IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

16-3982

UNITED STATES OF AMERICA,

Appellant,

v.

BEAU BRANDON CROGHAN,

Appellee.

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF IOWA
HONORABLE ROBERT W. PRATT, U.S. DISTRICT COURT JUDGE

APPELLEE'S BRIEF

Brad Hansen
FEDERAL DEFENDER'S OFFICE
701 Pierce Street, Suite 400
Sioux City, Iowa 51101
PHONE: (712) 252-4158
FAX: (712) 252-4194

ATTORNEY FOR APPELLEE

SUMMARY OF THE CASE AND REQUEST FOR ORAL ARGUMENT

This case stems from the FBI's investigation of "Playpen," a child pornography website on a private Internet network called "Tor." The FBI seized controlled of Playpen and continued its operations, including the dissemination of child pornography, in an effort to apprehend the website's users.

To unravel Tor's privacy features, the FBI obtained a search warrant authorizing the deployment of malware (called a "Network Investigative Technique," or "NIT") to any computer that logged into Playpen. That malware sent back to the FBI identifying information about any such computer. Through that process, the FBI surmised that Beau Croghan had accessed Playpen, which led to his home being searched pursuant to a separate warrant.

The government appeals the district court's decision to suppress evidence derived from the NIT warrant. As argued in this brief, the district court correctly suppressed the evidence, because the NIT warrant violated both the Fourth Amendment and Federal Rule of Criminal Procedure 41(b).

The legal issues presented by the Playpen NIT warrant have divided federal district courts and have not been resolved by this Court or any other circuit court. Accordingly, Mr. Croghan agrees with the government that 15 minutes of oral argument per side is appropriate.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Circuit Court Cases

District Court Cases

Others

JURISDICTIONAL STATEMENT

The decision appealed: The government has appealed the district court's order granting Mr. Croghan's motion to suppress. DCD No. 39.[1]

Jurisdiction of the court below: The district court has jurisdiction over Mr. Croghan's federal criminal prosecution pursuant to 18 U.S.C. § 3231: "The district courts of the United States shall have original jurisdiction . . . of all offenses against the laws of the United States."

Jurisdiction of this Court: This Court has jurisdiction over the government's interlocutory appeal pursuant to 18 U.S.C. § 3731: "An appeal by the United States shall lie to a court of appeals from a decision or order of a district court suppressing or excluding evidence or requiring the return of seized property in a criminal proceeding, not made after the defendant has been put in jeopardy and before the verdict or finding on an indictment or information, if the United States attorney certifies to the district court that the appeal is not taken for purpose of delay and that the evidence is a substantial proof of a fact material in the proceeding."

[1] In this brief, "DCD" refers to the district court's docket in *United States v. Croghan*, No. 15-cr-00048-RP (S.D. Iowa).

STATEMENT OF THE ISSUES PRESENTED FOR REVIEW AND MOST APPOSITE AUTHORITIES

I. THE EVIDENCE SHOULD BE SUPPRESSED BECAUSE THE NETWORK INVESTIGATIVE TECHNIQUE ("NIT") WARRANT FAILED TO DESCRIBE THE PLACE TO BE SEARCHED WITH SUFFICIENT PARTICULARITY.

U.S. Const. amend. IV

Steagald v. United States, 451 U.S. 204 (1981)

In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013)

II. THE EVIDENCE SHOULD BE SUPPRESSED BECAUSE THE MAGISTRATE JUDGE EXCEEDED THE TERRITORIAL LIMITATIONS OF HER AUTHORITY.

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

United States v. Krueger, 809 F.3d 1109 (10th Cir. 2015)

United States v. Levin, ___ F. Supp. 3d ___, 2016 WL 2596010 (D. Mass. May 5, 2016)

United States v. Workman, ___ F. Supp. 3d. ___, 2016 WL 5791209 (D. Colo. Sept. 6, 2016)

III. THE GOOD-FAITH EXCEPTION TO THE EXCLUSIONARY RULE DOES NOT APPLY.

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

STATEMENT OF THE CASE

This case involves the intersection of 21st-century technology, privacy, and search and seizure law.

The Tor Network

The Internet that most people use is anything but anonymous. When an individual visits a website, the website generally registers the individual's Internet Protocol ("IP") address. The IP address is associated with a particular Internet Service Provider ("ISP") and a particular subscriber of the ISP. Thus, it is generally easy to determine who did what on the Internet.

For those in search of greater privacy, there is the "Tor" network (short for "The Onion Router"). The Tor network was originally developed by the United States Naval Research Laboratory to protect government communications; it is now an independent non-profit organization. Unlike the regular Internet, communications on Tor are routed through a system of network computers run by volunteers around the world. To access websites on Tor, an individual must download special software. When a Tor user visits a website, the only IP address registered by the website is the last computer through which the user's communications were routed (the "exit node"). Because it is impossible to trace

communications from the exit node back to the user's computer, users of the Tor network operate in relative anonymity. NIT Aff. ¶¶ 7-8.[2]

Those who run websites on the Tor network also enjoy general anonymity. Websites on the Tor network can be set up as "hidden services" that may be accessed only through Tor. The IP address for a Tor website is hidden. Unlike the traditional Internet, Tor websites are not indexed for searching, and a user must know the address of the hidden service to access it. *Id.* ¶¶ 9-10.

