

NO. \_\_\_\_\_

---

---

IN THE SUPREME COURT OF THE UNITED STATES

---

BRYAN GILBERT HENDERSON,

DUMAKA HAMMOND,

*Petitioners,*

v.

UNITED STATES OF AMERICA,

*Respondent.*

---

On Petition for Writ of Certiorari to the  
United States Court of Appeals  
For the Ninth Circuit

---

---

**PETITION FOR WRIT OF CERTIORARI**

---

---

STEVEN G. KALAR  
Federal Public Defender  
HANNI M. FAKHOURY\*  
Assistant Federal Public Defender  
*\*Counsel of Record*  
1301 Clay Street, Suite 1350N  
Oakland, CA 94612  
(510) 637-3500  
hanni\_fakhoury@fd.org

### QUESTION PRESENTED FOR REVIEW

Whether the good faith exception to the exclusionary rule of *United States v. Leon*, 468 U.S. 897 (1984) applies when law enforcement makes an obvious, systemic and deliberate mistake of Fourth Amendment law while executing a search warrant?

### **INTERESTED PARTIES**

There are no parties to the proceeding other than those named in the caption of the case.

## TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	iv
INTRODUCTION.....	1
OPINIONS BELOW .....	1
STATEMENT OF JURISDICTION.....	1
CONSTITUTIONAL PROVISION INVOLVED .....	2
STATUTORY PROVISION INVOLVED.....	2
STATEMENT OF FACTS .....	2
A.    The NIT Operation.....	3
B.    District Court Proceedings.....	5
1.    Mr. Henderson’s Case. ....	5
2.    Mr. Hammond’s Case. ....	5
C.    The Ninth Circuit Finds a Fourth Amendment Violation But Declines to Suppress.....	6
REASON FOR GRANTING THE WRIT .....	9
A.    This Court Has Never Decided Whether a Mistake of Constitutional Law Made by the Government When Executing a Warrant Triggers the Good Faith Exception to the Exclusionary Rule.....	10
B.    This Case Presents an Ideal Vehicle for Resolving the Issue.....	12
1.    The Government Made an “Obvious” Mistake of Law.....	13
2.    The Government’s Misconduct Was Systemic, Deliberate and Reckless. ....	15
CONCLUSION .....	20
APPENDIX .....	1a



## TABLE OF AUTHORITIES

### Cases

<i>Arizona v. Evans</i> , 514 U.S. 1 (1995) .....	10, 11
<i>Bryan v. United States</i> , 524 U.S. 184 (1998) .....	9
<i>Davis v. United States</i> , 564 U.S. 229 (2011) .....	10, 11, 15
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004) .....	13
<i>Hein v. North Carolina</i> , 135 S. Ct. 530 (2014) .....	11, 12, 20
<i>Herring v. United States</i> , 555 U.S. 135 (2009) .....	15, 16
<i>Hope v. Pelzer</i> , 536 U.S. 730 (2002) .....	20
<i>Hudson v. Michigan</i> , 547 U.S. 586 (2006) .....	19
<i>Illinois v. Krull</i> , 480 U.S. 340 (1987) .....	10
<i>In re Warrant to Search a Target Computer at Premises Unknown</i> , 958 F. Supp. 2d 753 (S.D. Tex. 2013) .....	17, 18
<i>Massachusetts v. Sheppard</i> , 468 U.S. 981 (1984) .....	10
<i>Riley v. California</i> , 573 U.S. 373 (2014) .....	16
<i>United States v. Horton</i> , 863 F.3d 1041 (8th Cir. 2017), <i>cert denied</i> 138 S. Ct. 1440 (2018) .....	3, 8, 9, 13

