No. _____

In the Supreme Court of the United States

JAMES KENNETH GANZER, JR., *PETITIONER*,

v.

UNITED STATES OF AMERICA, *RESPONDENT*.

PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

MAUREEN SCOTT FRANCO
Federal Public Defender

BRADFORD W. BOGAN
Assistant Federal Public Defender
Western District of Texas
727 E. César E. Chávez Blvd., B-207
San Antonio, Texas 78206-1205
(210) 472-6700
(210) 472-4454 (Fax)

Counsel of Record for Petitioner

QUESTION PRESENTED FOR REVIEW

Can the good faith exception to the Fourth Amendment's exclusionary rule apply to a search warrant that was void *ab initio*, and therefore without legal effect, because the magistrate judge who issued it lacked authority to do so?

No. _____

In the Supreme Court of the United States

JAMES KENNETH GANZER, JR., *PETITIONER*,

v.

UNITED STATES OF AMERICA, *RESPONDENT*.

PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

Petitioner James Kenneth Ganzer, Jr. asks that a writ of certiorari issue to review the opinion and judgment entered by the United States Court of Appeals for the Fifth Circuit on April 24, 2019.

PARTIES TO THE PROCEEDING

The caption of this case names all parties to the proceeding in the court whose judgment is sought to be reviewed.

TABLE OF CONTENTS

QUESTION PRESENTED FOR REVIEW i

PARTIES TO THE PROCEEDING ii

OPINION BELOW 1

JURISDICTION OF THE SUPREME COURT OF THE UNITED STATES 1

FEDERAL CONSTITUTIONAL PROVISION INVOLVED 1

FEDERAL RULE OF CRIMINAL PROCEDURE INVOLVED 1

STATEMENT 3

REASONS FOR GRANTING THE WRIT 9

CONCLUSION 19

APPENDIX *United States v. Ganzer*, 922 F.3d 579 (5th Cir. 2019)

TABLE OF AUTHORITIES

Cases

Arizona v. Evans,
514 U.S. 1 (1995) 13, 14

Herring v. United States,
555 U.S. 135 (2009) 13, 14, 15, 18

In re Warrant to Search a Target Computer at Premises Unknown,
958 F. Supp. 2d 753 (S.D. Tex. 2013) 15, 16

Steel Co. v. Citizens for Better Environment,
523 U.S. 83, 89 (1998) 14

United States v. Hazlewood,
526 F.3d 862 (5th Cir. 2008) 9, 10

United States v. Henderson,
906 F.3d 1109 (9th Cir. 2018),
cert. denied, 139 S. Ct. 2033 (2019) 9, 12

United States v. Horton,
863 F.3d 1041 (8th Cir. 2017),
cert. denied, 138 S. Ct. 1440 (2018) 9, 11, 12

United States v. Kienast,
907 F.3d 522 (7th Cir. 2018) 9, 12

United States v. Krueger,
809 F.3d 1109 (10th Cir. 2015) 9, 14

United States v. Leon,
468 U.S. 897 (1984) 13, 15, 18

United States v. Levin,
874 F.3d 316 (1st Cir. 2017) 8, 12

United States v. McLamb,
880 F.3d 685 (4th Cir.),
cert. denied, 139 S. Ct. 156 (2018) 8, 12

United States v. Moorehead,
912 F.3d 963 (6th Cir. 2019),
cert. denied, 139 S. Ct. 1639 (2019) 9, 12

United States v. Werdene,
883 F.3d 204 (3d Cir.),
cert. denied, 139 S. Ct. 260 (2018) 8, 9, 11, 12

United States v. Workman,
863 F.3d 1313 (10th Cir. 2017),
cert. denied, 138 S. Ct. 1548 (2018) 9, 12, 13