Individuals use Tor to protect themselves from identity thieves, businesses prone to data breaches, and censorship, among other things. *See* The Tor Project, Inception, https://www.torproject.org/about/torusers.html.en (last visited Dec. 27, 2016). Tor is popular because its users believe that "anonymity is a requirement for a free and functioning society." *Id.* A survey from 2014 suggested that 11% of all Internet users worldwide have used Tor, which would correspond to tens of millions of people. *See* Jemima Kiss, *Privacy Tools Used by 28% of the Online*

---

[2] The application for the NIT search warrant at issue in this appeal, attachments, and affidavit in support of the application, and the search warrant itself, were filed as Exhibit A to Mr. Croghan's motion to suppress (DCD No. 33). In this brief, citations to "NIT Aff." refer to FBI Special Agent Douglas Macfarlane's affidavit in support of the search warrant application. "NIT App." refers to the application for the search warrant itself, and "NIT App. Attach. A" and "NIT App. Attach. B" refer to Attachments A and B to the application.

World, Research Finds, The Guardian, Jan. 21, 2014, https://www.theguardian.com/technology/2014/jan/21/privacy-tools-censorship-online-anonymity-tools.

Playpen

As with most any advancement in technology, Tor can be used for good and, as this case illustrates, for bad.

In approximately September 2014, the FBI began investigating a Tor website called "Playpen." According to the FBI, Playpen was a message board website devoted to the dissemination of child pornography. Playpen had more than 150,000 total members. NIT Aff. ¶ 11.

In December 2014, a foreign law enforcement agency informed the FBI that it suspected that a particular IP address was associated with Playpen. Through further investigation, the FBI learned that the IP address was owned by a server-hosting company in Lenoir, North Carolina. *Id.* ¶ 28.

In January 2015, the FBI executed a search warrant at the server-hosting company. Pursuant to the warrant, the FBI seized a copy of the server that was assigned the IP address suspected to be associated with Playpen. FBI agents reviewed the contents of the server and found that it contained a copy of the Playpen website. The FBI placed its copy of the server containing Playpen in a government-controlled facility in the Eastern District of Virginia. *See id.*

On February 19, 2015, the FBI arrested the suspected administrator of Playpen. After the arrest, the FBI "assumed administrative control" of the website. *Id.* ¶ 30.

NIT Warrant

Incredibly, despite seizing control of Playpen, the FBI opted to allow the website's operations to continue in order to further its investigation, which allowed for the continued dissemination of child pornography on the government's watch. *See id.* Because of the anonymous nature of Tor, however, the FBI was, for the most part, unable to identify IP addresses (and, thus, identities) of users of Playpen through traditional techniques. *Id.* ¶ 29 & n.7.

To circumvent that anonymity, the FBI applied for a search warrant in the Eastern District of Virginia to employ a Network Investigative Technique, or "NIT," to locate and identify users and other administrators of Playpen. According to FBI Special Agent Douglas Macfarlane's affidavit in support of the search warrant application, the NIT would secretly transmit a computer code to any individual who logged into Playpen's website. This government-sponsored malware[3] would then cause that individual's computer to send various identifying

[3] "'Malware' is a term for any software that gets installed on [a] machine and performs unwanted tasks, often for some third party's benefit." MIT Info. Sys. & Tech., Viruses, Spyware, and Malware, https://ist.mit.edu/security/malware (last

information back to an FBI computer in the Eastern District of Virginia, including the IP address, operating system, host name, username, and Media Access Control address[4] of the individual's computer. *Id.* ¶¶ 30-34.

The application for the NIT warrant signed by Special Agent Macfarlane stated under penalty of perjury that the property to be searched was "located in the Eastern District of Virginia" and identified in Attachment A to the application. NIT App. In turn, Attachment A stated that the warrant would authorize the FBI to deploy the NIT from the government computer server in the Eastern District of Virginia that hosted Playpen. NIT App. Attach. A. The NIT would seize the information described in Attachment B – specifically, the IP address and other previously mentioned identifying information of computers "wherever located," NIT Aff. ¶ 46a; NIT App. Attach. B – from the computer of "any user or administrator who logs into [Playpen] by entering a username and password." NIT App. Attach. A.

---

visited Dec. 27, 2016).

[4] A Media Access Control, or "MAC," address "is a unique identifier assigned to a network adapter or network interface card (NIC) by the manufacturer for identification." Univ. of Ill. at Chi. Academic Computing and Commc'ns Ctr., What is My IP Address / MAC Address?, http://accc.uic.edu/answer/what-my-ip-address-mac-address (last visited Dec. 27, 2016). In other words, a MAC address is another way to identify a particular computer.

The FBI requested that it be allowed to continue Playpen's operations and employ the NIT for a period of 30 days. The search warrant application also requested permission to use the NIT at any time of the day that an individual's computer accessed Playpen. NIT Aff. ¶¶ 43-45. Moreover, the FBI requested permission to delay notice of the search to any affected individual until 30 days after the individual had been identified. *Id.* ¶¶ 38-41.

On February 20, 2015, Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia granted the NIT warrant under the terms requested by the FBI. Appellant's Add. at 4.

