No._____

IN THE SUPREME COURT OF THE UNITED STATES

GABRIEL WERDENE,
PETITIONER,

- VS. -

UNITED STATES OF AMERICA,
RESPONDENT.

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

BRETT G. SWEITZER
Assistant Federal Defender
Chief of Appeals
Counsel of Record

LEIGH M. SKIPPER
Chief Federal Defender

FEDERAL COMMUNITY DEFENDER OFFICE
FOR THE EASTERN DISTRICT OF PENNSYLVANIA
Suite 540 West - Curtis Center
601 Walnut Street
Philadelphia, PA 19106
(215) 928-1100

Counsel for Petitioner

QUESTIONS PRESENTED

The government sought, and received from a U.S. Magistrate Judge sitting in the Eastern District of Virginia, a warrant permitting it to search—at its discretion—any computer throughout the world that accessed a server under government control in that district. The Third Circuit held the warrant invalid under the Fourth Amendment and Federal Rule of Criminal Procedure 41(b), but declined to order suppression of the resulting evidence based on a determination that government agents acted in good faith.

The questions presented are:

I. Whether the good-faith exception to the exclusionary rule applies when a warrant is void from the outset due to the issuing authority's lack of jurisdiction.

II. Assuming the good-faith exception applies, whether under the circumstances of this case it was objectively reasonable for government agents to rely on a warrant purporting to authorize discretionary searches of tens of thousands of unspecified computers throughout the world.

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

FEDERAL CASES **PAGE(S)**

TABLE OF AUTHORITIES – continued

PAGE(S)

FEDERAL STATUTES **PAGE(S)**

OTHER **PAGE(S)**

No. _____

IN THE SUPREME COURT OF THE UNITED STATES

GABRIEL WERDENE,
PETITIONER

– VS. –

UNITED STATES OF AMERICA,
RESPONDENT.

PETITION FOR A WRIT OF CERTIORARI

Petitioner Gabriel Werdene respectfully requests that a writ of certiorari issue to review the judgment of the United States Court of Appeals for the Third Circuit entered in this case on February 21, 2018.

OPINION BELOW

The precedential opinion of the court of appeals affirming the district court's judgment is published at 883 F.3d 204, and is attached as Appendix A.

JURISDICTION

The district court had jurisdiction over this federal criminal case pursuant to 18 U.S.C. § 3231, and the court of appeals had jurisdiction under 28 U.S.C. § 1291. This petition is timely filed pursuant to Rule 13.1 and the granting of petitioner's applications for an extension of time, docketed at No. 17A1243. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS 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.

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

(b) Authority to Issue Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge —in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside the district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside of the jurisdiction of any state or district, but within [certain enumerated locales].

Fed. R. Crim. P. 41(b) (2015).

STATEMENT OF THE CASE

This case is about a highly unorthodox criminal investigation. In late 2014, the Federal Bureau of Investigation became aware of a large child-pornography website, called Playpen, and quickly seized its computer server and arrested its operator. Playpen and the people accessing it utilized widely-available privacy software, called Tor (formerly known as "The Onion Router"), which made it difficult for the FBI to identify Playpen's users. Rather than immediately shutting Playpen down and prosecuting its operator, the FBI decided to operate the website itself while trying to actively identify its users. To that end, the FBI obtained a warrant from a United States Magistrate Judge in the Eastern District of Virginia authorizing it to remotely install software on every computer in the world that accessed the website, to search those computers for certain identifying information, and to seize that information and electronically send it back to a government-controlled server.

Mr. Werdene's computer in the Eastern District of Pennsylvania was one of the approximately 9,000 computers searched pursuant to the warrant. The district court declined to suppress evidence derived from the search in Mr. Werdene's subsequent prosecution, holding that a non-constitutional violation of Federal Rule of Criminal Procedure 41(b) had occurred and that government agents acted in good faith. The Third Circuit affirmed on good-faith grounds, but not before holding the warrant invalid under both the Fourth Amendment and Rule 41(b).

