NO. _____

IN THE SUPREME COURT OF THE UNITED STATES

ANTHONY ALLEN JEAN,
Petitioner,
v.
UNITED STATES OF AMERICA,
Respondent

On Petition for a Writ of Certiorari to the
United States Court of Appeals for the Eighth Circuit

PETITION FOR A WRIT OF CERTIORARI

Respectfully submitted,

BRUCE D. EDDY
FEDERAL PUBLIC DEFENDER
WESTERN DISTRICT OF ARKANSAS

C. Aaron Holt
Research and Writing Specialist
Counsel of Record
3739 Steele Blvd., Ste. 280
Fayetteville, Arkansas 72703
(479) 442-2306
aaron_holt@fd.org

QUESTIONS PRESENTED FOR REVIEW

I. Can the good-faith exception to the exclusionary rule announced by this Court in *United States v. Leon*, 468 U.S. 897 (1984), be applied in cases in which a warrant is void *ab initio*?

II. If the *Leon* good-faith exception applies to warrants void *ab initio*, did law enforcement act in objectively reasonable reliance on the void warrant in performing thousands of searches of unknown computers around the world?

LIST OF PARTIES

The only parties to the proceeding are those appearing in the caption to this petition.

TABLE OF CONTENTS

Page

INDEX TO APPENDICES

TABLE OF AUTHORITIES

Rules

Constitutional Provisions

PETITION FOR A WRIT OF CERTIORARI

OPINIONS BELOW

On June 1, 2018, the court of appeals entered its opinion and judgment affirming the district court's denial of Petitioner Anthony Allen Jean's motion to suppress. *United States v. Jean*, 891 F.3d 712 (8th Cir. 2018). A copy of the opinion is attached at Appendix ("App.") A. The district court's order denying Petitioner's motion to suppress can be found at *United States v. Jean*, 207 F. Supp. 3d 920 (W.D. Ark. 2016), and it is attached at App. B.

JURISDICTION

The judgment of the court of appeals was entered on June 1, 2018. A petition for en banc and panel rehearing was timely filed on June 15, 2018. On July 11, 2018, an order was entered denying the petition for rehearing. This petition is timely submitted. Jurisdiction to review the judgment of the court of appeals is conferred upon this Court by 28 U.S.C. § 1254.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Petitioner refers this Honorable Court to the following constitutional and statutory provisions:

U.S. CONST. amend. IV:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

During the relevant time period, Federal Rule of Criminal Procedure 41(b) provided:

> **(b) Authority to Issue Warrant.** At the request of a federal law enforcement officer or an attorney for the government:
>
> **(1)** a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;
>
> **(2)** a magistrate judge with authority in the district has authority to issue a warrant for 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;
>
> **(3)** a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
>
> **(4)** a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
>
> **(5)** a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside of the jurisdiction of any state or district, but within [certain enumerated locales].

STATEMENT OF THE CASE

1. This case stems from the FBI's investigation of a child-pornography website known as "Playpen," which operated on the "Tor" network. The Tor network was originally designed by the U.S. Naval Research Laboratory and is freely available to the public. It is designed to protect user privacy and facilitate anonymous communication over the internet by routing communications through multiple computers to protect the confidentiality of the internet protocol ("IP") addresses and other identifying information of its users. The network is readily accessed by downloading free software and, like the internet in general, can be used for both legitimate and illicit purposes.

The FBI took control of the server hosting the Playpen website and transferred a copy of the site to a government facility in Virginia, where it operated that site between February 20, 2015 and March 4, 2015. Because the site's operation on the Tor network prevented the FBI from identifying the IP addresses of the site's users, it sought a warrant giving it permission to employ a "Network Investigative Technique," or "NIT," which would allow it to secretly send computer code to any computer that accessed the site. This code would search the accessing computer for certain identifying information and then transmit that information back to the government.