With the warrant in hand, the FBI began deploying the NIT on the same date that the warrant was granted. On March 4, 2015, the FBI stopped deploying the NIT and took the Playpen website offline – short of the 30-day period permitted under the NIT warrant. *Id.*

Mr. Croghan's Case

The FBI identified user "beau2358" as having accessed Playpen during the period in which the NIT was deployed. Through the NIT, the FBI obtained the IP address of the computer used by beau2358. Further investigation led law

enforcement to conclude that Mr. Croghan had accessed Playpen from his home in Council Bluffs, Iowa. *See* Iowa Warrant Aff. ¶¶ 25-41.[5]

Armed with the information seized pursuant to the NIT warrant, law enforcement obtained a search warrant in the Southern District of Iowa for Mr. Croghan's person, home, and car. That warrant was executed on July 17, 2015. *See* Appellant's Add. at 4.

On November 24, 2015, a grand jury in the Southern District of Iowa returned an indictment against Mr. Croghan charging him with accessing or attempting to access child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). DCD No. 3.

Suppression Proceedings

Mr. Croghan filed a motion to suppress evidence (DCD No. 33). He argued that the NIT warrant was issued in violation of Federal Rule of Criminal Procedure 41(b), which describes a magistrate judge's authority to issue search warrants. He argued that suppression is the appropriate remedy for the violation. The

[5] The application for the search warrant for Mr. Croghan's person, home and car; attachments to the application; affidavit in support of the application; and the search warrant itself, were filed as Exhibit B to Mr. Croghan's motion to suppress (DCD No. 33). In this brief, any citations to "Iowa Warrant Aff." refer to FBI Special Agent Jacob Foiles' affidavit in support of the Iowa search warrant application.

government resisted (DCD No. 36), arguing that Rule 41(b)(4) authorized the NIT warrant, and that in any event, suppression was unwarranted for any violation.

The district court entered an order granting Mr. Croghan's motion to suppress.[6] In so ruling, the court recognized that the legality of the Playpen NIT warrant had divided other district courts, but ultimately sided with those courts holding that the NIT warrant violated Rule 41(b), and that the evidence stemming from it should be suppressed. *See United States v. Levin*, ___ F. Supp. 3d ___, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Arterbury*, No. 15-cr-182, Docket No. 42 (N.D. Okla. Apr. 25, 2016) (Appellant's App. at 1-30); *see also United States v. Workman*, ___ F. Supp. 3d. ___, 2016 WL 5791209 (D. Colo. Sept. 6, 2016). The court also recognized that several other district courts had held that the NIT warrant violated Rule 41(b), but that suppression was not warranted. Finally, the court also recognized that other courts have concluded that the NIT warrant was lawful under Rule 41(b). *See* Appellant's Add. at 5-6.

The district court in this case rejected the government's argument that Rule 41(b)(4) authorized the NIT warrant. Rule 41(b)(4) provides that "a magistrate judge with authority in the district has authority to issue a warrant to install within

---

[6] The district court also granted Steven Horton's motion to suppress, which presented the same issue, in the same order. Mr. Horton's case is the companion case to Mr. Croghan's in this appeal.

the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." Fed. R. Crim. P. 41(b)(4). The court reasoned that the NIT was not a "tracking device," because rather than "track" anything, "it caused computer code to be installed on the activating user's computer, which then caused such computer to relay specific information to the government-controlled computers in Virginia." Appellant's Add. at 10.

The district court correctly stated that a Rule 41 violation is cause for suppression only in certain circumstances – specifically, if the violation implicates the Fourth Amendment; or if the violation is non-constitutional, when the defendant was prejudiced or law enforcement recklessly disregarded proper procedure. *Id.* at 12 (citing *United States v. Hyten*, 5 F.3d 1154, 1157 (8th Cir. 1993), among others).

With that standard in mind, the court concluded that suppression was the appropriate remedy for the violation. The court reasoned that the violation at issue was constitutional, because "a warrant issued without proper jurisdiction is void *ab initio* and . . . any search conducted pursuant to such warrant is the equivalent of a warrantless search." The court declined to apply the good-faith exception to the exclusionary rule. *Id.* at 14-15. Alternatively, the court held that Mr. Croghan

was prejudiced by the violation, because "neither the search pursuant to the NIT Warrant nor the search[] pursuant to [the warrant for Mr. Croghan's person, home, and car] would have occurred without the violation of Rule 41(b)." *Id.* at 18. The court also suggested that the FBI recklessly disregarded proper procedure, because Special Agent Macfarlane was "sufficiently experienced" to understand the shortcomings of the NIT warrant, and "there existed adequate case law casting doubt on magisterial authority to issue precisely this type of NIT Warrant." *Id.*

This interlocutory appeal by the government follows. The government filed a timely notice of its intent to appeal. *See* DCD No. 42.

SUMMARY OF THE ARGUMENT

First, the NIT warrant failed the Fourth Amendment's particularity requirement. The warrant targeted thousands of unknown individuals in unknown locations throughout the world. By doing so, the warrant provided the FBI with an unconstitutional degree of discretion in its execution.

Second, by issuing the NIT warrant, the magistrate judge exceeded the territorial limits on her authority under the Federal Magistrates Act and Federal Rule of Criminal Procedure 41(b). The NIT warrant was not a "tracking device," as permitted under Rule 41(b)(4), and even if it were, it was not installed in the Eastern District of Virginia, as required by the rule. A violation of Rule 41(b)

goes to the fundamental authority of the magistrate judge to issue a warrant, and thus the violation is constitutional in nature. Even if the violation were deemed non-constitutional, suppression remains appropriate because Mr. Croghan suffered prejudice, and the FBI's conduct constituted reckless disregard for proper procedure.