<i>United States v. Johnson</i> , 457 U.S. 537 (1982) .....	20
<i>United States v. Jones</i> , 565 U.S. 400 (2012) .....	7
<i>United States v. Kienast</i> , 907 F.3d 522 (7th Cir. 2018), <i>cert petition docketed</i> March 22, 2019, No. 18-1248 ....	2
<i>United States v. Krueger</i> , 809 F.3d 1109 (10th Cir. 2015) .....	8, 9, 13
<i>United States v. Leon</i> , 468 U.S. 897 (1984) .....	9, 10, 11, 14
<i>United States v. Levin</i> , 874 F.3d 316 (1st Cir. 2017) .....	2
<i>United States v. McLamb</i> , 880 F.3d 685 (4th Cir. 2018), <i>cert denied</i> 139 S. Ct. 156 (2019) .....	2, 8
<i>United States v. Moorehead</i> , 912 F.3d 963 (6th Cir. 2019) .....	2
<i>United States v. Potts</i> , 586 F.3d 823 (10th Cir. 2009) .....	15
<i>United States v. Vasey</i> , 834 F.3d 782 (9th Cir. 1987) .....	15
<i>United States v. Werdene</i> , 883 F.3d 204 (3d Cir. 2018), <i>cert denied</i> 139 S. Ct. 260 (2018) .....	<i>passim</i>
<i>United States v. Workman</i> , 863 F.3d 1313 (10th Cir. 2017), <i>cert denied</i> 138 S. Ct. 1546 (2018) .....	3

### Statutes

18 U.S.C. § 2252 .....	5, 6
18 U.S.C. § 2510 .....	4
28 U.S.C. § 1254 .....	1

28 U.S.C. § 636 .....	7
-----------------------	---

### **Federal Rules**

Federal Rule of Criminal Procedure 41.....	<i>passim</i>
--	---------------

## **INTRODUCTION**

Petitioners Bryan Gilbert Henderson and Dumaka Hammond respectfully petition this Court for a writ of *certiorari* to review the judgments of the United States Court of Appeals for the Ninth Circuit in their respective cases.

## **OPINIONS BELOW**

The Ninth Circuit's published opinion affirming Mr. Henderson's conviction is reported at 906 F.3d 1109 (9th Cir. 2018), and included in the Appendix ("App.") at 2a. Its January 2, 2019 order denying Mr. Henderson's petition for rehearing en banc is unreported and included in the Appendix at 15a.

The Ninth Circuit's unpublished memorandum affirming Mr. Hammond's conviction, issued the same day as the opinion in *Henderson*, is reported at 740 Fed. Appx. 573 (9th Cir. 2018) and included in the Appendix at 16a. Its January 2, 2019 order denying Mr. Hammond's petition for rehearing en banc is unreported and included in the Appendix at 19a.

## **STATEMENT OF JURISDICTION**

Pursuant to Supreme Court Rule 12.4, because Mr. Henderson and Mr. Hammond's petitions involve two "judgments...to the same court and involve identical or closely related questions," they are filing a single petition seeking review of both judgments. The two cases were consolidated for oral argument before the Ninth Circuit.

This Court has jurisdiction under 28 U.S.C. § 1254(1). The Ninth Circuit entered its judgment in favor of respondent in both cases on October 23, 2018, denied

both petitions for rehearing en banc on January 2, 2019, and issued its mandate in both cases on January 10, 2019. This petition is filed within 90 days of the Ninth Circuit's denial of both petitions for rehearing en banc, and therefore timely under Sup. Ct. R. 13.3.

### **CONSTITUTIONAL PROVISION INVOLVED**

The Fourth Amendment states

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.

U.S. Const. AMEND. IV.

### **STATUTORY PROVISION INVOLVED**

The text of Federal Rule of Criminal Procedure 41 in effect in 2015 is reproduced in the Appendix at 21a.

### **STATEMENT OF FACTS**

Mr. Henderson and Mr. Hammond's convictions stem from a nationwide FBI operation targeting a child pornography website known as "Playpen." The operation has resulted in several published opinions from the federal Courts of Appeals. *See, e.g., United States v. Levin*, 874 F.3d 316 (1st Cir. 2017); *United States v. Werdene*, 883 F.3d 204 (3d Cir. 2018), *cert denied* 139 S. Ct. 260 (2018); *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), *cert denied* 139 S. Ct. 156 (2019); *United States v. Moorehead*, 912 F.3d 963 (6th Cir. 2019); *United States v. Kienast*, 907 F.3d 522 (7th Cir. 2018), *cert petition docketed* March 22, 2019, No. 18-1248; *United States*



*v. Horton*, 863 F.3d 1041 (8th Cir. 2017), *cert denied* 138 S. Ct. 1440 (2018); *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017), *cert denied* 138 S. Ct. 1546 (2018).