1. Tor is a method of using the internet that preserves privacy and anonymity, developed by the U.S. Naval Research Laboratory and now run by a nonprofit foundation. Tor, in effect, conceals internet protocol ("IP") addresses—the unique identifier assigned by an internet service provider to each computer having access to the internet, including computer servers that host websites. Often, a computer's IP address is logged by the websites the

computer user visits (creating a digital record of activity on each website), and a computer server's IP address is indexed so that websites hosted on the server can be located by search engines such as Google.

Tor scrambles this process, allowing users to visit websites without revealing their computer's true IP address. To accomplish this, a user runs a Tor-based web browser, which connects to websites not directly, but through other computers running the Tor software, called "relay nodes." Thus, numerous intermediary computers stand between the accessing computer and the website, and the website can log the IP address of only the final computer in the sequence, the "exit node." Because the exit node is random and the path through the relay nodes is difficult to trace, a Tor user's IP address is, in effect, concealed—even though the address is revealed to the first "node" in the sequence.

Computer servers can be configured to host websites accessible only through Tor. The Tor software creates unique, algorithmically generated URLs that cannot be located by conventional search engines. Users navigate to a Tor website by directly entering the URL into their browser, and they obtain the URL through means other than a search engine. As with Tor users, Tor websites run the gamut of topics—lawful and illicit—people wish to keep private. Due to their closely-held nature, Tor websites are known as "hidden services" (or collectively, the "dark web").

2. In January 2015, the FBI seized a server in North Carolina hosting a child-pornography website. The server was moved to a government facility in the Eastern District of Virginia, and a Title III wiretap order was obtained to permit the FBI to monitor communications on it. The server contained a message-board style website called "Playpen," which was dedicated primarily to child pornography. A review of the website revealed that Playpen had

over 150,000 registered users, 95,000 user posts, and many images and videos depicting child pornography. Users were required to create an account with a username and password, which were then entered each time the user visited the website.

Playpen operated through Tor, but with the server in hand the FBI was able to assume administrative control of website. Rather than immediately shut it down, the government let Playpen continue to operate while it tried to circumvent Tor in order to identify the website's users. The FBI determined that it might be able to identify Playpen's users by installing specialized software on the Playpen website, which would be able to retrieve information about accessing computers. When a user logged into Playpen, the government software would secretly send computer code to the accessing computer back through the Tor intermediary computers. Once on the accessing computer, the code would locate certain identifying information on that computer, and secretly transmit the information back to the government. The government refers to this as a "network investigative technique" (or "NIT"), but it is more commonly known by its real-world names—malware, or hacking.

3. The government obtained a search warrant to deploy its NIT from a U.S. Magistrate Judge in the Eastern District of Virginia. The warrant ambiguously describes the location of the property to be searched—the preprinted warrant form says the property to be searched is located in the Eastern District of Virginia, and an "Attachment A" (referenced on the warrant form and entitled "Place to be Searched") says the NIT is to be deployed in the Eastern District of Virginia and will "obtain[] information [specified by the warrant]" from "activating computers." "Activating computer" is defined as the computer of "any user or administrator who logs into [Playpen] by entering a username and password." Attachment A says nothing explicit about the location(s) of the activating computers. An affidavit submitted in support of

the warrant application states that the NIT will be "deployed" on the Playpen website in the Eastern District of Virginia, and in only one place—on page 29 of 31—hints that the accessing computers may be located outside the Eastern District of Virginia: "the NIT may cause an activating computer—wherever located—to send [identifying information]."

Although the affidavit sought authority to use the NIT to send computer instructions to every accessing computer, it stated that in executing the warrant the FBI may, in its discretion, limit use of the NIT to only some Playpen users, "such as those who have attained a higher status on [Playpen] by engaging in substantial posting activity, or in particular areas of [Playpen], such as [Playpen's] sub-forums [containing the most egregious examples of child pornography and/or dedicated to retellings of real world hands on sexual abuse of children]."[1]

4. The government knew that a NIT warrant's validity was dubious, at best. Six years earlier, in 2009, the Department of Justice's Computer Crime and Intellectual Property Section alerted U.S. Attorney's Offices of a Rule 41 "problem[]" with NIT warrants, and recommended seeking an individual warrant in each district in which computers to be searched may be located (rather than a single NIT warrant).[2] And two years before seeking the NIT warrant here, a different U.S. Magistrate Judge denied a government application for a similar

---

[1] The FBI apparently exercised this discretion, as it identified IP addresses for only approximately 6% of Playpen's users (8,700 of 150,000 registered users). *See* Order on Defendants' Motion to Dismiss, at 5, *United States v. Tippens*, No. 16-cr-5110 (W.D. Wash. Nov. 30, 2016).

