No. __-_____

IN THE

Supreme Court of the United States

HUNTER VAUGHAN EURE,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

PETITION FOR WRIT OF CERTIORARI

GEREMY C. KAMENS
Federal Public Defender

Andrew W. Grindrod
Assistant Federal Public Defender
Counsel of Record
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, VA 23510
(757) 457-0800
Andrew_Grindrod@fd.org

August 15, 2018

QUESTION PRESENTED FOR REVIEW

Under the Fourth Amendment, a warrant must "particularly describ[e] the place to be searched." U.S. Const. amend. IV. In *United States v. Leon*, this Court held that the good-faith exception to the exclusionary rule does not apply when a warrant is "so facially deficient – i.e., in failing to particularize the place to be searched or the things to be seized – that the executing officers cannot reasonably presume it to be valid." 468 U.S. 897, 923 (1984).

Here, the FBI remotely searched thousands of personal computers around the world, including Mr. Eure's. All of these searches were conducted pursuant to a single warrant. The warrant described the "place to be searched" as any computer that, in the future, accessed a certain website. But the warrant failed to describe any particular computer – by user, location, or otherwise. This single warrant authorized the FBI to conduct *a million* searches of 100,000 different computers.

The question presented is:

> Whether an FBI agent can reasonably rely on the validity of a single warrant that authorizes a million searches of 100,000 different computers without describing any particular place to be searched?

PARTIES TO THE PROCEEDINGS

All parties appear in the caption of the case on the cover page.

TABLE OF CONTENTS

INDEX TO APPENDICES

TABLE OF AUTHORITIES

Cases

Constitutional Provision, Statutes, and Rule

Other Authorities

PETITION FOR WRIT OF CERTIORARI

Petitioner Hunter Vaughan Eure respectfully asks this Court to issue a writ of certiorari to review the judgment entered in this case by the United States Court of Appeals for the Fourth Circuit.

OPINIONS BELOW

The decision of the court of appeals is reported at 723 F. App'x 238 (4th Cir. 2018), and appears at Pet. App. 1a.[1] The Fourth Circuit's decision in *Eure* applied the court's earlier decision in *United States v. McLamb*, which addressed an identical challenge to the same warrant based on largely the same record. The Fourth Circuit's *McLamb* decision is reported at 880 F.3d 685 (4th Cir. 2018), and appears at Pet. App. 11a-17a. The unreported decision of the district court, No. 2:16cr43, 2016 WL 4059663 (E.D. Va. July 28, 2016), appears at Pet. App. 2a-10a.

JURISDICTION

The district court in the Eastern District of Virginia had jurisdiction over this federal criminal case pursuant to 18 U.S.C. § 3231. The court of appeals had jurisdiction over Mr. Eure's appeal pursuant to 28 U.S.C. § 1291. That court issued its opinion and judgment on May 25, 2018. Mr. Eure did not seek rehearing.

The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

---

[1] "Pet. App." refers to the appendix attached to this petition. "C.A.J.A." refers to the joint appendix filed in the court of appeals.

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the United States Constitution provides:

> 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.

STATEMENT OF THE CASE

1. Factual Background. In 2015, the FBI seized a server hosting a website called Playpen. Playpen was a forum-style website with many forums related to child pornography. The FBI quickly located and arrested Playpen's administrator. But because Playpen operated on the Tor network,[2] the FBI could not locate Playpen's users through normal investigative techniques. The Department of Justice proposed a radical solution to this problem.

The government applied for a warrant that did not describe any particular place to be searched. Instead, the warrant described a category of places that might be searched: the "computers . . . of any user or administrator who logs into [Playpen]." In other words, the warrant authorized the FBI to hack into and search any computer in the world if it was used to access the website during a 30-day period. This type of warrant is known as a "watering-hole" warrant, a term that "derives from the concept

[2] Tor, which was created by the U.S. Naval Research Laboratory and is now operated by a non-profit primarily funded by the U.S. government, is computer software designed to protect users' privacy online. C.A.J.A. 61-62. Like the regular Internet, Tor can be used to conduct both legal and illegal activity.

of poisoning a watering hole where certain animals are known to drink." Am. Civ. Liberties Union, *et al.*, *Challenging Government Hacking in Criminal Cases*, at 1 (Mar. 2017), *available at* https://bit.ly/2HdTC1X (last accessed Aug. 14, 2018).