As a result, the facts in Mr. Henderson and Mr. Hammond’s respective cases are materially similar to each other, as well as these cited cases.

**A. The NIT Operation.**

In September 2014, FBI agents began investigating a child pornography website known as “Playpen,” which was accessible on the Tor computer network.

The Tor network consists of a computer network and software that provide Internet users with online anonymity by obscuring how and where users get online. Users first download Tor software onto their computers to connect to a network of computers—known as “nodes” or “relays”—operated by volunteers. When connected to Tor, a user’s Internet traffic does not go directly to the website. Instead, the user is connected to a volunteer node or relay, which passes the user’s Internet traffic to another volunteer node or relay, and so on, until it transits through an “exit node” and connects to the website. This allows users to mask their true location because the destination website will only know the Internet Protocol (“IP”) address of the exit node computer, not the original computer that sought to access the website. Tor users can also access “hidden services,” which are websites hosted on the Tor network that do not reveal its location. 3a.

Playpen operated as a Tor hidden service, accessible only through the Tor network. A visitor to the site logged in with a username and password and then could view the content on the website, which included discussion forums, private messaging

services, and images of child pornography. 3a.

The FBI learned the Playpen website was hosted on a server in North Carolina. In January 2015, the FBI executed a search warrant in the Western District of North Carolina and seized the server and website. *Id.* Rather than shut down the website, however, the FBI placed a copy of the seized server, including the child pornography contained on Playpen, onto a government-controlled server in Virginia. *Id.*

On February 20, 2015, federal prosecutors obtained a search warrant from a magistrate judge in the Eastern District of Virginia, authorizing it to deploy computer software called a Network Investigative Technique (“NIT”) onto the computers of users visiting the Playpen site, “wherever located,” when they logged into the site now controlled by the government. 4a. The NIT was inserted into the Playpen site and discreetly collected information directly from the user’s computer and then transmitted that information back to the FBI. Collected information included the user’s IP address. *Id.* The government also obtained authorization from a district judge to intercept electronic communications sent on the site in real time under the Wiretap Act, 18 U.S.C. §§ 2510, et. seq. *Id.*

Although the government was authorized to deploy the NIT for 30 days, on March 4, 2015, it abruptly stopped deploying the NIT and took the Playpen website offline. By then, the FBI had collected the IP addresses of thousands of computers across the country, which it used to make individualized federal cases nationwide.

**B. District Court Proceedings.**

**1. Mr. Henderson's Case.**

On March 1, 2015, a user logged into Playpen with the username "askjeff." 4a. The NIT was deployed onto "askjeff's" computer, revealing its IP address. The FBI used an administrative subpoena to determine this IP address had been assigned by Comcast to a house in San Mateo, California where Mr. Henderson lived. In August 2015, the FBI obtained a search warrant to search the home, and seized a number of computers and electronic devices. 4a.

Mr. Henderson was indicted for receiving child pornography, in violation of 18 U.S.C. § 2252(b)(2). 4a. He filed a motion to suppress the NIT warrant, arguing it violated Federal Rule of Criminal Procedure 41 because the Eastern District of Virginia magistrate judge who issued the NIT warrant could not authorize a search in the Northern District of California. 5a. the district court found a Rule 41 violation but denied the motion to suppress. Mr. Henderson plead guilty with a conditional plea agreement preserving his right to appeal the denial of the suppression motion. *Id.*

**2. Mr. Hammond's Case.**

The facts of Mr. Hammond's case are essentially identical to those in Mr. Henderson's case. During the time the FBI controlled Playpen, a user logged into the site with the username "jerkjerk." The NIT was deployed onto "jerkjerk's" computer, revealing its IP address. The FBI used an administrative subpoena to determine this IP address had been assigned by Comcast to a house in Richmond, California where



Mr. Hammond lived. In July 2015, the FBI obtained a search warrant to search the home, and seized a number of computers and electronic devices.