[2] *See* U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (3d ed. 2009), at 84-85 ("Search and Seizure Manual") (available at https://www.justice.gov/sites/default/ files/ criminal-ccips/legacy/ 2015/01/14/ ssmanual2009.pdf).

warrant on the ground that it would be invalid under Rule 41(b). *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). That prompted the Department of Justice—at the very same time it was procuring the NIT warrant here—to seek an amendment to Rule 41 to authorize such warrants. *See* Proceedings of Advisory Committee on Criminal Rules (Oct. 18, 2013), at 159-63 (available at http://www.uscourts.gov /sites/default/ files/fr_import/CR2013-10.pdf). Those efforts culminated in new Rule 41(b)(6), which purports to authorize NIT warrants but did not become effective until December 1, 2016—almost two years *after* the warrant was procured here.

5. Analysis of the NIT data revealed the IP address of a Playpen user, eventually identified as Mr. Werdene, residing in Bensalem, Pennsylvania. Based on the NIT information and further investigation, the FBI obtained a search warrant for Mr. Werdene's home. The warrant was executed on June 17, 2015, and the FBI seized one USB drive and one DVD containing child pornography. Mr. Werdene's is one of at least 70 prosecutions across the country arising from execution of the NIT warrant.

6. Mr. Werdene moved to suppress the fruits of the computer search, including the information revealed by the NIT and evidence subsequently seized from his home. He argued that the warrant was issued in violation of the jurisdictional and particularity requirements set forth in Federal Rule of Criminal Procedure 41, and that suppression is required because the violations are constitutional in nature and the good-faith exception to the exclusionary rule does not apply.

The district court denied the suppression motion, holding that while the magistrate judge in the Eastern District of Virginia lacked authority to issue the NIT warrant, that represents a technical violation of Rule 41(b) for which suppression is inappropriate. The court also

concluded that, even if the violation were of constitutional dimension, government agents acted in good faith.

7. The Third Circuit ultimately affirmed on good-faith grounds, but first held the NIT warrant invalid under both Rule 41(b) and the Fourth Amendment. As to the rule, the court of appeals rejected the government's only argument—that the NIT was a "tracking device" within the meaning of Rule 41(b)(4)—because the NIT did not operate as a tracking device and was not authorized by a tracking warrant. App. A at 12-16. As to the Constitution, the court concluded that the search of Mr. Werdene's computer was warrantless, in violation of the Fourth Amendment, insofar as the NIT warrant was void from the outset due to the magistrate judge's lack of jurisdiction to issue it. App. A at 11-12, 16-21. On the latter point, the court relied heavily on then-Judge Gorsuch's concurring opinion in *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), which detailed Rule 41(b)'s derivation from the Federal Magistrates Act (28 U.S.C. § 636(a)) and the Founding-era treatment of warrants exceeding an issuing authority's territorial jurisdiction. *Id.* The court declined to reach the merits of Mr. Werdene's argument that the NIT warrant failed to particularly describe the places to be searched. *Id.* at 16 n.6.

The court of appeals rejected both of Mr. Werdene's arguments against application of the good-faith exception to the exclusionary rule: that the exception does not apply where the warrant relied upon was void from the outset due to the issuing authority's lack of jurisdiction, and that, regardless, it was objectively unreasonable in the circumstances of this case for government agents to rely on a warrant that purported to authorize discretionary searches of tens of thousands of unspecified computers throughout the world.