Third, the good-faith exception to the exclusionary rule does not apply. That exception does not salvage a search conducted pursuant to a warrant that was void *ab initio*, or from its inception. Even if it did, the FBI's conduct was patently unreasonable and should be deterred through application of the exclusionary rule. In an effort to apprehend individuals interested in viewing child pornography, the FBI facilitated the distribution of child pornography and obtained an overbroad search warrant pursuant to a misleading application.

Therefore, this Court should affirm the district court's order suppressing the evidence seized pursuant to the NIT warrant.

ARGUMENT

In reviewing the decision to grant Mr. Croghan's motion to suppress, this Court reviews the district court's factual findings for clear error and its legal conclusions *de novo*. *United States v. Wells*, 223 F.3d 835, 838 (8th Cir. 2000). This Court will not reverse the district court's decision on a motion to suppress "unless it is not supported by substantial evidence on the record; it reflects an erroneous view of the applicable law; or upon review of the entire record, the appellate court is left with the definite and firm conviction that a mistake has been made." *United States v. Layne*, 973 F.2d 1417, 1420 (8th Cir. 1992).

I. THE EVIDENCE SHOULD BE SUPPRESSED BECAUSE THE NETWORK INVESTIGATIVE TECHNIQUE ("NIT") WARRANT FAILED TO DESCRIBE THE PLACE TO BE SEARCHED WITH SUFFICIENT PARTICULARITY.

The Fourth Amendment requires that any warrant "particularly describe[s] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "The Fourth Amendment was intended partly to protect against the abuses of the general warrants that had occurred in England and of the writs of assistance used in the Colonies." *Steagald v. United States*, 451 U.S. 204, 220 (1981); *see also Maryland v. King*, 133 S. Ct. 1958, 1980 (2013) (Scalia, J., dissenting) (noting that the Fourth Amendment protects against "warrants not grounded upon a sworn oath of a specific infraction by a particular individual, and

thus not limited in scope and application"). To satisfy the Fourth Amendment, "[t]he place must be described with sufficient particularity as to enable the executing officer to locate and identify it with reasonable effort." *United States v. Alberts*, 721 F.2d 636, 639 (8th Cir. 1983).

The NIT warrant authorized the search of any computer of "any user or administrator who log[ged] into [Playpen] by entering a username and password." NIT App. Attach. A. The warrant application erroneously claimed that any such place to be searched was in the Eastern District of Virginia. *See* NIT App. In reality, any computer wherever located that logged into Playpen was automatically subject to being searched pursuant to the warrant – entirely because a single magistrate judge issued a single, overbroad search warrant. Although this issue was not addressed below, the NIT warrant's unprecedented breadth fails the Fourth Amendment's particularity requirement.[7]

The NIT warrant failed to place any limit on the number of searches authorized by it. According to Special Agent Macfarlane's affidavit in support of

[7] This Court may affirm the district court on "any grounds supported by the record." *United States v. Allen*, 705 F.3d 367, 369 (8th Cir. 2013). Although the government correctly notes that some district courts have concluded that the NIT warrant was sufficiently particular, *see* Appellant's Br. at 11 n.7 (citing cases), those cases did not contain a particularly thorough examination of the issue. *See* Orin Kerr, *Government 'Hacking' and the Playpen Warrant*, Wash. Post (Volokh Conspiracy), Sept. 27, 2016, 2016 WLNR 29514662.

the warrant, Playpen had more than 150,000 users, NIT Aff. ¶ 11, and the FBI made no effort to tailor its warrant request to particular users or even a particular group of users. The FBI failed to do so even though it had identified usernames that were responsible for making a disproportionate number of posts on the site, *see id.* ¶ 19, and it knew which "sub-forums" of Playpen contained "the most egregious examples of child pornography and/or [were] dedicated to retellings of real world hands on sexual abuse of children." *Id.* ¶ 27. Thus, the NIT warrant unnecessarily subjected an enormous number of computers to intrusive searches for identifying information.

The NIT warrant also placed no limitation on the location of the computers to be searched. Notwithstanding the misleading language in the search warrant application, by authorizing searches of computers "wherever located," *id.* ¶ 46a, the NIT warrant allowed searches outside of the Eastern District of Virginia, across the United States, and even throughout the entire world.

This overbreadth afforded the FBI with "unfettered discretion" in deciding how to execute the NIT warrant, which the Fourth Amendment does not permit. *Steagald*, 451 U.S. at 220; *see also In re Grand Jury Proceedings*, 716 F.2d 493, 496-99 (8th Cir. 1983). Even though a sufficiently particular warrant leaves "nothing . . . to the discretion of the officer executing the warrant," *Marron v.*

United States, 275 U.S. 192, 196 (1927), the FBI deliberately sought the unconstitutional degree of flexibility granted by the NIT warrant. Although the warrant authorized deployment of the NIT to any user logged into Playpen, Special Agent Macfarlane expressly stated in his affidavit that the FBI may decide to "deploy the NIT more discretely against particular users," including users who engaged in "substantial posting activity" or who visited particular areas of the website. NIT Aff. ¶ 32 n.8.[8]

Special Agent Macfarlane's admission demonstrates that the FBI knew that it could have investigated Playpen in a more narrowly tailored manner to pass constitutional muster. By the time that the FBI requested the NIT warrant, it had already seized control of Playpen. *Id.* ¶ 30. With that control, the FBI could have reviewed activity on the website and sought search warrants tailored to particular users or activities, identified users by engaging in undercover communications, or investigated Playpen users by any number of other constitutional means.