Constitutional Provision

U.S. Const., amend. IV 1, 8, 15, 18

Statutes

18 U.S.C. § 1030(a)(5) 3

18 U.S.C. § 2252A(a)(5)(B) 6

18 U.S.C. § 2252A(b)(2) 6

28 U.S.C. § 636 ..... 7, 10

28 U.S.C. § 636(a) 9, 10, 11, 12

28 U.S.C. § 1254(1) 1

Rules

Fed. R. Crim. P. 41 17

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

Fed. R. Crim. P. 41(b)(1) 10, 16

Fed. R. Crim. P. 41(b)(2) 10

Fed. R. Crim. P. 41(b)(3) 10

Fed. R. Crim. P. 41(b)(4) 7, 10

Fed. R. Crim. P. 41(b)(5) 11

Fed. R. Crim. P. 41(b)(6) 11

Sup. Ct. R. 10(c) 19

Sup. Ct. R. 13.1 1

Other Authorities

Advisory Committee on Criminal Rules, Minutes (Apr. 7–8, 2014) 17

Memo from Sara Beale and Nancy King to Members, Criminal Rules Advisory Committee, Re: Rule 41 Proposal (Mar. 17, 2014) 17

Mythli Raman, Letter to the Honorable Reena Raggi, in Advisory Committee on Criminal Rules, Materials for April 7–8, 2014, Meeting (2013) 16, 17

Zoe Russell, Comment, *First They Came for the Pornographers: The FBI's International Search Warrant to Hack the Dark Web*, 49 St. Mary's L.J. 269 (2017) 4, 16

OPINION BELOW

The published opinion of the Fifth Circuit, *United States v. Ganzer*, 922 F.3d 579 (2019), is reproduced at Pet. App. 1a–12a.

JURISDICTION OF THE SUPREME COURT OF THE UNITED STATES

The Fifth Circuit entered its judgment on April 24, 2019. This petition is filed within 90 days after entry of judgment. *See* Sup. Ct. R. 13.1. The Court has jurisdiction to grant certiorari under 28 U.S.C. § 1254(1).

FEDERAL CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the United States Constitution reads:

> 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.

FEDERAL RULE OF CRIMINAL PROCEDURE INVOLVED

When the magistrate judge issued the warrant at issue in this case, Federal Rule of Criminal Procedure 41(b) read:

> (b) Authority to Issue a 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 the jurisdiction of any state or district, but within any of the following:
    (A) a United States territory, possession, or commonwealth;
    (B) the premises—no matter who owns them--of a United States diplomatic or consular mission in

> a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Effective December 1, 2016—after the warrant at issue in this case was issued—Rule 41(b) was amended to include paragraph 6:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> (A) the district where the media or information is located has been concealed through technological means; or
>
> (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

STATEMENT

1. This case arises out of the Government's seizure and continued operation of a child pornography website called "Playpen," and a warrant issued by a magistrate judge in the Eastern District of

Virginia to search any computer, anywhere in the world, that accessed the site during that time.[1]

Playpen was a message board website whose primary purpose was the advertisement and distribution of child pornography. It operated on "The Onion Router" (TOR), which is an anonymity network originally developed by the U.S. Navy to protect government communications, and now available to the public at large. It protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user."

FBI agents began accessing Playpen in September 2014. They seized the site in January 2015 after learning of its location from a foreign law enforcement agency. Rather than shutting down Playpen, the FBI, in an effort to identify the site's users, continued

---

[1] The warrant has spawned dozens of prosecutions around the country, and perhaps as many challenges to its validity. *See generally* Zoe Russell, Comment, *First They Came for the Pornographers: The FBI's International Search Warrant to Hack the Dark Web*, 49 St. Mary's L.J. 269 (2017).

to operate it from a government-controlled server in the Eastern District of Virginia.

Because of the anonymity provided by TOR, in February 2015 the FBI obtained a warrant from a magistrate judge in the Eastern District of Virginia to employ a "network investigative technique" (NIT) to identify visitors to Playpen. The NIT worked by attaching computer code to Playpen users when they logged onto the Playpen website, and that code directed the user's computer to send the user's IP address and other identifying information to federal investigators.[2] By its terms, the warrant authorized the Government

---

[2] Specifically, the warrant authorized collection of:

1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);

to deploy the NIT to extract information from any computer that accessed Playpen, regardless of whether that computer was within or outside the Eastern District of Virginia.