Mr. Hammond was indicted for possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). He filed a motion to suppress the NIT warrant, arguing it violated Rule 41 because the Eastern District of Virginia magistrate judge who issued the NIT warrant could not authorize a search in the Northern District of California. The district court found a Rule 41 violation but denied the motion to suppress. Mr. Hammond plead guilty with a conditional plea agreement preserving his right to appeal the denial of the suppression motion.<sup>1</sup>

**C. The Ninth Circuit Finds a Fourth Amendment Violation But Declines to Suppress.**

In Mr. Henderson's case, the Ninth Circuit decided in a published opinion that the NIT warrant violated the plain text of Rule 41(b), which at the time only allowed a magistrate judge "to issue a warrant to search for and seize a person or property *located within the district.*" 5a (quoting Fed. R. Crim. P. 41(b)(1) (2015) (emphasis in original)). There was no dispute that the NIT warrant issued in the Eastern District of Virginia authorized a search of Mr. Henderson's computer in Northern California. 5a. The court rejected the government's argument that the NIT warrant was a "tracking device" warrant authorized under Rule 41(b)(4). 6a. It noted that Rule 41(b) was amended on December 1, 2016 to "plainly... 'authorize[] warrants such as the NIT warrant here.'" 7a (quoting *Werdene*, 883 F.3d at 206, n.2). Thus, the Ninth Circuit

---

<sup>1</sup> The government filed a cross-appeal of the sentence in *Hammond*, which is not before this Court.

believed the “fact that Rule 41 was amended to authorize specifically these sorts of warrants further supports the notion that Rule 41(b) did not previously do so.” 7a.

Next, the court rejected the government’s argument that Rule 41 was “merely a technical ‘venue provision.’” 8a. It explained that federal magistrate judges “are creatures of statute,” specifically 28 U.S.C. § 636 which “defines the scope of a magistrate judge’s authority, imposing jurisdictional limitations on the power of magistrate judges that cannot be augmented by the courts.” *Id.* Section 636 authorizes magistrate judges to exercise powers contained within the Federal Rules of Criminal Procedure, and thus Rule 41(b) is “the sole source of the magistrate judge’s purported authority to issue the NIT warrant in this case.” *Id.* The court found the Eastern District of Virginia magistrate judge “exceeded the scope of her authority and jurisdiction” because Rule 41(b) did not permit her to authorize a search of Mr. Henderson’s computer in the Northern District of California. *Id.*

The Ninth Circuit found this violation constitutional. It explained the Fourth Amendment “must provide *at a minimum* the degree of protection...afforded when it was adopted.” 9a (quoting *United States v. Jones*, 565 U.S. 400, 411 (2012) (emphasis in original)). Citing Blackstone, the panel noted that “[a]t the time of the framing,” a warrant could only be executed “so far as the jurisdiction of the magistrate and himself extends” and that “acts done beyond, or without jurisdiction...are utter nullities.” 9a (quotations, citations and brackets omitted). Citing a Tenth Circuit opinion by then-Judge Gorsuch, the Ninth Circuit explained

[L]ooking to the common law at the time of the framing it becomes quickly obvious that a warrant issued for a search or seizure beyond the territorial jurisdiction of a magistrate's powers under positive law was treated as no warrant at all—as *ultra vires* and *void ab initio* . . .—as null and void without regard to potential questions of ‘harmlessness.’

10a (quoting *United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring) (quotations omitted). The court noted both the Third and Eighth Circuits found the Rule 41 violation during the NIT operation was “a fundamental, constitutional error.” 10a (citing *Werdene*, 883 F.3d at 214; *Horton*, 863 F.3d at 1049). The Ninth Circuit agreed, concluding, “a warrant purportedly authorizing a search beyond the jurisdiction of the issuing magistrate judge is void under the Fourth Amendment.” 11a.

Despite this clear mistake of law, the Ninth Circuit declined to suppress the evidence. Instead, it determined the government acted in good faith and the exclusionary rule did not apply. 14a. Although “every circuit court that has addressed the question has found the NIT warrant violated Rule 41,” and the panel found the violation was—in the words of then-Judge Gorsuch—a “obvious” violation of the Fourth Amendment from the time of the framing, it nonetheless believed the “legality” of the NIT was “unclear.” 13a (citing *McLamb*, 880 F.3d at 691) (quotations omitted). The panel wondered “how an executing agent ought to have known that the NIT warrant was void when several district courts have found the very same warrant to be valid.” 13a.