Without any tailoring, the NIT warrant was general enough that innocent parties could have been caught in the dragnet. Although the affidavit claimed that it was highly unlikely that individuals could stumble upon Playpen without seeking out child pornography, *id.* ¶ 10, that alone did not protect an innocent computer

[8] Additionally, the FBI exercised the overly broad degree of discretion afforded to it by taking Playpen offline short of the 30-day period for the NIT allowed by the warrant. *See* Appellant's Add. at 3-4.

owner from intrusion. With all of its generality, the warrant contained no assurances that the NIT would operate reliably in the Tor network and necessarily cause itself to be deployed to the Playpen user's computer, as opposed to an "innocent" computer in the network. It also contained no protections for computers located in a public place or owned by "innocent" third parties. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013).

The generality of the NIT warrant is unprecedented in Fourth Amendment jurisprudence. For instance, although certain wiretaps tied to a specific suspect but not a particular place may pass constitutional muster, *see United States v. Karo*, 468 U.S. 705, 718 (1984), the NIT warrant went further by targeting *any* user or administrator who logged into Playpen over a 30-day period. Indeed, no appellate court has upheld a search warrant targeting unknown users *and* unknown places, *and* authorizing an untold number of searches.

The Fourth Amendment requires more. This Court should hold that the NIT warrant violated the Fourth Amendment's particularity requirement.

II. THE EVIDENCE SHOULD BE SUPPRESSED BECAUSE THE MAGISTRATE JUDGE EXCEEDED THE TERRITORIAL LIMITATIONS OF HER AUTHORITY.

The government contends that Magistrate Judge Buchanan in the Eastern District of Virginia had authority under Federal Rule of Criminal Procedure 41(b)(4) to issue the NIT warrant, even though it authorized searches outside of her district. *See* Appellant's Br. at 18-25. Alternatively, the government argues that even if the magistrate judge acted without authority, the evidence stemming from it should not be suppressed. *See id.* at 26-35. The district court correctly rejected these arguments.

A. Federal Rule Of Criminal Procedure 41(b) Did Not Authorize The NIT Warrant.

The Federal Magistrates Act provides that a magistrate judge may only exercise authority "within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law," including "by the Rules of Criminal Procedure for the United States District Courts." 28 U.S.C. § 636(a). In turn, Federal Rule of Criminal Procedure 41(b) defines the "territorial limits on a magistrate judge's authority to issue a warrant." *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d at 756.

The government relies entirely on Rule 41(b)(4) as the source of Magistrate

Judge Buchanan's power to issue the NIT warrant. At the time that the NIT warrant was issued, Rule 41(b)(4) provided as follows:

> **(b) Authority to Issue a Warrant.** At the request of a federal law enforcement officer or an attorney for the government:
>
> . . . .
>
> **(4)** a magistrate judge with authority in the district has authority to issue a warrant to *install within the district a tracking device*; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both . . . .

Fed. R. Crim. P. 41(b)(4) (2015) (emphasis added). Contrary to the government's argument, Rule 41(b)(4) did not authorize the NIT warrant because the NIT is not a "tracking device." Even if it were, the NIT was still illegal because it was "install[ed] within" Mr. Croghan's computer in the Southern District of Iowa – not the Eastern District of Virginia.

The government argues that the NIT was a "tracking device," because it followed data as it traveled from the Eastern District of Virginia to Mr. Croghan's computer in the Southern District of Iowa, and then it caused transmission of identifying data back to the government in the Eastern District of Virginia. *See* Appellant's Br. at 21-23. The district court correctly rejected this strained reading of Rule 41(b)(4)'s "tracking device" language. *See* Appellant's Add. at 8-12.

Under Rule 41, "'[t]racking device' has the meaning set out in 18 U.S.C.

§ 3117(b)," Fed. R. Crim. P. 41(a)(2)(E), which provides a circular definition of "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). A device that engages in "tracking" "follow[s] the tracks or traces of" or "search[es] for by following evidence until found." Merriam-Webster's Collegiate Dictionary 1246 (10th ed. 2002).

The NIT did not merely "follow" evidence, and it was not a "tracking device." To borrow from the government's own brief, the purpose of the NIT was to "cause[] the transmission of the location-identifying information [of Playpen users' computers] back to the government . . . allowing the government to identify and locate the user," wherever they were located. Appellant's Br. at 22. In this respect, the NIT did not "track the movement of a person or property," as conceived by Rule 41(b)(4). Instead, it traveled from the government's computer in the Eastern District of Virginia, searched an individual's computer, and sent identifying information about the individual's computer (and, by extension, the individual, as well) to the government. *See Workman*, 2016 WL 5791209, at *4; *Levin*, 2016 WL 2596010, at *6.

Although the government may be correct that Rule 41(b) is to be read flexibly, Appellant's Br. at 19-20 (citing *United States v. New York Tel. Co.*, 434 U.S. 159, 169 & n.16 (1977), and *United States v. Falls*, 34 F.3d 674, 678 (8th Cir.

1994)), Rule 41(b)(4) cannot reasonably be stretched as far as the government takes it. Unlike the transmitter affixed to a container addressed in *United States v. Knotts*, 460 U.S. 276, 277 (1983), the NIT had no tracking function whatsoever. It did not send the government information about its journey from the Eastern District of Virginia to an individual's computer, wherever located. In essence, the NIT hacked the individual's computer and hijacked identifying information, which was then sent back to the government's computer in the Eastern District of Virginia. *See* NIT Aff. ¶ 33.