In early March 2015, the NIT extracted computer information from a Playpen user who went by the name "marleyboy." The IP address was associated with Ganzer's residence in Austin, Texas. In December 2015, using the information extracted by the NIT, investigators obtained a search warrant for Ganzer's residence from a magistrate judge in the Western District of Texas. They found videos and still images of child pornography on Ganzer's computer. Ganzer admitted, in interviews at his home and at a police substation, that he possessed the pornography.

2. Ganzer was charged in a single-count indictment with possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2).

---

4. information about whether the NIT has already been delivered to the "activating" computer;
5. the "activating" computer's Host Name;
6. the "activating" computer's active operating system username;
7. the "activating" computer's media access control ("MAC") address[.]

Ganzer filed a motion to suppress all of the evidence—that was found on his computer, as well as his statements to investigators—obtained from the execution of the warrant. He argued, among other things, that the NIT warrant was invalid because the Federal Magistrates Act, 28 U.S.C. § 636, and Federal Rule of Criminal Procedure 41(b) did not authorize a magistrate judge in the Eastern District of Virginia to issue a search warrant for a computer outside that district, and that the good-faith exception did not apply to the FBI's execution of the warrant.

The district court denied Ganzer's motion. In a written order, the court concluded that the NIT warrant violated Rule 41(b) because Ganzer's computer was not in the Eastern District of Virginia at the time the warrant was issued or at the time the NIT extracted information from it, and because the NIT was not a "tracking device" within the meaning of Rule 41(b)(4). But the court ruled that the good-faith exception to the exclusionary rule applied, concluding that the warrant was supported by probable cause and that the FBI sought and obtained the warrant in good faith. The court also said that "[t]he deterrent purpose of the exclusionary rule would have little or no effect in this case because Rule 41(b) has been amended since the NIT warrant was issued to

explicitly allow magistrate judges to issues warrants like the NIT warrant."

After the district court denied the suppression motion, Ganzer pleaded guilty conditionally, reserving his right to appeal the denial of his motion to suppress. The district court sentenced Ganzer to 60 months' imprisonment, to be followed by 10 years' supervised release. Ganzer appealed.

3. The Fifth Circuit affirmed the district court's denial of Ganzer's motion to suppress. The court of appeals assumed, without deciding, that the magistrate judge in Virginia did not have authority to issue the NIT warrant, "that the warrant was void *ab initio* and … never had any legal effect[,]" and that deploying the NIT to search Ganzer's computer violated the Fourth Amendment. Pet. App. 6a, 8a. But the court held that the good faith exception can apply to warrants that are void *ab initio*, and that it applied to the NIT warrant in particular. Pet. App. 9a–12a. In so holding, the Fifth Circuit joined all other circuits that have addressed the question. Pet. App. 12a; *see United States v. Levin*, 874 F.3d 316, 321–24 (1st Cir. 2017); *United States v. Werdene*, 883 F.3d 204, 215–18 (3d Cir.), *cert. denied*, 139 S. Ct. 260 (2018); *United States v. McLamb*, 880 F.3d 685, 689–91 (4th Cir.), *cert. denied*, 139 S. Ct. 156 (2018); *United States v. Moorehead*, 912 F.3d 963, 967 (6th Cir.

2019), *cert. denied*, 139 S. Ct. 1639 (2019); *United States v. Kienast*, 907 F.3d 522, 527–29 (7th Cir. 2018); *United States v. Horton*, 863 F.3d 1041, 1049–52 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018); *United States v. Henderson*, 906 F.3d 1109, 1120 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 2033 (2019); *United States v. Workman*, 863 F.3d 1313, 1317 (10th Cir. 2017), *cert. denied*, 138 S. Ct. 1548 (2018).