Second, the Ninth Circuit found no evidence that the FBI officers involved in the NIT operation acted in bad faith. 13a. Instead, it held the good faith exception of



*United States v. Leon*, 468 U.S. 897 (1984) applied “because the issuing magistrate’s lack of authority has no impact on police misconduct.” 12a (quoting *Werdene*, 883 F.3d at 216-17) (quotations omitted). It believed “penalizing the officer for the magistrate’s error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations.” 12a (quoting *Horton*, 863 F.3d at 1050) (quotations omitted).

Finally, the Ninth Circuit noted suppressing was “unlikely to deter future violations of this specific kind” because Rule 41 was amended in December 2016, after the NIT operation, to allow a magistrate judge to authorize a search of a computer in another district under certain circumstances. 13a.

As to Mr. Hammond, in an unpublished memorandum, the Ninth Circuit cited to its opinion in *Henderson* and concluded “suppression is not required because the good faith exception to the exclusionary rule applies.” 17a.

### **REASON FOR GRANTING THE WRIT**

The mantra that “ignorance of the law is no excuse” should apply to law enforcement as much as it applies to criminal defendants. *Bryan v. United States*, 524 U.S. 184, 196 (1998). Yet in this case, the Ninth Circuit excused a constitutional error that, based on “historical tradition and recent precedent,” was “obvious.” 10a (quoting *Krueger*, 809 F.3d at 1124 (Gorsuch, J., concurring)). This Court has never decided whether a mistake of constitutional law made by law enforcement when executing a search warrant can trigger the good faith exception to the exclusionary rule. This case presents an ideal vehicle to decide that issue.

A. This Court Has Never Decided Whether a Mistake of Constitutional Law Made by the Government When Executing a Warrant Triggers the Good Faith Exception to the Exclusionary Rule.

This Court has never decided the precise question raised in this petition: whether the good faith exception can excuse an “obvious” mistake of Fourth Amendment law made by law enforcement, such as the one made by DOJ here.

In *Leon*, this Court ruled that searches made in “objectively reasonable reliance” on a warrant later deemed invalid for lack of probable cause were exempt from the exclusionary rule. *See* 468 U.S. at 922. This Court has extended *Leon*’s good faith exception to the exclusionary rule to searches conducted by police in reasonable reliance on (1) a judge advising law enforcement that clerical changes would be made which were not in fact made, *Massachusetts v. Sheppard*, 468 U.S. 981 (1984); (2) a statute later deemed unconstitutional, *Illinois v. Krull*, 480 U.S. 340 (1987); (3) incorrect information in a court’s database indicating a defendant had an outstanding arrest warrant, *Arizona v. Evans*, 514 U.S. 1 (1995); and (4) binding appellate precedent later overruled, *Davis v. United States*, 564 U.S. 229 (2011).

In all of these cases, this Court found there would be no benefit to suppression because the police could not be faulted for the mistake. In *Sheppard*, this Court “refuse[d] to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested.” 468 U.S. at 989-90. In *Krull*, this Court concluded the good faith exception applied because suppressing “will not deter future Fourth Amendment violations by an officer who has simply fulfilled his responsibility to

enforce the statute as written.” 480 U.S. at 350. In *Evans*, the mistake was made by court staff, who “have no stake in the outcome of particular criminal prosecutions,” and so the “threat of exclusion of evidence could not be expected to deter such individuals from failing to inform police officials that a warrant had been quashed.” 514 U.S. at 15. In *Davis*, this Court explained “when binding appellate precedent specifically authorizes a particular police practice, well-trained officers will and should use that tool to fulfill their crime-detection and public-safety responsibilities.” 564 U.S. at 241.

But *Leon* itself noted its “discussion of the deterrent effect of excluding evidence obtained in reasonable reliance on a subsequently invalidated warrant assumes, of course, that the officers properly executed the warrant and searched only those places and for those objects that it was reasonable to believe were covered by the warrant.” 468 U.S. at 918 n. 19. Yet this Court has never examined the contours of whether the good faith exception applies when law enforcement improperly execute a warrant based on a mistake of law and search places for which it would be unreasonable to believe were covered by the warrant.