Even if the NIT were deemed a "tracking device," it was only authorized if it was "install[ed] within the" Eastern District of Virginia. Fed. R. Crim. P. 41(b)(4). The government contends that the NIT's "deployment [in the Eastern District of Virginia] constituted installation of a tracking device under Rule 41." Appellant's Br. at 23. According 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. *Id.*

This "virtual trip" aspect of the government's argument misunderstands the difference between downloading (from the government's computer in the Eastern District of Virginia) and installing software (on the Playpen user's computer). *In re Warrant to Search a Target Computer at Premises Unknown* illustrates this

distinction. In that case, the government sought to "surreptitiously install data extraction software" on a target computer "allegedly used to violate federal bank fraud, identity theft, and computer security laws." 958 F. Supp. 2d at 755. The magistrate judge denied the application for the search warrant. *Id.* at 761. In so doing, the court rejected the government's reliance on Rule 41(b)(4), reasoning that "there is 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." *Id.* at 758.

An amendment to Rule 41(b) made effective subsequent to the NIT warrant provides further support to the conclusion that Rule 41(b)(4) did not authorize the warrant when it was issued. Effective December 1, 2016, Rule 41(b)(6) provides that "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 . . . the district where the media or information is located has been concealed through technological means." Fed. R. Crim. P. 41(b)(6). This is "an entirely new grant of magistrate judge authority"

that did not exist at the time of the NIT warrant. *Workman*, 2016 WL 5791209, at *4.

Accordingly, because the NIT was neither a "tracking device" nor "installed within the" Eastern District of Virginia, the district court correctly concluded that Magistrate Judge Buchanan lacked authority pursuant to Rule 41(b)(4) to issue the NIT warrant.

B. Suppression Is The Appropriate Remedy.

After a Rule 41 violation has been established, evidence stemming therefrom must be suppressed if the violation is tantamount to a "constitutional infirmity," *see Hyten*, 5 F.3d at 1157, or if it "prejudice[s] a defendant or show[s] reckless disregard of proper procedure." *Id.*[9] Suppression is appropriate on all of these bases.

1. The Violation Was Constitutional In Nature.

The government argues that there is no constitutional infirmity for any search warrant so long as "it is (1) supported by probable cause, (2) sufficiently particular, and (3) issued by a neutral and detached magistrate." *See* Appellant's Br. at 28. Further, the government suggests that as long as a magistrate is "neutral and detached . . . and capable of determining probable cause," any search warrant

[9] The good-faith exception analysis subsumes the analysis of whether there was "reckless disregard of proper procedure" by law enforcement, Appellant's Br. at 35 n.19, so those issues are addressed together. *See infra* Part III.

issued by the magistrate passes constitutional muster. *See id.* at 30. The district court was unpersuaded by this argument – and with good reason. *See* Appellant's Add. at 12-15.

For one, as argued previously, the NIT warrant was not sufficiently particular. Thus, even without reaching the Rule 41(b) issue, evidence stemming from the NIT warrant must be suppressed based on a constitutional violation. *See supra* Part I.

Beyond that, the district court was correct to conclude that, in essence "there simply was no judicial approval" of the NIT warrant, and that it was "void *ab initio*." Appellant's Add. at 13. "[S]ensitive to the fact that magistrate judges do not enjoy life tenure and other independence-assuring protections found in Article III, Congress has taken particular care to limit the geographic range of [magistrate judges'] authority since the very inception of the office." *United States v. Krueger*, 809 F.3d 1109, 1125 (10th Cir. 2015) (Gorsuch, J., concurring). As such, Rule 41(b) "implicates substantive judicial authority," *id.* at 1115 n.7 (Ebel, J., majority) (quotation marks omitted), and is "the very sort of jurisdictional limitation on the execution of warrants that the common law and Fourth Amendment have enforced since time out of mind." *Id.* at 1126 n.7 (Gorsuch, J., concurring). Thus, as Judge Gorsuch recently explained, when a warrant is issued

by a magistrate judge without territorial authority to do so, "a warrant like that is no warrant at all." *Id.* at 1126 (Gorsuch, J., concurring).

Because the NIT warrant was void *ab initio*, the district court correctly determined that the violation at issue implicated the Constitution. *See Levin*, 2016 WL 2596010, at *7-8.

2. Even If The Violation Did Not Implicate The Constitution, Suppression Remains Appropriate Because The Violation Prejudiced Mr. Croghan.

To determine whether Mr. Croghan was prejudiced by the violation, this Court asks "whether the search would have occurred had the rule been followed." *Hyten*, 5 F.3d at 1157. The government claims that Mr. Croghan suffered no prejudice, because the search would have occurred if the NIT warrant had instead been authorized by a magistrate judge in the Southern District of Iowa. Appellant's Br. at 35.

Contrary to the government's argument based on a hypothetical, "prejudice in this context should be anchored to the facts as they actually occurred." *Krueger*, 809 F.3d at 1116. Accordingly, the prejudice inquiry for Rule 41(b) focuses on "whether the issuing federal magistrate judge could have complied with the Rule," *id.*, not whether a different judge could have lawfully issued the warrant. For the reasons already explained, Magistrate Judge Buchanan could not have

issued the NIT warrant in compliance with Rule 41(b). In fact, at the time that the NIT warrant was issued, "no magistrate judge ha[d] the authority to issue" it without violating the territorial limits of 28 U.S.C. § 636(a) and Rule 41(b). *Levin*, 2016 WL 2596010, at *8.