The government obtained a search warrant authorizing it to deploy the NIT that was issued by a U.S. Magistrate Judge in the Eastern District of Virginia. The first page of the warrant states that the property to be searched is located in the

Eastern District of Virginia. An "Attachment A" (referenced on the warrant form and entitled "Place to be Searched") indicates that the NIT is to be deployed in the Eastern District of Virginia and will "obtain[] information [specified by the warrant]" from "activating computers." The term "activating computer" is defined as the computer of "any user or administrator who logs into [Playpen] by entering a username and password." Attachment A says nothing explicit about the location(s) of the activating computers. The affidavit submitted in support of the warrant application states that the NIT will be "deployed" on the Playpen website in the Eastern District of Virginia, and only indicates in one place—on page 29 of the 31-page affidavit—that an accessing computer may be located outside the Eastern District of Virginia, when it notes that "the NIT may 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, [and] other information about the computer and the user of the computer . . . ."

2. The government was aware of the problematic nature of NIT warrants like the one at issue in this case. In 2009, the Department of Justice's Computer Crime and Intellectual Property Section alerted U.S. Attorneys of the "problems" associated with seeking such warrants under Rule 41, and recommended seeking an individual warrant in each district in which computers to be searched may be located rather than only a single NIT warrant. *See* U.S. Dep't of Justice, Criminal Div., Comput. Crime and Intellectual Prop. Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3d ed. 2009), at 84-85

(available at https://www.justice.gov/sites/default/files/criminal-ccips/2015/01/14/ssmanual2009.pdf) Two years before the FBI sought the NIT warrant at issue here, a different U.S. Magistrate Judge denied a government application for a similar warrant on the ground that it would be invalid under Rule 41(b). *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). This prompted the Department of Justice to seek the amendment of Rule 41 to allow magistrate judges to authorize NIT warrants. *See* Proceedings of Advisory Committee on Criminal Rules (Oct. 18, 2013), at 159-63 (available at http://www.uscourts.gov/sites/default/files/fr_import/CR2013-10.pdf). Those efforts resulted in the new Rule 41(b)(6), which purports to authorize magistrate judges to issue NIT warrants, and which only became effective as of December 1, 2016—almost two years after the NIT warrant here was issued.

3. After the warrant was issued, the FBI began deploying the NIT to "activating computers" all over the world. On March 4, 2015, the FBI stopped deploying the NIT and took the Playpen site offline. On or about March 1, 2015, the FBI obtained the IP address of Playpen user "regalbegal" through deployment of the NIT. FBI agents determined that the IP address associated with user "regalbegal" was operated by internet service provider Cox Communications. An administrative subpoena was served upon Cox Communications in March 2015 requesting information related to the user associated with that IP address; Cox responded with Mr. Jean's subscriber information and address. Based upon this information revealed as the direct result of the deployment of the NIT, a search warrant was obtained in

the Western District of Arkansas to search Mr. Jean's home, which was located in that district. When the search warrant was executed, certain computer equipment was seized. Analysis of this equipment revealed various images of child pornography. During the execution of the warrant, Mr. Jean cooperated with agents and made incriminating statements. He also made incriminating statements in a subsequent interview with law enforcement agents on July 17, 2015.

4. Mr. Jean moved to suppress all evidence obtained as the result of the NIT warrant and subsequently executed search warrant. He argued that the NIT warrant did not authorize deployment of the NIT to his computer in the Western District of Arkansas because the warrant, on its face, only authorized searches of property located in the Eastern District of Virginia. Alternatively, if the court were to determine that the NIT warrant authorized searches of computers across the country and around the world, Mr. Jean argued that the magistrate judge was without authority to issue the warrant under Rule 41(b). He further argued that suppression was warranted because he was prejudiced by the violation of Rule 41 and because there was evidence that the FBI had acted in reckless disregard of proper procedure.

5. The district court denied Mr. Jean's motion to suppress. The court found that the NIT warrant was adequately supported by probable cause and that it met the Fourth Amendment's particularity requirement. The court concluded that the NIT was analogous to a tracking device and that Rule 41(b)(4) therefore authorized the warrant's issuance. Although it found the seizure of evidence from Mr. Jean's

computer to be lawful on this basis, it went on to conclude that suppression would not be warranted even if Rule 41(b) had been violated. The court found that if there was any violation of the rule, it was non-fundamental, and that Mr. Jean could not show prejudice or a reckless disregard of procedure. Finally, the court determined that if the warrant were somehow deemed deficient in some respect, the good-faith exception would save the evidence from suppression.