The warrant application revealed that Playpen had 158,094 members, and over 11,000 weekly visitors. It therefore was clear that this single warrant would authorize searching the computers of tens of thousands of persons then unknown. It was also clearly an *anticipatory* warrant, i.e., one for which probable cause hinged on a future event. Specifically, the warrant's search authority would be triggered by any computer user navigating through Playpen's homepage. The warrant did not require the user to have visited Playpen before, or to access the site's illicit content located past the homepage.

A federal magistrate judge signed the warrant in the form proposed by the government. Two days later, Petitioner Eure accessed Playpen. The FBI then hacked into his computer, searching for and seizing data from his computer including his MAC address, host name, IP address, operating system username, and the type of operating system he was running. Over the course of two weeks, the FBI conducted thousands of similar searches around the world, many of which became the subject of litigation. *See United States v. Gaver*, No. 3:16-cr-88, 2017 WL 1134814, at *8 (S.D. Ohio Mar. 27, 2017) (collecting Playpen cases).

Because the warrant did not specify a place to be searched, at the time the warrant issued, the scope of search authority was open-ended. But since then, even the government has acknowledged the remarkable breadth of search authority actually

conveyed by this warrant. In a public filing, the government averred that between February 20 and March 4, 2015, approximately 100,000 unique user accounts logged in to Playpen, and there were approximately one million total logins. Every login authorized a new search. But the FBI apparently exercised its discretion to search only about 9,000 computers.

The government used evidence from the watering-hole search of Mr. Eure's computer to obtain a search warrant for his home. In the lower courts, the government did not dispute that all of the evidence against Mr. Eure was fruit of the watering-hole search.

2. Proceedings in the District Court. In the district court, Mr. Eure was charged by indictment with three counts of receiving images of minors engaged in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(2), and one count of possessing the same, in violation of § 2252(a)(4)(B). Mr. Eure challenged the warrant's particularity in a motion to suppress,[3] which was denied by the district court. Pet. App. 2a.

After the district court denied the suppression motion, Mr. Eure entered a conditional guilty plea to a single count of possessing child pornography and was sentenced to 24 months in prison. The remaining counts of the indictment were dismissed.

3. Proceedings in the Court of Appeals. Pursuant to his conditional plea agreement, Mr. Eure appealed several suppression issues to the Fourth Circuit. Mr.

---

[3] Mr. Eure filed two motions to suppress raising numerous challenges to the warrant, but this petition seeks review only of the particularity and related good-faith issues.

Eure's appeal was held in abeyance pending the Fourth Circuit's decision in *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018), a case that raised identical issues on a nearly identical record. In *McLamb*, the Fourth Circuit held: "Even if the warrant is unconstitutional, the district court properly denied [Mr. McLamb's] motion to suppress because the *Leon* good faith exception applies." 880 F.3d at 688. The Fourth Circuit specifically held that the warrant in *McLamb* was not "so 'facially deficient . . . that the executing officers [could not] reasonably presume it to be valid.'" *Id.* at 691 (quoting *Leon*, 468 U.S. at 923 (alterations in *McLamb*)). But the Fourth Circuit did not elaborate on how a warrant that failed to identify any particular place to be searched could be anything other than facially deficient.

The *Eure* panel wrote that, in *McLamb*, the Fourth Circuit had "addressed a substantially similar challenge to the same warrant at issue here and concluded that, even if the warrant was unconstitutional, the good faith exception precluded suppression of the evidence." Pet. App. 1a. Because *McLamb* and *Eure* raised identical legal questions based on identical facts, the decision in *McLamb* was binding on the *Eure* panel. The Fourth Circuit affirmed the denial of Mr. Eure's suppression motion.

REASONS FOR GRANTING THE PETITION

This Court should grant review to decide whether anticipatory watering-hole warrants that fail to identify any particular place to be searched are so lacking in particularity as to be facially deficient.[4]

I. This case presents the Court with the opportunity to consider *Leon*'s paradigmatic example of facial deficiency based on a warrant's failure to particularize the place to be searched.