REASONS FOR GRANTING THE WRIT

"The Federal Magistrates Act, 28 U.S.C. § 636(a), authorizes federal magistrate judges to exercise the 'powers and duties conferred ... by the Rules of Criminal Procedure' in three geographic areas: '[1] within the district in which sessions are held by the court that appointed the magistrate judge, [2] at other places where that court may function, and [3] elsewhere as authorized by law.'" *United States v. Werdene*, 883 F.3d 204, 210 (3d Cir. 2018) (quoting statute; alterations in *Werdene*); *see also United States v. Krueger*, 809 F.3d 1109, 1118 (10th Cir. 2015) (Gorsuch, J., concurring). Thus, § 636(a) creates "'jurisdictional limitations on the power of magistrate judges' because it 'expressly and independently limits where those powers will be effective.'" *Id.* (quoting *Krueger*, 809 F.3d at 1119 (Gorsuch, J., concurring)); *see also United States v. Hazlewood*, 526 F.3d 862, 864 (5th Cir. 2008) ("In

the Federal Magistrates Act, 28 U.S.C. § 636, Congress conferred jurisdiction to federal magistrate-judge[s] ….”). What’s more, “[w]hile § 636(a) defines the geographic scope of a magistrate judge’s powers, the Rules of Criminal Procedure—including Rule 41(b)—define *what* those powers are.” *Id.*

Rule 41(b) authorizes a magistrate judge “to issue a warrant to search for and seize a person or property located within the district[.]” Fed. R. Crim. P. 41(b)(1). At the time the NIT warrant issued, in February 2015, Rule 41(b) contained four exceptions to this general geographic restriction:

1. for property that is located within the district at the time the warrant issues but which might move outside the district by the time the warrant is executed, Fed. R. Crim. P. 41(b)(2);
2. for property in terrorism investigations, Fed. R. Crim. P. 41(b)(3);
3. to install a tracking device on property within the district to track its movement outside the district, Fed. R. Crim. P. 41(b)(4); and

4. for property located outside the jurisdiction of any state or district, if activities related to the crime occurred within the district, Fed. R. Crim. P. 41(b)(5).

"Notably, none of these Rule 41(b) exceptions expressly allow a magistrate judge in one jurisdiction to authorize the search of a computer in a different jurisdiction." *Werdene*, 883 F.3d at 210 (quoting *United States v. Horton*, 863 F.3d 1041, 1047 (8th Cir. 2017), *cert. denied* 138 S. Ct. 1440 (2018)) (cleaned up).[3]

For that reason, the magistrate judge in the Eastern District of Virginia lacked jurisdiction to issue a warrant for a search of computers outside her district, and "the NIT warrant was void *ab initio*," making it "the constitutional equivalent of a warrantless search." *Horton*, 863 F.3d at 1049; *see Werdene*, 883 F.3d at 214 ("The magistrate judge not only exceeded the territorial scope of Rule 41(b), but, as a result of that violation, she also exceeded the jurisdiction that § 636(a) imposes on magistrate judges. … The

[3] "On December 1, 2016, Rule 41(b) was amended to authorize magistrate judges to issue warrants to search computers and seize or copy electronically stored information located outside the magistrate judge's district if the district where the computer or information is located has been concealed through technological means." *Werdene*, 883 F.3d at 206 n.2 (citing Fed. R. Crim. P. 41(b)(6)).

NIT warrant was therefore void *ab initio* because it violated § 636(a)'s jurisdictional limitations and was not authorized by any positive law.")