6. After entering a conditional plea of guilty to one count of receipt of child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) & (b)(1), and one count of possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2), Mr. Jean appealed the district court's denial of his motion to suppress to the Eighth Circuit Court of Appeals. The court of appeals had jurisdiction pursuant to 28 U.S.C. § 1291, which gives it jurisdiction over all final decisions of the district courts of the United States. The district court had jurisdiction over this federal criminal case pursuant to 18 U.S.C. § 3231. Shortly after Mr. Jean filed his opening brief with the Eighth Circuit, that court decided *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018), which involved the same NIT warrant at issue in Mr. Jean's case. The court determined that the magistrate judge was not authorized to issue the NIT warrant under Rule 41(b), that this violation of the rule was of constitutional magnitude, and that the warrant was void *ab initio*. However, the court also concluded that the good-faith exception to the exclusionary rule announced by this Court in *United States v. Leon*, 468 U.S. 897 (1984), could be applied to warrants void *ab initio*, and that the exception did in fact apply to prevent

exclusion of the evidence obtained pursuant to the NIT warrant. The court of appeals ultimately followed *Horton* in affirming the district court's denial of Mr. Jean's motion to suppress on the basis that the good-faith exception applied to the NIT warrant. (App. 3-4a). Mr. Jean filed a timely petition for rehearing that was denied on July 11, 2018. (App. 31a).

This petition for a writ of certiorari follows.

REASONS FOR GRANTING THE PETITION

Based on evidence discovered as the result of the NIT warrant, the government has prosecuted over 70 individual defendants; because the NIT was deployed to approximately 9,000 computers, it is likely that evidence was collected that could lead to the prosecution of many more. The number of defendants—and potential defendants—connected to this particular warrant is sufficient by itself to warrant a grant of certiorari. But the issue of the expansion of the *Leon* good-faith exception to the exclusionary rule to situations involving void warrants has even farther-reaching effects which also merit this Court's attention. This Court has never addressed the question of whether the good-faith exception applies in situations in which the judge who issues a warrant lacks the authority to do so. This case presents an appropriate vehicle for the Court to do so.[1]

I. This Court Should Decide Whether the Good-Faith Exception Applies in Cases Involving a Warrant Determined to Be Void *Ab Initio*.

This Court has addressed the applicability of the good-faith exception in several different contexts. The exception is available when law enforcement relies in good faith on a warrant that was unsupported by sufficient probable cause. *United*

[1] Mr. Jean recognizes that the Court has denied certiorari in two cases involving the NIT warrant, *Horton v. United States*, No. 17-6910 (cert. denied Apr. 2, 2018), and *Workman v. United States*, No. 17-7042 (cert. denied Apr. 16, 2018), and that petitions for certiorari are currently pending in two other cases, *McLamb v. United States*, No. 17-9341, and *Werdene v. United States*, No. 18-5368, both of which are scheduled to be considered at the conference of September 24, 2018. Mr. Jean submits that the number of petitions filed with this Court reinforces the importance of the Court deciding the issues raised in connection with the NIT warrant, and suggests that if certiorari should be granted in one or more of these pending cases, it would be appropriate to consolidate his case with such case(s) for disposition.

States v. Leon, 468 U.S. 897, 900, 925-26 (1984). The exception is likewise available when a warrant lacks sufficient particularity, *Massachusetts v. Sheppard*, 468 U.S. 981, 987-88 (1984), when a warrant has been quashed, *Arizona v. Evans*, 514 U.S. 1, 4 (1995), and when a warrant has been recalled, *Herring v. United States*, 555 U.S. 135, 137-38 (2009). The exception has been applied when a search was performed in reliance upon a statute or binding legal decision that was later overturned. *See, e.g.*, *Davis v. United States*, 564 U.S. 229, 232, 241 (2011); *Illinois v. Krull*, 480 U.S. 340, 356-57 (1987).

However, the Court has yet to address whether the exception is available in a case in which the warrant was authorized by a judge who lacked jurisdiction to issue it. The Eighth Circuit and at least one of its sister circuits have held that such a warrant is void *ab initio*, meaning that it was as if the warrant had never been issued. *See United States v. Horton*, 863 F.3d 1041, 1049 (8th Cir. 2017); *United States v. Werdene*, 883 F.3d 204, 214 (3d Cir. 2018). To the extent the NIT warrant was construed to authorize a search of computers located outside the Eastern District of Virginia, Mr. Jean agrees that it was void *ab initio*.