In *United States v. Leon*, this Court announced the paradigmatic circumstance in which the good-faith exception to the exclusionary rule does not apply: When a warrant is "so facially deficient – i.e., in failing to particularize the place to be searched or the things to be seized – that the executing officers cannot reasonably presume it to be valid." 468 U.S. 897, 923 (1984). Since *Leon*, however, this Court has addressed facial deficiency only in the context of a warrant that failed to identify the things to be seized. *See Groh v. Ramirez*, 540 U.S. 551, 558-63 (2004) (finding facial deficiency in warrant that "did not describe the items to be seized at *all*"). Here, Mr. Eure challenged the warrant's failure to describe the place to be searched.

"The manifest purpose of this particularity requirement was to prevent general searches." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Indeed, the particularity requirement was born of the Framers' own experience living under a government that possessed roving search authority. "The hated writs of assistance had given customs

---

[4] Nearly identical petitions for certiorari are pending in *McLamb v. United States*, No. 17-9341, and *United States v. Darby*, No. 18-5508. Another petition challenging the same warrant is pending in *Werdene v. United States*, No. 18-5368. Should the petitions in *McLamb*, *Werdene*, or *Darby* be granted, Mr. Eure's case should be held or consolidated with those cases for disposition.

officials blanket authority to search where they pleased for goods imported in violation of the British tax laws." *Stanford v. Texas*, 379 U.S. 476, 481 (1965). And in England, "officers of the Crown" had been "given roving commissions to search where they pleased in order to suppress and destroy the literature of dissent." *Id.* at 482. As this Court has observed, the "principal evil of the general warrant was addressed by the Fourth Amendment's particularity requirement." *Ashcroft v. al-Kidd*, 563 U.S. 731, 742-43 (2011).

The text of the Fourth Amendment's Warrant Clause is "precise and clear." *Stanford*, 379 U.S. at 481. "The Fourth Amendment by its terms requires particularity *in the warrant*, not in the supporting documents." *Groh*, 540 U.S. at 557 (emphasis added). The clarity of the constitutional text, the inevitability that particularity defects will appear on a warrant's face, and the importance of particularity to protecting against the principal evil of the general warrant led this Court to single out particularity defects as likely candidates for suppression. *Leon*, 468 U.S. at 923. A warrant that fails "to particularize the place to be searched" is so facially deficient that "the executing officers cannot reasonably presume it to be valid," so the good-faith exception to the exclusionary rule does not apply. *Id.*

Over thirty years have passed since the Court identified this paradigmatic example of facial deficiency, yet this Court has never had occasion to apply *Leon*'s rule to a warrant that failed to identify the place to be searched. In *Groh*, the Court analyzed a warrant that "did not describe the items to be seized at *all*," and found the warrant facially deficient. 540 U.S. at 558. But describing the "place to be searched"

is at least as important as describing the items to be seized. Restricting *where* an officer may search protects the people from roving government invasions. *Cf.* Orin S. Kerr, *An Economic Understanding of Search and Seizure Law*, 164 U. Pa. L. Rev. 591, 619 (2016) (observing that, under the particularity requirement, "the government can typically search only one home at a time"). The Fourth Amendment fought off the "principal evil of the general warrant" by requiring a limit on the geographic scope of search authority to appear on the face of every warrant. *See al-Kidd*, 563 U.S. at 742. This Court's cases demonstrate the importance of the Fourth Amendment's requirement that a warrant identify the particular place to be searched. But the Court has not yet had occasion to say when a warrant's failure to do so renders it facially invalid.

This Court's recent decisions applying the exclusionary rule have emphasized the relationship between the availability of this remedy and its purpose of deterring government misconduct. *See, e.g.*, *Davis v. United States*, 564 U.S. 229, 231, (2011); *Herring v. United States*, 555 U.S. 135, 141 (2009); *Hudson v. Michigan*, 547 U.S. 586, 594 (2006). Granting this petition would give the Court an opportunity to clarify that principle by reference to *Leon*'s paradigmatic example. When, as here, a warrant so clearly fails to comply with plain text of the Fourth Amendment, which explicitly requires a warrant to describe with particularity the place to be searched, no reasonable officer can rely on that warrant in good faith.