REASONS FOR GRANTING THE PETITION

This Court has recently addressed several important issues at the intersection of the Fourth Amendment and modern digital life: GPS tracking, cell phone searching, and cell-site location information gathering. *See United States v. Jones*, 565 U.S. 400 (2012); *Riley v. California*, 134 S. Ct. 2473 (2014); *Carpenter v. United States*, __ S. Ct. __, 2018 WL 3073916 (Jun. 22, 2018). NIT warrants present one of the most important of these issues, given their unprecedented scope—they authorize deployment of malware to search a limitless number of unspecified computers throughout the world.

The government sought the NIT warrant in this case from a magistrate judge plainly lacking jurisdiction to issue it, and in clear disregard of the Constitution's particularity requirement, Federal Rule of Procedure 41(b), extant case law, and Department of Justice guidelines. Certiorari should be granted to address the open question of whether the good-faith exception to the exclusionary rule even applies in this context, and if so, whether suppression is appropriate given the warrant's obvious defects and the circumstances of its procurement. This case is an appropriate vehicle for resolving those questions, as the issues are fully preserved and the court of appeals ruled the NIT warrant invalid under both the Fourth Amendment and Rule 41(b).[3]

[3] The Court has denied certiorari in two Playpen cases, *Horton v. United States*, No. 17-6910 (cert. denied Apr. 2, 2018) and *Workman v. United States*, No. 17-7042 (cert. denied Apr. 16, 2018), and a certiorari petition is pending in a third, *McLamb v. United States*, No. 17-4299 (distributed for conference of Sept. 24, 2018). *McLamb* challenges good faith reliance only insofar as the NIT warrant failed to particularize the place to be searched, whereas the instant petition raises that issue as well as the good-faith implications of the magistrate judge's lack of jurisdiction and the circumstances of the warrant's procurement. Should certiorari be granted in

continued…

A. This case presents important issues affecting a large number of present and future cases.

As evidenced by the Court's docket in recent Terms, the Fourth Amendment implications of modern technology are critically important. NIT warrants present a most extreme example. Unlike the GPS tracker in *Jones*, the cell phone search in *Riley*, and the cell-site location information gathering in *Carpenter*, a NIT warrant is an astonishingly blunt tool: it authorizes the government to hack into a limitless number of unspecified computers throughout the world. And while Mr. Werdene's case gives the Court the opportunity to rule on the constitutionality of such warrants, it also permits the Court—through the good-faith lens—to establish a benchmark for how the government must comport itself when faced with new technological capabilities.

These important issues affect a large number of present and future cases. The Playpen investigation alone involves at least seventy prosecutions across the country, each of which turns on the validity of the same NIT warrant and the good faith, or lack thereof, of the same government agents. And the use of NIT warrants is set to explode, as the government has successfully advocated for an amendment to Rule 41(b) to authorize their issuance. *See* Fed. R. Crim. P. 41(b)(6) (2016).[4] Contrary to the government's contention in other Playpen cases, *see*

McLamb, Mr. Werdene's case should either be held or consolidated with that case for disposition.

[4] *See* 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; 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 NIT warrants), available at https://bit.ly/2kT6NMW.

Briefs for the United States in Opposition in Nos. 17-6910 and 17-7042, the amendment of Rule 41(b) does not moot the questions presented going forward and therefore does not weigh against the granting of certiorari. First of all, the amendment itself is of doubtful validity: it purports to expand jurisdiction under the Federal Magistrates Act without Congressional authorization to do so. *See, e.g.*, *Kontrick v. Ryan*, 540 U.S. 443, 453 (2004) ("[I]t is axiomatic that [rules promulgated under the Rules Enabling Act] do not create or withdraw federal jurisdiction.").[5] But regardless of the amendment's validity, the good-faith issue turns not on whether this specific violation of Rule 41(b) needs to be deterred in the future, but on whether the government's deliberate disregard of constitutional and procedural rules in general ought to be deterred.

B. The court of appeals incorrectly extended the good-faith exception to the exclusionary rule to warrants void from the outset due to the issuing authority's lack of jurisdiction.

This Court has never considered whether the good-faith exception to the exclusionary rule applies when a warrant is void from the outset due to the issuing authority's lack of jurisdiction. There are very good reasons why the exception should not apply, as briefly outlined below, and the Court should resolve this important open question.