Searches performed pursuant to the NIT warrant, such as the search of Mr. Jean's computer, were warrantless searches. In this case, the FBI did not rely in good faith upon a warrant that was later invalidated; instead, it performed a warrantless, unconstitutional search of Mr. Jean's computer (and thousands of others). The FBI did not rely in good faith upon a warrant because there was no warrant to rely upon.

The good-faith exception has been overextended, and this Court should grant certiorari in this case to correct this error and clearly establish the limits of *Leon*.

II. Even If the Good-Faith Exception Can Apply to Warrants Void *Ab Initio*, Law Enforcement's Reliance on the NIT Warrant Was Not Objectively Reasonable.

Even if the good-faith exception may be properly applied in cases involving void warrants, the Eighth Circuit was incorrect in applying it under the circumstances presented by the NIT warrant at issue in this case. The affiant who applied for the NIT warrant stated in the application, under oath, that the property to be searched was located in the Eastern District of Virginia. The warrant on its face authorized the search of property located in the Eastern District of Virginia. The FBI treated the warrant as authorizing the deployment of the NIT to thousands of computers all around the world, despite that fact that it was issued by a magistrate judge with clear limitations on her jurisdictional authority to issue warrants under Federal Rule of Criminal Procedure 41(b). "[T]he 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. Surely the conduct of law enforcement in connection with the NIT warrant fits under at least one of these categories, and merits deterrence. As has been pointed out above, the Department of Justice was well aware of the jurisdictional limitations of Rule 41(b), and accordingly lobbied for amendment of the rule so that NIT warrants such as the one at issue here could be validly issued in the future. A reasonably well trained officer could not have believed that the magistrate possessed the authority to issue such a warrant given the clear

limitations of Rule 41(b). Rule 41(b)(1) simply states that a magistrate can authorize a search of property "located within the district," yet the agents clearly knew that they intended to search a huge number of computers located outside the district. Law enforcement cannot be said to have acted in good faith in a case in which a magistrate judge so clearly exceeded her authority.

Mr. Jean has also argued below that the warrant, on its face, did not actually authorize the search of any computers outside the Eastern District of Virginia. The Eighth Circuit did not address this argument in its opinion, although the argument was raised in Jean's motion to suppress and in his initial brief on appeal, reiterated in his reply brief, and again raised in his petition for rehearing. The face of the NIT warrant authorized only a search of "property located in the Eastern District of Virginia," and the cover sheet of the warrant application likewise indicated that a warrant was being sought concerning property located in the Eastern District of Virginia. The only place in the warrant application where it was specified that the FBI intended to deploy the NIT to any activating computer, "wherever located," was on page 29 of the 31-page affidavit. The warrant itself did not contain this "wherever located" language in its description of what constituted an "activating computer"—or anywhere else. Even if the warrant application had plainly indicated that a warrant was being sought to search computers all over the world, it is clear that what is contained within the four corners of the actual warrant that matters. *Cf. Groh v. Ramirez*, 540 U.S. 551, 557 (2004) ("The fact that the *application* adequately described the 'things to be seized' does not save the *warrant* from its facial invalidity.

The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents."). Because the warrant itself did not allow the search of any computers outside of Virginia, law enforcement could not rely in good faith upon it to justify a search of Jean's computer in the Western District of Arkansas. The good-faith exception should not have been found to be applicable in this case, or in any other case involving a search performed outside the Eastern District of Virginia pursuant to the NIT warrant. The number of defendants and potential defendants affected by this invalidly executed warrant merits this Court's review of this case.

CONCLUSION

For all of the foregoing reasons, Petitioner Anthony Allen Jean respectfully requests that this Court grant the petition for a writ of certiorari, and accept this case for review.

DATED: this 24th day of September, 2018.

Respectfully submitted,

BRUCE D. EDDY
Federal Public Defender
Western District of Arkansas

/s/ *C. Aaron Holt*

C. Aaron Holt
Research and Writing Specialist
Office of the Federal Public Defender
3739 Steele Blvd., Ste. 280
Fayetteville, Arkansas 72703
(479) 442-2306
aaron_holt@fd.org

Counsel for Petitioner