Even setting that fundamental issue aside, the government's argument fails because there is no evidence that the government would have surmised that user "beau2358" was accessing Playpen from the Southern District of Iowa. Thus, beyond pure speculation, there is no reason to expect that the government would have sought the NIT warrant in that district.

Accordingly, Mr. Croghan was indeed prejudiced by the violation of Rule 41(b).

III. THE GOOD-FAITH EXCEPTION TO THE EXCLUSIONARY RULE DOES NOT APPLY.

The good-faith exception to the exclusionary rule applies when evidence is "obtained in objectively reasonable reliance on a subsequently invalidated search warrant," *United States v. Leon*, 468 U.S. 897, 922 (1984), or in very limited circumstances, when evidence is obtained without a warrant but in objective good faith. *See* 1 Wayne R. LaFave, Search & Seizure § 1.3(g) (5th ed. 2016). In summary, the government argues that the good-faith exception applies even if the NIT warrant was void *ab initio*, and that the FBI acted in an objectively reasonable

manner on the NIT warrant issued by the magistrate judge. *See* Appellant's Br. at 37-50.

A. The Good-Faith Exception Does Not Apply When Law Enforcement Relied Upon A Warrant That Was Void At Its Inception.

The district court correctly concluded that the good-faith exception is inapplicable because the NIT warrant "was issued without jurisdiction and was, therefore, void *ab initio*." Appellant's Add. at 15.

The Supreme Court in *Leon* explained that the good-faith exception is based on the premise that "[r]easonable minds frequently may differ on the question whether a particular affidavit establishes probable cause." 468 U.S. at 914. Accordingly, the Court concluded that "the preference for warrants is most appropriately effectuated by according great deference to a magistrate's determination." *Id.* (quotation marks omitted); *see also United States v. Carpenter*, 341 F.3d 666, 671 (8th Cir. 2003). The Supreme Court has not applied the good-faith exception to warrantless searches beyond "rather special situations." *Davis v. United States*, 564 U.S. 229, 258 (2011) (Breyer, J., dissenting).

Nothing in *Leon* suggests that such deference applies to a magistrate judge's erroneous determination as to whether she has authority to issue a warrant in the first place. Through its overly broad search warrant application, the FBI invited

Magistrate Judge Buchanan's error, which breached the limits of the modest authority that Congress assigned to magistrates. The error did not simply lead to a single search or arrest based on information that may or may not amount to probable cause; rather, it subjected thousands of individuals to searches based on authority that the magistrate judge did not have. As such, the good-faith exception does not apply. *See Levin*, 2016 WL 2596010, at *10-12.

In its attempt to expand the bounds of the good-faith exception, the government cites several Supreme Court cases addressing the exception's application to warrantless searches – all of which are distinguishable. In *Davis*, the Supreme Court applied the good-faith exception to a warrantless search of a car's driver that was based on later-overruled legal precedent. 564 U.S. at 232, 241. Likewise, in *Illinois v. Krull*, 480 U.S. 340 (1987), the Court held that the good-faith exception salvaged the admissibility of evidence seized pursuant to a warrantless search of a junkyard based on a state statute later ruled unconstitutional. *Id.* at 356-57. In each case, the Court concluded that officers acted in reasonable reliance on then-existing authority – a far cry from a search warrant that a magistrate judge never had authority to issue in the first place.

The other two cases relied upon by the government are also inapt. *Herring v. United States*, 555 U.S. 135, 137-39 (2009), and *Arizona v. Evans*, 514 U.S. 1,

15-16 (1995), applied the good-faith exception in cases involving arrests based on warrants that had been recalled or quashed, but were relied upon because of negligence or clerical error. Again, in each instance, the officers relied upon authority (a warrant) that was, at one point, valid, as opposed to a warrant that was void *ab initio*. The district court's reasoning did not "ignore[] controlling Supreme Court precedent," as claimed by the government. Appellant's Br. at 38.

In sum, the Court should not indulge the government's effort to expand the good-faith exception to salvage the admissibility of evidence seized pursuant to a warrant that was void *ab initio*.

B. The FBI's Objectively Unreasonable Conduct Should Be Deterred.

The district court also correctly concluded that suppression is appropriate because the FBI's conduct constituted systemic error or reckless disregard of constitutional requirements and was not objectively reasonable. Appellant's Add. at 18-19.

The Supreme Court has noted that "the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring*, 555 U.S. at 144. The exclusionary rule should be applied where "the benefits of deterrence . . . outweigh the costs" of exclusion. *Id.* at 141.