The common theme in all of the Court's good-faith cases is that police reasonably relied on some positive law that appropriately issued, even though it was later invalidated. Whether that be a warrant (as in *United States v. Leon*, 468 U.S. 897 (1984), *Arizona v. Evans*, 514 U.S. 1 (1995), and *Herring v. United States*, 555 U.S. 135, 145 (2009)); a statute (as in *Illinois v. Krull*,

[5] Under Article III, § 1 of the Constitution, "[o]nly Congress may determine a lower federal court's subject matter jurisdiction." *Id.* at 452. *See also Willy v. Coastal Corp.*, 503 U.S. 131, 135 (1992); *Owen Equip. & Erection Co. v. Kroger*, 437 U.S. 365, 370 (1978); *Snyder v. Harris*, 394 U.S. 332, 337 (1969); *Sibbach v. Wilson & Co.*, 312 U.S. 1, 10 & n.9 (1941).

480 U.S. 340, 356 (1987)); or binding case law (as in *Davis v. United States*, 564 U.S. 229 (2011), the authority relied upon indisputably *had the force of law when issued*. Officers' reliance might be reasonable or unreasonable (which will determine the appropriateness of suppression), but in every instance there is reliance on something the law recognized at the time of issuance.

The situation is different when a warrant is void from the outset due to the issuing authority's lack of jurisdiction. "All proceedings of a court beyond its jurisdiction are void"—they are nothing in the eyes of the law. *Ex parte Watkins*, 28 U.S. 193, 197 (1830). *See also* 11 Wright & Miller, Federal Practice and Procedure § 2862. Although parties normally must obey even objectionable court orders, an order issued without jurisdiction "may be violated with impunity," because it is "a nullity." *In re Novak*, 932 F.2d 1397, 1401 (11th Cir. 1991) (citing *In re Green*, 369 U.S. 689 (1962)). And courts must enforce other courts' erroneous judgments, except where the original court lacked jurisdiction, in which case its judgment is void. *See, e.g.*, *Underwriters Nat'l Assur. Co. v. N.C. Life and Acc. Health Ins. Guaranty Ass'n*, 455 U.S. 691, 704 (1982). Because the NIT warrant was void from the outset due to the magistrate judge's lack of jurisdiction, there is simply no positive law upon which the FBI agents relied.

C. The court of appeals incorrectly held it objectively reasonable for government agents to rely on a warrant purporting to authorize discretionary searches of tens of thousands of unspecified computers throughout the world.

The court of appeals found good faith reliance under the following uncontroverted circumstances:

- six years before Mr. Werdene's case, the Department of Justice's Computer Crime and Intellectual Property Section alerted U.S. Attorney's Offices of the Rule 41 "problem[]" with NIT warrants, and recommended

instead that government agents seek individual warrants in each district in which computers to be searched may be located;

- two years before Mr. Werdene's case, a U.S. Magistrate Judge denied a government application for a similar warrant on the ground that it would be invalid under Rule 41(b);

- while procuring the NIT warrant at issue here, the government simultaneously sought an amendment to Rule 41(b) to actually permit NIT warrants;

- the warrant application conspicuously represented the property to be searched as in the Eastern District of Virginia, and noted that searched computers may be located "wherever" only on page 29 of a 31-page affidavit;

- the NIT warrant authorized discretionary searches of tens of thousands of unspecified computers.

If good faith means anything at all, surely this is not it—both the circumstances of the NIT warrant's procurement and the warrant's obvious lack of particularity establish that.

Circumstances of procurement. Under the good-faith exception to the exclusionary rule, evidence is to be suppressed only when a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances. *See, e.g.*, *Herring v. United States*, 555 U.S. 135, 145 (2009); *United States v. Leon*, 468 U.S. 897, 922 n.23 (1984). Deliberate, reckless, grossly negligent, and recurring negligent conduct on the part of government agents is deterrable and worth the cost of exclusion. *Herring*, 555 U.S. at 144.