The Court’s most recent decision concerning mistakes of law and the Fourth Amendment did not resolve this issue. In *Hein v. North Carolina*, 135 S. Ct. 530 (2014), a police officer pulled over a motorist believing his brake lights were not in compliance with state law. 135 S. Ct. at 534-35. A subsequent consent search of the car resulted in the discovery of drugs. *Id.* at 534. The officer was ultimately mistaken about the brake lights, which did in fact comply with state law. *Id.* This Court



nonetheless held that the police officer's reasonable mistake of law could provide the reasonable suspicion necessary to support the traffic stop. *Id.* at 540.

But *Heien* distinguished an officer's mistake of law about whether a defendant's conduct was illegal—which could nonetheless provide reasonable suspicion—with “an officer's mistaken view that the conduct at issue did *not* give rise” to a Fourth Amendment violation. *Id.* at 539 (emphasis in original). This Court noted the mistake of law at issue “relates to the antecedent question of whether it was reasonable for an officer to suspect that the defendant's conduct was illegal. If so, there was no violation of the Fourth Amendment in the first place.” *Id.* at 539; *see also id.* at 541 n. 1 (Kagan, J., concurring) (agreeing with majority but noting “one kind of mistaken legal judgment—an error about the contours of the Fourth Amendment itself—can never support a search or seizure.”).

This case presents the Court with an ideal opportunity to make clear that a mistake of law in the execution of a search warrant does not trigger the good faith exception to the exclusionary rule.

**B. This Case Presents an Ideal Vehicle for Resolving the Issue.**

The extensive and complex NIT operation here, which resulted in the illegal searches of thousands of computers across the country under a universally recognized invalid search warrant, is a good vehicle for this Court to resolve the issue. The overwhelming majority of federal courts have recognized the NIT operation was clearly unconstitutional. The nature of the investigation makes clear that this was not isolated negligence, but a systemic, deliberate and reckless operation.

## 1. The Government Made an “Obvious” Mistake of Law.

It was the government, not the magistrate judge, which made the mistake of constitutional law at issue here. Specifically, FBI agents and the federal prosecutors assisting them failed to comply with not only Rule 41 and the Fourth Amendment, but also Department of Justice (“DOJ”) policy when it only sought a search warrant in the Eastern District of Virginia to search computers outside that district.

Although the NIT warrant dealt with modern technology, its defect was as old as the constitution. The Ninth Circuit recognized the jurisdictional defect in the NIT warrant was in the words of then-Judge Gorsuch an “obvious” mistake of law. 10a (quoting *Krueger*, 809 F.3d at 1123 (Gorsuch, J., concurring)). That is because both “historical tradition and recent precedent” have made clear “a warrant may travel only so far as the power of its issuing official.” 9a (quoting *Krueger*, 809 F.3d at 1124 (Gorsuch, J., concurring)). Unsurprisingly, “every circuit court that has addressed the question has found the NIT warrant violated Rule 41.” 13a; *see also Werdene*, 883 F.3d at 210-14; *Horton*, 863 F.3d at 1047-48.

Critically, law enforcement personnel are presumed to know the policies and guidelines of their own departments, particularly when it comes to obtaining and executing search warrants. *See Groh v. Ramirez*, 540 U.S. 551, 565 (2004). Here, the DOJ’s own policy on searching computers in multiple locations would have made clear the NIT warrant’s flaw. The DOJ’s manual on “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations” (“DOJ Manual”) recognizes the problem with using a warrant issued in one district to seize and search



digital information stored in another district.<sup>2</sup> Addressing the precise issue here, the DOJ's Manual states that, when

data is stored remotely in two or more different places within the United States and its territories, *agents should obtain additional warrants for each location where the data resides to ensure compliance with a strict reading of Rule 41(a)*. For example, if the data is stored in two different districts, agents should obtain separate warrants from the two districts.

*See* DOJ Manual at 84-85 (emphasis added).

This policy directive shows why this mistake of law was committed by the government, not the magistrate judge. The defect in the NIT warrant was its authorization of searches outside of the Eastern District of Virginia. Searches conducted *within* the Eastern District of Virginia under the authority of the NIT warrant were valid. The problem, then, was that the DOJ did not follow its policy—intended to avoid a constitutional violation of Rule 41—to seek NIT warrants in districts *outside* the Eastern District of Virginia. Instead, it chose to rely on the Eastern District of Virginia warrant to deploy the NIT onto “activating” computers... *wherever located*.” 5a (emphasis in original).