II. The use of anticipatory watering-hole warrants to remotely search electronic devices is an issue of national importance.

The constitutionality of watering-hole warrants is an issue of national importance that this Court should not wait to address. First, watering-hole warrants make an end run around the limitation on anticipatory warrants this Court announced twelve years ago in *United States v. Grubbs*, 547 U.S. 90 (2006). Every watering-hole warrant is an anticipatory warrant to search literally any computer in the world. Second, because watering-hole warrants authorize mass government hacking, a single warrant threatens the privacy of thousands of people. Third, although watering-hole warrants have been used sparingly in the past, their use is likely to increase dramatically with recent changes to Federal Rule of Criminal Procedure 41.

A. Police use watering-hole warrants as an end run around *Grubbs*'s probable-cause requirement for anticipatory warrants.

In *Grubbs*, this Court clarified the probable-cause requirement for anticipatory warrants that place a condition (other than the mere passage of time) upon their execution. 547 U.S. at 96. In those circumstances, the probable-cause requirement "looks [ ] to the likelihood that the condition will occur." *Id.* Without that requirement, "an anticipatory warrant could be issued for every house in the country, authorizing search and seizure if contraband should be delivered – though for any single location there is no likelihood that contraband will be delivered." *Id.*

Watering-hole warrants make an end run around *Grubbs*'s probable-cause requirement. They authorize police to search the contents of *any* computer in the world if the computer is used to access a given website. Search authority is triggered

by a computer accessing the website. So the government demonstrates probable cause to believe the triggering condition will occur by showing that *some* (unidentified) computer is likely to enter the website. But that probable-cause showing depends entirely on the warrant's failure to identify any particular place to be searched. A watering-hole warrant is, in effect, an anticipatory warrant for every computer in the world.

Watering-hole warrants avoid a probable-cause deficiency only by substituting a particularity problem. But the Fourth Amendment requires both probable cause *and* particularity. With anticipatory warrants, either deficiency results in the expansive search authority this Court warned against in *Grubbs*. The Court should take this case to stop law enforcement's creative attempts to skirt the rule recognized in *Grubbs*.

B. One watering-hole warrant impacts the rights of thousands of people to be secure in their houses, papers, and effects.

A watering-hole warrant authorizes the search of an uncapped number of electronic devices. At the time the warrant issues, both the number of searches and the number of different locations that could be searched are limitless. The facts of this case demonstrate the breadth of the privacy interests affected by a single warrant.

Here, a single warrant signed by a U.S. Magistrate Judge in the Eastern District of Virginia authorized the FBI to search the computer of any person who navigated to a certain website. The government has acknowledged that this warrant eventually authorized the FBI to conduct a million searches involving 100,000 unique users. The FBI apparently exercised its discretion to search only about 9,000 computers. *See*

Order on Defendants' Motion to Dismiss, at 5, *United States v. Tippens*, No. 16-cr-5110 (W.D. Wash. Nov. 30, 2016) (ECF No. 106).

Were Mr. Eure challenging a technological tool used by law enforcement to conduct individualized searches in a new way, perhaps this Court could allow questions over the legality of this technology to percolate further in the lower courts. But Mr. Eure is not challenging a new *technology*. Rather, he challenges a new kind of *warrant*. And watering-hole warrants do not merely represent a new move by prosecutors and law enforcement; they represent a change in the game. With a watering-hole warrant, one magistrate authorizes a mass government hacking operation in which – without having identified a single place to be searched – the government searches thousands of people's personal computers.[5]

The warrant challenged here implicated the rights of 100,000 people to be secure in their houses, papers, and effects. So will the next. This Court should not wait to address the constitutionality of watering-hole warrants that authorize mass government hacking.

[5] Mr. Eure is not alone in asserting the importance of this issue. The broad impact of the development of the law in this area was also recognized by the Electronic Frontier Foundation, Privacy International, and the National Association for Criminal Defense Lawyers, who supported Mr. Eure's position as amici in the Fourth Circuit.