Nevertheless, every court of appeals to have addressed the question has held that the good faith exception to the exclusionary rule excused the Government's reliance on the NIT warrant. *see United States v. Levin*, 874 F.3d 316, 321–24 (1st Cir. 2017); *United States v. Werdene*, 883 F.3d 204, 215–18 (3d Cir.), *cert. denied*, 139 S. Ct. 260 (2018); *United States v. McLamb*, 880 F.3d 685, 689–91 (4th Cir.), *cert. denied*, 139 S. Ct. 156 (2018); *United States v. Ganzer*, 922 F.3d 579 (5th Cir. 2019) (reproduced in Pet. App.); *United States v. Moorehead*, 912 F.3d 963, 967 (6th Cir. 2019), *cert. denied*, 139 S. Ct. 1639 (2019); *United States v. Kienast*, 907 F.3d 522, 527–29 (7th Cir. 2018); *United States v. Horton*, 863 F.3d 1041, 1049–52 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018); *United States v. Henderson*, 906 F.3d 1109, 1120 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 2033 (2019); *United States v. Workman*, 863 F.3d 1313, 1317 (10th Cir. 2017), *cert. denied*, 138 S. Ct. 1548 (2018). That exception "allow[s] admission at trial of 'evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate' but later invalidated." Pet. App. 7a (quoting *United States v. Leon*, 468 U.S.

897, 900 (1984)). Those decisions, and the decision below, are wrong, given the nature of the violation here and the circumstances surrounding the issuance of the NIT warrant.

This Court has never addressed whether the good-faith exception applies to warrants issued without jurisdiction. Courts considering this issue have thus far looked to *Herring v. United States*, 555 U.S. 135 (2009), and *Arizona v. Evans*, 514 U.S. 1 (1995). *See Workman*, 863 F.3d at 1318–19. These cases do not hold or suggest that the good faith exception should apply to a case in which the magistrate issuing the search warrant lacked jurisdiction.

Both *Herring* and *Evans* considered cases in which the police arrested an individual based on failure-to-appear arrest warrants issued by local courts. *Herring*, 555 U.S. at 137; *Evans*, 514 U.S. at 4–5. In both cases, the arrest warrant had in actuality been withdrawn, *Herring*, 555 U.S. at 138, or quashed, *Evans*, 514 U.S. at 4, by the time the police encountered the defendant and arrested him based on the warrant. Still, in both cases, the arresting officer believed that a warrant existed because of a notation in a computer system and arrested the defendant on that basis. *Herring*, 555 U.S. at 138; *Evans*, 514 U.S. at 5. There was no question in either case about the conduct of government agents in seeking a search warrant and no question that the court or judge in question could issue

the arrest warrant after the defendant failed to appear. Conceptually, then, these cases stand for nothing more than the proposition that an officer acted reasonably when he relied on computer databases that informed him that an arrest warrant existed.

This case is different because the magistrate judge did not have jurisdiction to issue the NIT warrant in the first place. Unlike the existence or non-existence of a notation in a computer database, the defect in the NIT warrant is fundamental and goes to "the court['s] statutory or constitutional power to adjudicate the case." *Steel Co. v. Citizens for Better Environment*, 523 U.S. 83, 89 (1998). The jurisdictional issue in this case is the territorial limitation imposed by statute on a magistrate judge, something that Congress has tightly controlled. *Krueger*, 809 F.3d at 1121 (Gorsuch, J., concurring) ("Congress has always taken care to impose relatively tight territorial limits on the powers of magistrate judges and their predecessors (commissioners)."). Given the gulf between *Herring* and *Evans* and the case at hand, the Court should resist any request to extend the good faith exception to this case.

Even if the good faith exception could apply to a warrant issued without jurisdiction, the exception should not apply here because the government acted recklessly or with gross negligence in seeking the warrant. "[S]uppression is not an automatic consequence

of a Fourth Amendment violation." *Herring*, 555 U.S. at 137. "Instead, the question turns on the culpability of the police and the potential of exclusion to deter wrongful police conduct." *Id*. "The basic insight of the *Leon* line of cases is that the deterrence benefits of exclusion vary with the culpability of the law enforcement conduct at issue. When the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs." *Davis*, 564 U.S. at 238 (cleaned up). The record in this case amply demonstrates that the government acted recklessly or with gross negligence in seeking a warrant that it knew was beyond the scope of Rule 41(b). Accordingly, the good faith exception should not apply.

