; *Matish*, 2016 WL 3545776, at **17-18.

consistent with Rule 41(b)(4), the NIT was installed in the Eastern District of Virginia when the FBI agents configured the government-controlled server with the NIT code, thus setting the trap for Playpen users who thereafter requested content from the Playpen website.[10]

Adopting the inflexible approach to Rule 41 rejected by this Court, *see United States v. Falls*, 34 F.3d 674, 679 (8th Cir. 1994), Croghan claims (at 21-22) that the "NIT had no tracking function whatsoever" because it did not "'follow' evidence" or "send the government information about its journey." In the same breath, however, Croghan recognizes (at 21) that the NIT "sent identifying information about the individual's computer" to the government. In facilitating the identification of anonymous Tor users who accessed Playpen for the purpose

[10] Croghan erroneously asserts (at 22) that, "[a]ccording to the government, installation occurred after an individual made a 'virtual trip' via Playpen to the government's computer in the Eastern District of Virginia." That is not the government's position. Rather, as we articulated this point in our opening brief, "*[a]fter 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." Gov't Br. 23 (emphasis added); *see also id.* at 7 ("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."). Thus, once the government seized a copy of the Playpen website and began operating it from a government-controlled server in Newington, Virginia, FBI agents configured this government-controlled server by installing the NIT code on it. NIT Aff. ¶¶ 28-30, 32. The NIT was thus not "'install[ed] within' Mr. Croghan's computer in the Southern District of Iowa," as he asserts (at 20).

of downloading child pornography, the NIT worked to determine the activating computer's location, "just as traditional tracking devices inform law enforcement of a target's location." *Matish*, 2016 WL 3545776, at *18. A tracking device that pings (if you will) just once upon coming to rest, is still a tracking device. Indeed, the fact "that the NIT was purposely designed to allow the FBI to electronically trace the activating computer by causing it to return location identifying information from outside the Eastern District of Virginia—is not only authorized by Rule 41(b)(4), but is the very purpose intended by the exception." *Jean*, 2016 WL 4771096, at *17.

Croghan additionally suggests that Rule 41(b)(6) "provides further support to the conclusion that Rule 41(b)(4) did not authorize the warrant when it was issued" because (b)(6) is an "'entirely new grant of magistrate judge authority' that did not exist at the time of the NIT warrant." Br. at 23-24 (quoting *United States v. Workman*, 2016 WL 5791209, at *4 (D. Colo. Sept. 6, 2016)). But the Rule 41 amendment "effort shows nothing more than an intention on the part of the Judicial Conference's Committee on Rules of Practice and Procedure to keep the rules more current with the times." *Hammond*, 2016 WL 7157762, at *5. By simply "clarifying the propriety of warrants like the NIT Warrant," *id.*, Rule 41(b)(6) actually confirms that, interpreted flexibly, Rule 41(b)(4) always empowered Magistrate Judge

Buchanan to issue the warrant authorizing the use of the NIT as a tracking device.

B. Suppression Is Inappropriate Because Any Rule 41 Violation Was a Non-constitutional Violation and Croghan and Horton Were Not Prejudiced

Even assuming a Rule 41 violation, this Court "appl[ies] the exclusionary rule to violations of Rule 41 only if a defendant is prejudiced or reckless disregard of proper procedure is evident." *United States v. Bieri*, 21 F.3d 811, 816 (8th Cir. 1994). "This rule applies unless the defect permitted an unconstitutional warrantless search." *United States v. Gatewood*, 786 F.2d 821, 824 (8th Cir. 1986); *see also United States v. Freeman*, 897 F.2d 346, 350 (8th Cir. 1990). As the government showed in its opening brief (at 26-35), any Rule 41 violation was a non-constitutional, technical violation that did not prejudice appellees or reflect deliberate disregard of the rule.

Croghan contends otherwise (at 24-25), repeating his contentions that the violation was constitutional in nature because the NIT Warrant "was not sufficiently particular" and "void *ab initio.*" Horton similarly asserts (at 8-9) that the violation "sp[oke] to the substantive constitutional protections" of the Rule because it was the "equivalent of a warrantless search." As demonstrated at pp. 4-8, 13-16 *supra*, however, these constitutional arguments lack merit.

Croghan and Horton also contend (at 26-27; 11-12) that, even if the Rule 41 violation did not implicate the Fourth Amendment, it prejudiced them because Magistrate Judge Buchanan could not have issued the NIT warrant in compliance with Rule 41(b). They maintain that the proper prejudice test "focuses on 'whether the issuing federal magistrate judge could have complied with the Rule,' not whether a different judge could have lawfully issued the warrant." Croghan Br. 26 (quoting *Krueger*, 809 F.3d at 1116). This out-of-circuit prejudice test, however, ignores that *this* Court asks only "whether the *search* would have occurred had the rule been followed," *United States v. Hyten*, 5 F.3d 1154, 1157 (8th Cir. 1993) (emphasis added),[11] which certainly permits an assessment of whether a different judge could have issued the warrant. And, when the potential Rule 41 prejudice is properly measured by this Court's test, it is clear the search would have still occurred had the NIT Warrant been

[11] *See also United States v. Welch*, 811 F.3d 275, 281 (8th Cir.) (same), *cert. denied*, 136 S. Ct. 2476 (2016); *United States v. Beckmann*, 786 F.3d 672, 681 (8th Cir.) (same), *cert. denied*, 136 S. Ct. 672 (2015); *United States v. Schoenheit*, 856 F.2d 74, 77 (8th Cir. 1988) (same); *United States v. Brown*, 584 F.2d 252, 258 (8th Cir. 1978) (same). The majority of courts of appeals have adopted essentially the same search-based test as this Court. *See United States v. Burgos-Montes*, 786 F.3d 92, 109 (1st Cir.), *cert. denied*, 136 S. Ct. 599 (2015); *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. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988); *United States v. Luk*, 859 F.2d 667, 671 (9th 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. Wyder*, 674 F.2d 224, 226 (4th Cir. 1982).

presented to a federal magistrate judge in the Southern District of Iowa. *See* Fed. R. Crim. P. 41(b)(1).

Even if this Court was not bound by its prior decisions, it would be illogical to apply the prejudice inquiry adopted in *Krueger* for all Rule 41(b) violations. As one district court that evaluated the NIT Warrant reasoned, that "interpretation makes no sense, because under that interpretation, all searches executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter how small or technical the error might be." *Michaud*, 2016 WL 337263, at *6. Further, "[s]uch an interpretation would defeat the need to analyze prejudice separately from the Rule 41(b) violation" itself. *Id.* Indeed, a blanket application of *Krueger*'s test would mean that every Rule 41(b) violation would necessarily result in prejudice. If a particular magistrate judge is found, *post hoc*, to have lacked authority to approve a warrant for an out-of-district search under Rule 41(b), it necessarily follows that the judge never could have complied with the Rule. Otherwise, there would not have been a violation in the first place.[12]

[12] In claiming that he was prejudiced, Horton argues (at 12-14) that he had a reasonable expectation of privacy in his IP address and the information stored on his computer, but we have not suggested otherwise.

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 January 6, 2017, 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 23 pages containing 5,419 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