C. The use of watering-hole warrants is likely to surge after recent changes to Federal Rule of Criminal Procedure 41.

The federal government has used watering-hole warrants at least twice before.[6] But in 2013, a federal magistrate judge in Texas denied a warrant application that sought authority "to hack a computer" by "surreptitiously installing software designed . . . to extract certain stored electronic records." *In re Warrant*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013). The court ruled that the warrant application did not satisfy the "territorial limits on a magistrate judge's authority to issue a warrant" set out in Federal Rule of Criminal Procedure 41(b). *Id.* at 756.

This 2013 decision chilled the widespread use of watering-hole warrants, since they were seen as being of questionable legality under Rule 41. The Department of Justice, however, lobbied for changes to Rule 41 that would eliminate the territoriality problem highlighted by the Texas decision.[7] These efforts were successful and changes to Rule 41 went into effect on December 1, 2016. *See* Fed. R. Crim. P. 41(b)(6) (2016).

---

[6] *See e.g.*, *In the Matter of the Search of Computers that Access "Websites 1-23"*, No. 8:13-mj-1744, ECF Nos. 23-25 (D. Md. July 22, 2013) (watering-hole warrant to remotely search computers used to access any one of 23 different websites); *In the Matter of the Search of computers that access the website "Bulletin Board A" located at http://jkpos24pl2r3urlw.onion*, No. 8:12-mj-356 (D. Neb. Nov. 16, 2012) (watering-hole warrant to remotely search computers used to access website).

[7] Letter from Mythili Raman, Acting Asst. Attorney Gen. to Hon. Reena Raggi, Chair, Advisory Committee on Crim. R., 2 (Sept. 18, 2013) (asking Committee "to update the provisions [of Rule 41] relating to the territorial limits for searches" to allow searches via "remote access"), *available at* https://bit.ly/2kJSkTx (last accessed Aug. 14, 2018); Memorandum from David Bitkower, Deputy Asst. Attorney Gen. to Hon. Reena Raggi, Chair, Advisory Committee on Crim. R., 6-7 (Dec. 22, 2014) (asking for Rule 41 to be changed to allow for watering-hole warrants), *available at* https://bit.ly/2sC8qlq (last accessed Aug. 14, 2018).

The addition of Rule 41(b)(6), which now provides a federal venue for watering-hole warrants, "has opened the courthouse door . . . to applications seeking these warrants." Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 Duke L. & Tech. Rev. 161, 183 (2018). The impending surge in the use of watering-hole warrants makes now the time for this Court to act. Mr. Eure's case presents this Court with an excellent opportunity to announce that law enforcement hacking operations must comply with the Fourth Amendment's particularity requirement, and that warrants entirely lacking in particularity will not be saved by the good-faith exception.

III. Establishing the facial invalidity of watering-hole warrants on particularity grounds now will eliminate the need to address thornier extraterritoriality concerns later.

Because watering-hole warrants authorize the search of any computer that enters a website – and because law enforcement does not know the location of the computer it is searching until after the search is complete – these warrants allow U.S. law enforcement to hack into and search computers located anywhere in the world. The extraterritorial reach of U.S. law enforcement operations in the digital age can present thorny questions of international law and can impact foreign relations. *Cf. United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (finding question over U.S. law enforcement's use of § 2703 warrant to obtain emails stored in foreign country mooted by CLOUD Act).

The implications of watering-hole operations for foreign relations and international law have received attention from the legal academy. *See, e.g.*, Ahmed

Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1135-36 (2017) (arguing that law enforcement hacking techniques amount to "overseas cyberexfiltration operations that may violate the sovereignty of other nations," and describing associated risks as "enormous: disability of U.S. foreign relations, exposure of the United States and its citizens to countermeasures, and exposure of the investigators performing overseas searches and seizures to prosecution by foreign nations"); *see also* Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 Stan. L. Rev. Online 58, 60 (2017) (agreeing that extraterritoriality of watering-hole warrants can offend other nations and violate international law but disagreeing over extent of the problem); John Douglass, Note, *The Legality of Watering-Hole-Based NITs under International Law*, 2 Geo. L. Tech. Rev. 67 (2017).