Even before seeking the NIT warrant, the Department of Justice understood that Rule 41(b) did not authorize it. This understanding is demonstrated by the DOJ's request for an amendment to Rule 41(b) that would authorize such NIT warrants. Indeed, the effort to amend Rule 41(b) began just a few months after a magistrate judge in the Southern District of Texas denied a similar NIT warrant in an unrelated fraud investigation in April 2013, in *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). In that case, the judge denied the

warrant in part because "the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)." *Id.* at 757.

In the aftermath of that decision, the DOJ sought an amendment to Rule 41(b) that would specifically authorize this type of warrant. *See* Zoe Russell, Comment, *First They Came for the Child Pornographers: The FBI's International Search Warrant to Hack the Dark Web*, 49 St. Mary's L.J. 269, 274–75 (2017). On September 28, 2013, the DOJ wrote to the chair of the Advisory Committee on the Criminal Rules and asked for an amendment that would "authorize[ ] a court in a district where activities related to a crime have occurred to issue a warrant—to be executed via remote access—for electronic storage media and electronically stored information located within or outside that district." Mythli Raman, Letter to the Honorable Reena Raggi, in Advisory Committee on Criminal Rules, Materials for April 7–8, 2014, Meeting at 171 (2013).[4] Among the reasons for the amendment, the letter pointed to the

---

[4] *Available at* http://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf (last visited July 23, 2019).

magistrate judge's decision in the Southern District of Texas. *Id.* at 172. The Advisory Committee's notes likewise reflect the decision. *See* Memo from Sara Beale and Nancy King to Members, Criminal Rules Advisory Committee, Re: Rule 41 Proposal at 3 (Mar. 17, 2014).[5] At a later meeting of the Advisory Committee on Criminal Rules, a representative of the DOJ acknowledged that Rule 41(b) "on its face does not work with" cases involving anonymizing sites like the Tor network and suggested that, absent the requested amendment, the Government would be left to litigate the issue and "hope the courts will create an exception to" Rule 41(b). *See* Advisory Committee on Criminal Rules, Minutes at 13 (Apr. 7–8, 2014).[6]

While the decision from the Southern District of Texas was just one case, the fact that the DOJ took specific and concrete action in response to that decision demonstrates an official recognition on the part of the federal law enforcement apparatus as a whole that the decision set forth the correct interpretation of Rule 41's limits in this setting. In short, the potential limitations of Rule 41(b) were

---

[5] *Available at id.*

[6] *Available at* http://www.uscourts.gov/sites/default/files/fr_import/criminal-min-04-2014.pdf (last visited July 23, 2019).

well understood by the government more than a year before federal agents sought the NIT warrant in this case, thus defeating any claim of good faith.

This then is one of those cases where evidence should be suppressed because the DOJ can properly be charged with having foreknowledge that the search would be unconstitutional under the Fourth Amendment. *Herring*, 555 U.S. at 143 ("evidence should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment") (cleaned up). Said differently, because of the Government's knowledge about the state of the law, this is one of those cases where the suppression of evidence will "result in appreciable deterrence" and exclusion is therefore appropriate. *Leon*, 468 U.S. at 909 (cleaned up). It is not enough to say that there is nothing to deter because Rule 41(b) now authorizes magistrate judges to issue warrants like the NIT warrant. Suppressing the evidence in this case will help deter the Government in the future from asking magistrate judges to issue warrants that they do not have jurisdiction to issue.

This question—whether the good faith exception to the exclusionary rule applies to a warrant that was void *ab initio*—is an

important one that this Court has not yet addressed. Thus, notwithstanding the unanimity of the courts of appeals on this question, it is a question should be resolved by this Court. *See* Sup. Ct. R. 10(c).

CONCLUSION

For these reasons, the Court should grant the petition.

Respectfully submitted.

MAUREEN SCOTT FRANCO
Federal Public Defender
Western District of Texas
727 E. César E. Chávez Blvd., B-207
San Antonio, Texas 78206
Tel.: (210) 472-6700
Fax: (210) 472-4454

s/ Bradford W. Bogan
BRADFORD W. BOGAN
Assistant Federal Public Defender

Attorney for Defendant-Appellant

DATED: July 23, 2019