The FBI's conduct throughout the Playpen saga is worth deterring. The government correctly notes that child pornography offenses are "abhorrent," Appellant's Br. at 49, as images of child pornography "are a permanent record of the children's participation [in sexual abuse,] and the harm to the child is exacerbated by their circulation." *New York v. Ferber*, 458 U.S. 747, 759 (1982). Nonetheless, the FBI chose to operate a child pornography website that it could have shut down, thereby facilitating the continued dissemination of thousands of images of child pornography.[10] In doing so, the FBI sanctioned a more serious crime – distribution of child pornography, *see* 18 U.S.C. § 2252(b)(1) – than Mr. Croghan and others allegedly committed by accessing and viewing such images. *See* 18 U.S.C. § 2252A(a)(5)(B). The FBI also violated federal law by failing to maintain images of child pornography "in the care, custody, and control of either the Government or the court," 18 U.S.C. § 3509(m)(1), and by evidently failing to consult with the victims depicted in the images to obtain their consent to the continued dissemination of their images. *See generally* 18 U.S.C. § 3771. In sum, the FBI's misconduct epitomizes why "[g]overnmental 'investigation'

[10] According to one published report, while Playpen was under the FBI's control, it "included links to more than 23,000 sexually explicit images and videos of children, including more than 9,000 files that users could download directly from the FBI." Brad Heath, *FBI Ran Website Sharing Thousands of Child Porn Images*, USA Today, Jan. 22, 2016, at 01A (available on Westlaw at 2016 WLNR 2108860).

involving participation in activities that result in injury to the rights of its citizens is a course that courts should be extremely reluctant to sanction." *United States v. Archer*, 486 F.2d 670, 677 (2d Cir. 1973).

The government incorrectly claims that the magistrate judge is to blame for the illegal NIT warrant, so the FBI's conduct should be immunized. *See* Appellant's Br. at 41-42. Magistrate Judge Buchanan did not choose to facilitate the dissemination of child pornography for the sake of luring individuals interested in viewing child pornography. Moreover, the government's argument overlooks the fact that the FBI conceived and developed the NIT, requested the overbroad NIT warrant, and executed the warrant. Although in an "ideal system" a magistrate judge would ferret out "an unreasonable request for a warrant," it is "reasonable to require the officer applying for the warrant to minimize this danger by exercising reasonable professional judgment." *Malley v. Briggs*, 475 U.S. 335, 345-46 (1986). The FBI simply should not be immunized for executing the illegal search warrant that it requested to use malware that it developed.

The FBI also bears responsibility for the NIT warrant because it was the product of its misleading search warrant application. As the Supreme Court recognized in *Leon*, the good-faith exception does not apply when a warrant is obtained through statements made with "reckless disregard of the truth." 468 U.S.

at 923. In this case, the application falsely stated that the places to be searched (the computers that accessed Playpen) were "located in the Eastern District of Virginia." NIT App. Buried in Special Agent Macfarlane's affidavit in support of the application, he acknowledged that such searches would occur in computers that logged into Playpen "wherever located." NIT Aff. ¶ 46a. As one district court noted, it is reasonable to conclude that Magistrate Judge Buchanan may not have "understood that the NIT technology would search computers in other districts," *Workman*, 2016 WL 5791209, at *5, and if she had, "she probably would not have issued the NIT Warrant given the limitations of the Rule [41(b)]." *Id.*

Finally, the good-faith exception does not apply because the FBI should have known that the NIT warrant was invalid. *Leon* noted that the good-faith exception does not apply where a warrant is "so facially deficient – *i.e.*, in failing to particularize the place to be searched or the things to be seized." 468 U.S. at 923. Here, for the reasons previously discussed, the FBI should have realized that a warrant targeting unknown individuals in the thousands in unknown locations in the United States and worldwide was "facially deficient." *See supra* Part I.

CONCLUSION

Child pornography offenses are indisputably serious. In this case, the FBI's overzealousness in an investigation of such offenses got the better of it: the agency facilitated the continued dissemination of child pornography, and it caused the issuance of a warrant that violated constitutional, statutory, and rule-based authority. Exclusion of the evidence seized pursuant to the FBI's misdeeds is an appropriate remedy.

The district court should be affirmed.

Respectfully submitted,

/s/ Brad Hansen

BRAD HANSEN
Assistant Federal Defender
Federal Defender's Office
701 Pierce Street, Suite 400
Sioux City, Iowa 51101
PHONE: (712) 252-4158
FAX: (712) 252-4194

CERTIFICATE OF FILING AND SERVICE

I certify that on December 27, 2016, I electronically filed the foregoing brief with the Clerk of Court for the United States Court of Appeals for the Eighth Circuit by using the CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the CM/ECF system. The brief was scanned for viruses using Symantec Endpoint Protection version 12.1.6318.6100.105. I further certify that, within five days of receipt of the notice that the brief has been filed, I will transmit 10 paper copies of the brief to the Clerk of Court via FedEx and one paper copy each to David B. Goodhand (counsel for the Appellant) and Mr. Croghan via the United States Postal Service.

Respectfully submitted,

/s/ Brad Hansen

BRAD HANSEN
Assistant Federal Defender
Federal Defender's Office
701 Pierce Street, Suite 400
Sioux City, Iowa 51101
PHONE: (712) 252-4158
FAX: (712) 252-4194

FED. R. APP. P. 32(A)(7) AND 8TH CIR. RULE 28A(C) CERTIFICATION

I certify that the foregoing brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7). The brief uses a proportional space, 14 point New Times Roman font. Based on a word count under Microsoft Word Version 14.0.7159.5000, the brief contains 8,469 words and 920 lines of text.

Respectfully submitted,

/s/ Brad Hansen

BRAD HANSEN
Assistant Federal Defender
Federal Defender's Office
701 Pierce Street, Suite 400
Sioux City, Iowa 51101
PHONE: (712) 252-4158
FAX: (712) 252-4194