As explained more fully in Privacy International's amicus brief in the court of appeals, the foreign relations and international law concerns implicated by watering-hole warrants are real. But those problems stem directly from these warrants' failure to identify with particularity the place to be searched. If this Court holds that watering-hole warrants violate the Fourth Amendment's particularity requirement, lower courts will not have to grapple with more nebulous questions of international law or judge the impact of such warrants on foreign relations. This Court can end that debate before it begins by resolving this case based on the plain text of the

Fourth Amendment. This is yet another reason for the Court to grant certiorari now on the straightforward question presented by this petition.

IV. This case is the ideal vehicle to consider the facial invalidity of watering-hole warrants.

Mr. Eure challenges the facial sufficiency of a watering-hole warrant's description of the place to be searched. Therefore, the question presented can be answered based on the face of the warrant. *See Groh*, 540 U.S. at 557 ("The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents."). Mr. Eure raised this objection in the district court. C.A.J.A. 39-44, 144-50. He raised this issue again in the court of appeals, and the government did not argue that any waiver or standing issues should have prevented that court from reaching the merits. The issue is preserved and cleanly presented.

The scope of search authority the government obtained under this warrant was largely undisputed. The parties agreed below that the warrant described the place to be searched as the "computers . . . of any user or administrator who logs into [Playpen] by entering a username and password." C.A.J.A. 145. It was undisputed, therefore, that the warrant authorized an uncapped number of searches of an unlimited number of unspecified computers. Any computer that accessed the Playpen website during a 30-day window could be searched pursuant to this warrant.

It is also undisputed that this single warrant ended up authorizing the government to conduct about one million searches of about 100,000 different computers. In fact, those figures come from a government filing in a related case, which asserted that between February 20 and March 4, 2015, approximately 100,000

unique user accounts logged in to Playpen, and there were approximately one million total logins.

To be sure, the decision in *Eure* merely adopted the decision in *McLamb*. And the Fourth Circuit's opinion in *McLamb* assumed without deciding that the warrant violated the Fourth Amendment, skipping directly to the good-faith inquiry. In the context of particularity, however, the good-faith inquiry is wrapped up in the substantive constitutional question. In other contexts, the substantive Fourth Amendment issue can be largely divorced from deciding the question whether the executing officer was entitled to rely on the warrant in good faith. For example, when a deficiency in the application renders a warrant invalid, the good-faith issue turns on a separate inquiry into whether police intentionally or recklessly misled the magistrate. *See Franks v. Delaware*, 438 U.S. 154, 168 (1978). By contrast, Mr. Eure acknowledges that suppression is required here only if the warrant's particularity defect rendered it so facially deficient that the executing officer could not reasonably presume it to be valid. The substantive particularity question and the good-faith analysis thus involve the same fundamental inquiry. Accordingly, the Fourth Circuit's choice to assume a constitutional violation (rather than affirmatively finding one) is of no consequence to the quality of this case as a vehicle for deciding the good-faith question.

In the court of appeals, Mr. Eure raised a number of other issues related to the magistrate's authority to issue the Playpen warrant. This Court has since denied two petitions raising those issues. *See United States v. Workman*, 863 F.3d 1313 (10th Cir.

2017), *cert. denied*, 138 S. Ct. 1546 (2018); *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018). But those issues are not raised here. The only question raised in this petition is Mr. Eure's challenge to the warrant's lack of particularity. This issue was preserved below and no procedural issues will prevent this Court from reaching the merits. All facts relevant to this question were either undisputed below or affirmatively provided by the government.

In sum, the outcome of this case hinges on a clear question of law: Can an FBI agent reasonably rely on the validity of a warrant that authorizes a million searches of 100,000 different computers without describing any particular place to be searched?

CONCLUSION

For the reasons given above, the petition for a writ of certiorari should be granted. In the alternative, should the Court grant any of the petitions presently pending in *McLamb v. United States*, No. 17-9341, *Werdene v. United States*, No. 18-5368, or *Darby v. United States*, No. 18-5508, this case should be held for or consolidated with those cases for disposition. *See supra* page 6, n.4.

Respectfully submitted,

GEREMY C. KAMENS
Federal Public Defender
for the Eastern District of Virginia

Andrew W. Grindrod (by FHE)
Andrew W. Grindrod
Assistant Federal Public Defender
Counsel of Record
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, VA 23510
(757) 457-0800
Andew_Grindrod@fd.org

August 15, 2018