The mistake was not in the *issuance* of the NIT warrant, then, but rather in its *execution*. The resulting unconstitutional seizures and searches were thus caused by DOJ when it failed to seek additional NIT warrants for computers outside the Eastern District of Virginia. As explained in *Leon*, the good faith exception “assumes...that the officers properly executed the warrant and searched only those

---

<sup>2</sup> Available at <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>.

places and for those objects that it was reasonable to believe were covered by the warrant.” 468 U.S. at 918 n. 19; *see, e.g., United States v. Potts*, 586 F.3d 823, 833 (10th Cir. 2009) (“proper execution of an invalid warrant is a pre-condition” to *Leon* good faith exception); *United States v. Vasey*, 834 F.3d 782, 789 (9th Cir. 1987) (“The constitutional error was made by the officer in this case, not by the magistrate as in *Leon*” and so good faith exception unavailable). The mistake of law here, then, was caused by the government, not the magistrate judge.

## **2. The Government’s Misconduct Was Systemic, Deliberate and Reckless.**

Because the mistake was made by the officers executing the warrant rather than the magistrate judge who issued it, this case involves the sort of “‘deliberate,’ ‘reckless,’ or ‘grossly negligent’ disregard for Fourth Amendment rights” where “the deterrent value of exclusion is strong and tends to outweigh the resulting costs.” *Davis*, 564 U.S. at 238 (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)); *see also Herring*, 555 U.S. at 147 (good faith exception does not apply to police mistakes demonstrating “systemic error or reckless disregard of constitutional requirements”).

The NIT operation was clearly systemic. It was a complex government investigation that took weeks to plan, involved moving a website across state lines onto a government server, and obtaining Title III wiretap authorization. In fact, it was an international digital dragnet run by the government. The surveillance technology in the NIT deployed purpose-built malware on unknown computers around the world. The calculated use of this invasive new tactic, operating without

geographic limits, underscores why the good faith doctrine should not apply. Comparing the warrant check in *Herring* to an NIT is “like saying a ride on horseback is materially indistinguishable from a flight to the moon.” *Riley v. California*, 573 U.S. 373, 393 (2014). The government’s failure to apply for warrants in other districts—leading to an “obvious” Fourth Amendment violation—amounts to the “systemic negligence” with respect to warrant requirements that *Herring* called out.

Moreover, the government’s conduct was deliberate and reckless. Fourth Amendment reasonableness is a question of collective knowledge. A court must “consider the objective reasonableness, not only of the officers who eventually executed a warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination.” *Herring*, 555 U.S. at 140 (quoting *Leon*, 468 U.S. at 923 n. 24). *Leon* explicitly warned that the government could not obtain a void warrant “and then rely on colleagues who are ignorant of the circumstances under which the warrant was obtained to conduct the search.” 468 U.S. at 923 n. 24.

Law enforcement efforts to police the internet are collaborative endeavors, and the Playpen operation was no different. The FBI devised a strategy with federal prosecutors to take over a child pornography website in order to install malware on any computer that attempted to log into it. From the outset, the plan was to conduct a global investigation that would yield multiple prosecutions by local authorities around the country. Indeed, the FBI touts that, as of May 2017, the operation had “sent more than 1,000 leads” to field offices around the country, yielding “at least”



350 domestic arrests.<sup>3</sup> The government reportedly shared “thousands more” leads with law enforcement authorities abroad.

While the government’s goal of pursuing individuals who harm and exploit children is undeniably laudable, it is the means that justify the end, and not vice versa. Here, the government disregarded “obvious” Fourth Amendment principles known since the founding of the country and ignored its own computer searching policies.

In fact, the DOJ knew it was on shaky legal grounds by relying on one warrant from the Eastern District of Virginia to search computers across the country and the world, but proceeded anyway. When the NIT was deployed, the DOJ was in the midst of seeking an amendment to Rule 41. In 2013, a magistrate judge in the Southern District of Texas issued an opinion rejecting the government’s request for a search warrant remarkably similar to the NIT warrant. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). The government sought a search warrant that would “surreptitiously install data extraction software on the Target Computer;” once installed, the software “has the capacity to search the computer’s hard drive, random access memory, and other storage media; to activate the computer’s built-in camera; to generate latitude and longitude coordinates for the computer’s location; and to transmit the extracted data

---

<sup>3</sup> Fed. Bureau of Investigation, News, ‘Playpen’ Creator Sentenced to 30 Years: Dark Web ‘Hidden Service’ Case Spawned Hundreds of Child Porn Investigations, (May 5, 2017), *available at* <https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years>.

to FBI agents within this district.” *In re Warrant*, 958 F. Supp.2d at 755. The government acknowledged that it did not know the location of the suspects or their computer. The magistrate judge denied the warrant, noting that he had no authority under Rule 41(b) to issue a warrant because it was possible the computer would be outside the Southern District of Texas. *Id.* at 756-58, 761.