The NIT warrant here was sought in February 2015—six years after contrary internal government guidance was promulgated, two years after the first judicial authority denying a NIT-type warrant issued, and almost eighteen months after the government began the process of seeking an amendment to Rule 41(b) to permit NIT warrants. The agents here knew, without a doubt, that computers in virtually every federal district would be searched—the warrant affidavit

noted that Playpen had 150,000 registered users, and explained—however obliquely— that accessing computers would be searched "wherever located." Yet, apparently because it was deemed too much trouble to submit essentially the same warrant application in each district, the FBI sought one warrant for a worldwide search. That is not good faith—it is reckless, grossly negligent, or recurrent negligent behavior that exhibits a deliberate disregard for Rule 41(b).

Lack of particularity. In *Leon*, the 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. at 923. The Court enforced that standard in *Groh v. Ramirez*, 540 U.S. 551, 558-63 (2004), where suppression was ordered because a warrant failed to describe the items to be seized, and it is now time to do the same with respect to a warrant failing to particularly describe the place to searched.

The purpose of the particularity requirement is to eliminate, as much as possible, the discretion the executing officer has over the place to be searched or the things to be seized. *See Stanford v. Texas*, 379 U.S. 476, 481-83 (1965). The most extreme example of discretion in this context is the general warrant, the use of which against the American colonists inspired the adoption of the Fourth Amendment. *Id*. at 481-82. Early general warrants were the most open-ended, giving officers discretion to search wherever they pleased for libelous writings, for instance. *Id*. at 482. They were more circumscribed by the founding era, "typically authoriz[ing] [the search] of all persons connected [with] the premises [or] all persons connected with the publication of a particular libel." *Id*.

Ultimately, the particularity required is circumstance-specific, but in order to pass constitutional muster, the warrant must be as specific as possible so that "nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). *Cf. Matter of Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197, 212 (2d Cir. 2016) (to avoid being general, "[w]arrants issued in accordance with the Fourth Amendment . . . identify discrete objects and places, and restrict the government's ability to act beyond the warrant's purview—of particular note here, outside the place identified, which must be described in the document").

No reasonably well trained agent would think that a single warrant authorizing the search of 150,000 unspecified places—while permitting the agent unlimited discretion, exercised here, to determine which of those places to actually search—passes muster under the Fourth Amendment. All the more so where, as here, the warrant could have particularized the places to be searched by the usernames of those accessing unlawful areas of Playpen. Indeed, the breadth of the NIT warrant alone makes reliance unreasonable. One cannot imagine a magistrate judge issuing, or a court upholding, a single warrant authorizing an in-person search of the homes of 150,000 Americans—even assuming probable cause and identification by address. The only difference here is that the potential intrusion into 150,000 homes was far more easily and quietly accomplished. But that is a powerful reason to enforce the particularity requirement, not to disregard it. *See Riley v. California*, 134 S. Ct. 2473, 2494 (2014) (comparing broad authority to search cell phones to general warrants).

D. This case is an appropriate vehicle for resolving the questions presented.

This case is an appropriate vehicle for resolving the questions presented, as the issues are fully preserved and the court of appeals ruled the NIT warrant invalid under both the Fourth Amendment and Rule 41(b). Although the court did not reach the merits of the particularity issue, it did hold that—for good-faith purposes—the warrant was not so deficient in this regard as to make reliance unreasonable. App. A at 16 n.6, 26. All aspects of the good-faith issue are therefore presented in this case, as are the underlying merits issues implicating the Fourth Amendment and Rule 41(b). There are no impediments to further review of these important questions, and Mr. Werdene urges the Court to grant his petition and resolve them here.

CONCLUSION

For all of the foregoing reasons, a writ of certiorari should issue to review the judgment of the United States Court of Appeals for the Third Circuit entered in this case on February 21, 2018.

Respectfully submitted,

/s/ Brett G. Sweitzer

BRETT G. SWEITZER
Assistant Federal Defender
Chief of Appeals

LEIGH M. SKIPPER
Chief Federal Defender

Federal Community Defender Office
for the Eastern District of Pennsylvania
Suite 540 West, Curtis Center
601 Walnut Street
Philadelphia, PA 19106
(215) 928-1100