Rather than appeal the magistrate judge’s decision, the DOJ instead proposed to amend Rule 41 to allow precisely what it did here. An Amendment to Rule 41 sent to Congress by this Court in April 2016 permitted “a magistrate judge with authority in any district where activities related to a crime may have occurred...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.” This amendment is now codified in Federal Rule of Criminal Procedure 41(b)(6), which went into effect on December 1, 2016.

What is crucial here is that the purpose of this Amendment was to respond specifically to the magistrate judge’s decision in *In re Warrant*. In the Preliminary Draft of the proposed amendment, released August 2014, the Judicial Conference’s Committee on Rules of Practice and Procedure explained that the reason for the proposed Rule change was because

one judge recently concluded that the territorial requirement in Rule 41(b) precluded a warrant for a remote search when the location of the computer was not known, and he suggested that the Committee should consider updating the territorial limitation to accommodate advancements in technology.

Preliminary Draft of August 2014 Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil and Criminal Procedure at p. 325 (citing *In re Warrant*).<sup>4</sup> Public comment on the proposed Rule Amendment was open until February 17, 2015, three days before the government sought the NIT warrant.<sup>5</sup>

Thus, the DOJ itself was fully aware that the territorial and jurisdictional limitations of Rule 41 did not permit the multi-district computer hacking warrant it sought here. Its internal policies advised agents to obtain warrants from multiple districts in identical scenarios. A magistrate judge had rejected a similar warrant request and the DOJ was seeking to amend Rule 41 to expand a magistrate judge's jurisdiction. Nonetheless, the DOJ sought the NIT warrant in only one district, rather than multiple districts, before Rule 41 was amended. The resulting Fourth Amendment violation caused by the government's execution of the warrant, resulted in thousands of Fourth Amendment violations across the country. If this scenario does not warrant application of the exclusionary rule, then no mistake of law made by law enforcement ever will.

Ultimately, reasonable law enforcement officials are expected to know "what is required of them" under the law, particularly the Constitution. *Hudson v. Michigan*, 547 U.S. 586, 599 (2006). That includes understanding the "obvious" jurisdictional and territorial limits of a search warrant. The unique facts surrounding the deployment of the NIT is no excuse; law enforcement "can still be on

---

<sup>4</sup> Available at <https://www.regulations.gov/document?D=USC-RULES-CR-2014-0004-0001>.

<sup>5</sup> See <https://www.regulations.gov/docket?D=USC-RULES-CR-2014-0004>.



notice that their conduct violates established law even in novel factual circumstances.” *Hope v. Pelzer*, 536 U.S. 730, 741 (2002). Otherwise, “in close cases, law enforcement officials would have little incentive to err on the side of constitutional behavior.” *United States v. Johnson*, 457 U.S. 537, 561 (1982).


Suppressing here will deter law enforcement from engaging in searches in violation of the law and its own policy manuals. Suppressing will deter law enforcement from rushing to conduct a search before the law authorizing it has gone into effect. Most importantly, suppressing will ensure law enforcement “can gain no Fourth Amendment advantage through a sloppy study of the laws he is duty-bound to enforce.” *Heien*, 135 S. Ct. at 539-40. This Court should grant *certiorari*.

### CONCLUSION

For the reasons stated above, Mr. Henderson and Mr. Hammond respectfully request this Court issue a writ of *certiorari*.

Dated: April 1, 2019

STEVEN G. KALAR  
Federal Public Defender



---

HANNI M. FAKHOURY  
Assistant Federal Public Defender  
*Counsel of Record*

1301 Clay Street, Suite 1350N  
Oakland, CA 94612  
(510) 637-3500  
hanni\_fakhoury@fd.org